Por una Red más Segura

X1RED+SEGURA

Informando y educando

v1.0

Ángel-Pablo Avilés
"Angelucho"

"Vídeo de presentación del libro"
Canción por: David Insonusvita

"Haz click aquí para ir al vídeo"

por Angelucho

Basado en la obra

"El Blog de Angelucho"

http://www.elblogdeangelucho.com/

X1RED+SEGURA

INFORMANDO Y EDUCANDO V 1.0

Ángel-Pablo Avilés
“Angelucho“

Autor: Ángel-Pablo Avilés “Angelucho”

Diseño de Portada: David Avilés

Corrección: Laura Fernández Frutos

Maquetación: Laura Fernández Frutos y Paula García Arizcun

Depósito Legal: TO-326-2013

Primera edición, mayo de 2013

Impreso en España / Printed in Spain

“Internet no es informática, es información, es la vida real presentada en un mundo virtual.”

“Informar, educar y sensibilizar es el camino para conseguir una Red más segura para poder disfrutar de sus bondades.”

“Nosotros somos nuestra mayor vulnerabilidad en Internet, pero también somos nuestro mejor antivirus.”

A mi familia.

A los que estuvisteis y ya no estáis.

A los que sufrís mi ausencia aún estando presente.

A los que me aguantáis cada día.

A los que me animáis, porque me dais ganas de seguir.

A los que me desanimáis, porque potenciáis mi ánimo.

A tod@s los que me habéis informado y enseñado.

ÍNDICE

PRÓLOGO

En un libro como el que tiene usted entre las manos, querido lector, descubrirá en breve que, la parte menos interesante, es este prólogo.

Desgranando la vida digital, o vida 2.0 (casi ya 3.0) como dicen los gurús de las Tecnologías de la Información, encontramos multitud de aproximaciones más o menos técnicas y más o menos acertadas sobre lo que es y qué contiene este universo "conectado" en el que vivimos nosotros, padres 1.0, y el que viven nuestros hijos que son completamente 2.0 y 3.0.

¿Qué veo diferente en el libro de Ángel que no veo en otros libros o escritos sobre este extenso concepto que es Internet? Lo primero de todo, que Ángel ha escrito un libro dirigido a personas. Sobre todo, a personas que sienten, aman, disfrutan, sufren o, simplemente, desarrollan sus vidas con la tecnología a su alrededor. No es un libro más que requiera incorporar términos abstractos, ajenos a nuestra vida cotidiana.

Lo segundo, la importancia que Ángel da al componente moral de esas personas cuyo universo se extiende más allá de las fronteras físicas. ¿Y por qué es tan importante este componente moral? Porque, por desgracia, no todas las personas que aprovechan la tecnología, lo hacen con el objetivo de hacer el mundo mejor; como hace Ángel con este libro, como intentan hacer muchas de las personas sobre las que leerá más adelante.

Existen riesgos y amenazas en Internet. Como existen en la calle. Con la sutil, y muchas veces imperceptible, diferencia de que las amenazas en Internet no se quedan en la calle cuando cerramos las puertas de nuestras casas sino que, en un mundo donde todo está conectado, hasta nuestro teléfono móvil es una potencial fuente de dolores de cabeza y preocupaciones.

¿Cuál es la excelente noticia? Que Ángel es un maestro en transmitir los consejos y trucos, de los que muchas veces diremos "evidentes" (aunque nunca nos

hemos parado a pensar en ellos), para tener una vida "saludable" en, con, a través y dentro de la tecnología e Internet.

Porque, como bien aprenderemos a través de la experiencia, vivencias y sabiduría de Ángel, pequeñas acciones y un mínimo sentido común nos llevarán a que la tecnología aumente, mejore y enriquezca nuestras vidas.

Creo que no hay mejor conductor para este viaje tan apasionante que es descubrir un Internet seguro y sorprendente.

Román Ramírez Giménez

Responsable de Seguridad en Arquitecturas, Sistemas y Servicios
Ferrovial
Fundador del Congreso de Hackers Rooted CON

DECLARACIÓN DE INTENCIONES DEL LIBRO

1. INTRODUCCIÓN

Creo que la mejor forma de empezar, este apartado en particular y este libro en general, es empezar por lo que origina todo esto, la motivación que me mueve a escribir y lo que antecede a este libro.

Como leeréis más adelante me considero internauta desde el principio de los tiempos. Cambiar la **TNC**[1] por un módem de 14.400 **bps**[2] fue el principio de todo, mis primeros pasos en la Red corrieron a cargo del **radiopaquete**[3].

Internauta, que no informático, con una visión amplia de Internet y de lo que a su seguridad se refiere, dada mi trayectoria personal como usuario y profesional como componente, y muy orgulloso, del Grupo de Delitos Telemáticos de la Guardia Civil. Ambas trayectorias me hacen conocedor de las bondades, peligros y problemáticas que la Red de redes nos ofrece.

---

[1] **TNC (Controlador de Nodo Terminal)** es una "pequeña caja negra" unida al ordenador y la radio de radioaficionado que mediante un *software* específico convierte las señales de audio en paquetes, consiguiendo la comunicación entre ordenadores.

[2] **BPS** o **Bits por segundo** o **b/s**, en una transmisión de datos, es el número de impulsos elementales (1 o 0) transmitidos en cada segundo. Es la unidad del Sistema Internacional de Unidades utilizada para expresar la velocidad de transmisión de datos o *bit rate.*

[3] ***Packet radio*** o **radiopaquete** es un sistema de comunicación digital para las comunicaciones entre computadoras que emplea un sistema basado en las emisoras de radioaficionados. Consiste en el envío, a través de la radio, de señales digitales mediante en pequeños paquetes que luego son reensamblados en un mensaje completo en el destino final.

Si pretendéis leer un texto especializado en temas relacionados con la informática, o seguridad informática, podéis dejar de leer este libro, sinceramente estaréis perdiendo el tiempo. Como he dicho en muchas ocasiones, y aunque hago mis pinitos en el maravilloso mundo de los ceros y unos, yo soy de los informáticos de "botón gordo", sí, de esos a los que nos gusta solo "apretar" el botoncito y que el programa nos lo dé todo hecho.

Para escribir esos textos especializados en seguridad informática y hacer esos programas, de "botón gordo" o no tan gordo, están los que me enseñaron a definir como "Científicos de la Seguridad Informática", los verdaderos *HACKERS*, los GRANDES[4] *(ellos se reconocerán)*, a los que dedicaré más de una alusión a lo largo de este libro para intentar desmitificar los falsos conceptos de este colectivo *(Comunidad)*.

Sin embargo, en este libro, podréis encontraros con "traducciones" o "interpretaciones" de esos textos, guías o manuales, sobre todo en lo relativo a la seguridad en Internet, dado que es el tema principal del libro.

Como os imaginaréis, tras leer este comienzo de *X1Red+Segura: Informando y Educando v1.0*, no vais a encontrar ningún manual de cómo utilizar un programa específico (salvo algún antivirus), cómo solucionar un mal funcionamiento de nuestro ordenador por un problema de ***hardware***[5] (salvo por algún ***malware***[6]), o cómo configurar una aplicación para un mejor funcionamiento (salvo configuración relativa a la protección en la Red).

2. EL ORIGEN

Todo empieza ante la cabezonería de intentar hacer llegar a mi círculo de contactos próximo (familiares y amigos), los problemas y peligros que me encontraba de forma cotidiana en Internet, para que pudieran evitarlos sin caer en ellos. Quería hacerles llegar alertas de cada uno de los problemas que yo detectaba e intentar evitar, con ello, que mis próximos fuesen víctimas de estafas, robos de identidad, o lo peor, que los más pequeños sufriesen en primera persona las graves

[4] **GRANDE** es el calificativo utilizado, en este libro, para hacer alusión a los *hackers*, a los *hackers* buenos, a los de verdad.

[5] ***Hardware*** es el conjunto de los componentes que integran la parte material de un ordenador.

[6] ***Malware:*** Como veremos en un apartado específico, *malware* se refiere a virus, programa malicioso o programa malintencionado.

consecuencias de topar con un ciberdepredador. Y todo por falta de educación digital por parte de todos y por falta del llamado "control parental" por parte de los mayores hacia los más pequeños.

Comencé informando de estos peligros a mi círculo, de la forma más tradicional, por teléfono o correo electrónico, incluso mediante una técnica muy antigua y olvidada, la conversación persona a persona *(difícil de explicar en esta era digital)*. Después decidí comenzar a transmitirles mis "descubrimientos" haciendo uso de las redes sociales, pero para eso debía crearme un perfil en alguna de ellas.

Antes tenía que elegir un nombre, todo internauta que se precie tiene que tener un pseudónimo *(nick)*. El problema era serio, tenía que elegir un "apodo" con el cual me sintiese identificado, algo que estuviera ligado a mí de forma natural. En mi época de radioaficionado, utilicé varios indicativos de estación de radio, unos eran combinaciones de cifras y letras a modo de matrículas que asignaba el organismo que gestionaba las licencias, eso no quedaría muy "personal", otros eran "apodos de radio", normalmente eran personajes de ficción, pero eso no quedaría serio.

De pronto me vino un "flash" que terminaría rotundamente con esta primera incidencia. Me di cuenta de que yo ya tenía *"nick",* "pseudónimo" o como queramos llamarlo: ***Angelucho***. Así es como me llamaban mis abuelos desde el mismo día en que nací y hasta el fin de sus días, eso sí que era un "*nick*" personalizado, y además el legado de mis abuelos.

Tras la creación de una cuenta en Facebook totalmente personal y privada me lancé al maravilloso mundo del *"microblogging*" en Twitter, donde mi "pseudónimo" estaba ya utilizado por lo que tuve que registrarme con uno similar ***"@_Angelucho_"***.

Poco después, los 140 caracteres de Twitter se me quedaban cortos, por lo que decidí escribir un blog en Internet. Un blog que tendría la misma intención, pero esta vez para llegar a los que suponía pocos lectores que se lo encontrasen por casualidad; pero me equivoqué y empezaron a leerlo más personas de las que yo podría haber pensado. Ni comparación con un blog "profesional" pero para mí todo un logro, por el mero hecho de llegar a alguien desconocido y que pudiera evitar el que cayese en las garras de un ciberdelincuente.

La mejor forma que tengo de presentaros ese blog es reproduciros de forma íntegra la entrada que publiqué para presentar *El Blog de Angelucho* en sociedad.

3. PRESENTACIÓN DE *EL BLOG DE ANGELUCHO*

"Bienvenidos a mi blog espero poder poner mi pequeño granito de arena para conseguir tener una Red más segura." Hasta aquí mi escueta presentación en mi primera entrada en *El Blog de Angelucho.*

Todavía no hace un mes desde que comenzó la singladura de este blog y ahora me doy cuenta de que no había hecho una presentación como Dios manda, una presentación en la que quede claro el porqué de este blog.

Mis comienzos en Internet datan desde antes de que existiera Internet como tal, desde mis tiempos de radioaficionado y el radiopaquete. También quiero dejar claro que yo no soy un especialista en seguridad informática, que me pierdo con el código binario, el lenguaje de los ceros y unos y por eso mi aprendizaje en las nuevas tecnologías ha seguido los consejos del sabio refranero español "la letra con sangre entra". Vamos, que llevo en las espaldas, o más bien en los ojos, horas y horas de monitor, de pantallas negras con sus formateos y muchas noches en blanco intentando arreglar lo que había roto o hasta que aprendía a configurar ese programa tan complicado.

Mi trabajo, desde hace unos años, está estrechamente ligado a Internet y todo lo que está relacionado con este medio, del que decían que era el futuro, pero yo digo que es el presente y casi el pasado.

Hace tiempo me rondaba la idea de colaborar con alguna asociación de mayores, pensando que podía ayudarles a **"conect@rse"** con las nuevas tecnologías perdiendo el miedo a las "maquinitas".

También mi interés se encaminaba en colaborar con asociaciones que fomentan la educación de padres e hijos en la utilización segura de Internet para evitar los "daños colaterales" de la Red en los menores, dado que tanto los unos como los otros, faltos de información y educación específica, caen en un grado de inconsciencia que desvirtúa la realidad de los peligros que existen en la Red al considerarse completamente inmunes y anónimos tras las pantallas de sus ordenadores o *smartphones* al estar totalmente protegidos en la soledad de una habitación.

Y, por supuesto, tenía muchísimo interés en aportar mi granito de arena para luchar contra, según mi opinión personal, la gran lacra que se escuda en el falso anonimato de la Red, la pedofilia y la pederastia.

No pretendo ser alarmista con el blog, al contrario, precisamente por mi trabajo y mi trayectoria en la Red, puedo afirmar que Internet ofrece muchísimas más bondades que peligros pero, como todo en esta vida, la falta de información lo hace peligroso y por eso creo que una buena educación apoyada con información

hará que cualquier internauta pueda tener niveles aceptables de seguridad en su uso de Internet.

Pensando que los 140 caracteres de Twitter o la "privacidad" de Facebook me impedían llegar a tanta gente como me gustaría hizo que abriese este blog: *El Blog de Angelucho.*

Tras unos días en "el aire" comenzaron a leerme y a comentar mis *posteos, tweets* y entradas en las redes sociales o en el blog.

Estas lecturas y comentarios de apoyo y consejos venían, entre otras, de personas a las que considero GRANDES en el mundo de la seguridad informática y a los que llevaba mucho tiempo siguiendo y leyendo, los verdaderos *HACKERS*, **los de verdad, quedando lejos del falso estereotipo de *hacker* como un pirata informático** sino que, al contrario, personas que ayudan y dedican su día a día a que todos estemos más seguros en Internet combatiendo los peligros y lacras que en la Red se encuentran, colaborando incluso con organismos, asociaciones y con las Fuerzas y Cuerpos de Seguridad del Estado y, por supuesto, desde la sombra y el anonimato, haciéndoles más grandes todavía. Seguro que se reconocerán en este pequeño párrafo que quiero que sirva de agradecimiento hacia ellos por animarme a darle al botón "seguir" ;-) *(Va por ti)*.

Pero también estos comentarios venían de personas totalmente ajenas a este "nuevo mundo" totalmente desconocedoras de todo lo que rodea a Internet. Sirva como ejemplo el comentario de una persona de mi familia, internauta novel, que comenzó su paso en la Red recientemente al comprarse un *smartphone* que tuvo que ser configurado por su sobrino. Su comentario fue que cuando leía mis *post* entendía todo lo que se explicaba en ellos y que le servían de ayuda para "navegar" más segura.

Precisamente es eso lo que pretendo con este blog y con mi paso por las redes sociales, llegar sin tecnicismos a la gente que realmente es vulnerable, por desconocimiento, a los peligros de Internet y que con mi pequeña aportación sepa cómo evitarlos.

¡¡RECORDAD!! Si no os sentís seguros en Internet en un momento puntual, tenéis que hacer exactamente igual que cuando no os sentís seguros en un lugar físico: no arriesgaros, dar media vuelta y continuar por otro camino no arriesgando JAMÁS vuestra seguridad y privacidad (va por ti) ;-)

Y no olvidéis que *INFORMACIÓN + EDUCACIÓN = INTERNET SEGURO* y que nosotros mismos somos nuestra peor vulnerabilidad, pero también somos nuestro mejor antivirus.

4. EL LIBRO

El libro pretende ser más bien una guía en la que se presenta al lector, menos técnico, lo que es Internet desde sus comienzos hasta nuestros días. Se presenta de forma detallada y sencilla explicando su funcionamiento y los servicios que nos ofrece, con el fin de que pueda ser accesible a los usuarios internautas más básicos en cuanto a conocimientos técnicos informáticos.

Igualmente, una vez detallados los conceptos básicos de Internet y los servicios que ofrece, se presentan los peligros actuales a los que nos podemos enfrentar en la Red de redes, con ello conoceremos su origen, su forma de actuar, quién los dirige y hacia qué objetivos. Gracias a ese análisis aprenderemos a identificarlos en sus distintas formas y "presentaciones" y por consiguiente sabremos defendernos y evitarlos.

Una guía en la que aparecen la inmensa mayoría de las entradas disponibles en *El Blog de Angelucho*, artículos, alertas, ciberconsejos, etc., relativos todos a la seguridad en la Red y dirigidos a todos los internautas aunque el objetivo principal es el navegante menos experimentado y por lo tanto con más posibilidades de convertirse en "cibervíctima".

Ni que decir tiene que, aunque los lectores de estos contenidos son mayoritariamente internautas adultos, el principal objetivo a proteger son los navegantes más jóvenes, niños y adolescentes, al ser los más desprotegidos en la Red por desconocimiento de los peligros que les amenazan en muchos de los casos, pero en la mayoría de las ocasiones el problema se da por una considerable ausencia del denominado "control parental".

El libro está estructurado en siete capítulos.

Con el *Capítulo I. Internet,* el más literario y posiblemente el que pudiera resultar más técnico*,* se pretende mostrar al lector, y de forma muy somera, un pequeño análisis de lo que conocemos como Internet, desde sus orígenes hasta nuestros días, presentando los servicios que nos ofrece al usuario básico que utiliza la Red como una forma de comunicación, divertimiento y fuente de información.

La información que se presenta en este capítulo ha sido recabada de la fuente de información mayor que existe en la actualidad, Internet, por supuesto haciendo uso de su "oráculo": Google.

En los siguientes capítulos, alma del libro, se presentan de forma desglosada y explicada en lenguaje popular, los principales riesgos que nos encontramos en la Red, generalmente las formas de estafas que son utilizadas por los ciberdelincuentes

empleando distintas técnicas, desde los engaños más burdos a las técnicas de **ingeniería social**[7] más elaboradas.

Los cibercriminales, al igual que la tecnología, se encuentran en constante evolución, modificando y adaptando tanto las actividades como sus *modus operandi* acordes a las evoluciones tecnológicas.

No puede faltar en este libro una alusión a la comunidad *hacker*, a los buenos, a los que a pesar de ser tan vapuleados por la "mala prensa" que siempre los tacha de "delincuentes" siguen forzándose por mejorar sus conocimientos en cuestiones de seguridad, colaborando y luchando contra las lacras sociales que aprovechan el "falso anonimato" de la Red para cometer sus actividades delictivas, ciberdelincuentes a quienes confunden con los ***hackers***[8] de verdad y que no merecen el calificativo de *hacker*.

Por ello, la presencia de este colectivo en el libro tenía que hacerse notar. Presentes en el prólogo del libro, escrito por el fundador de uno de los mayores congresos de seguridad informática *(hacking)* de España, que en una ocasión me propuso colaborar en campañas de concienciación a padres y niños sobre los peligros de la Red. Presente en las entrevistas, realizadas a expertos en seguridad *(hackers)* que transmiten las medidas de seguridad que debemos utilizar todos los internautas y que colaboran, de forma activa, en la lucha contra la pedofilia en la Red. Por supuesto que en este apartado podrían aparecer muchísimos otros más, otros de los muchos *"hackers"* que se han cruzado en mi vida (profesores, compañeros, amigos…), pero necesitaríamos siete libros para que apareciesen todos.

Por supuesto, la presencia de a quién va dirigido el libro no puede olvidarse, me refiero a los denominados "inmigrantes digitales". Estando presente también en forma de entrevista con la que se pretende transmitir los ejemplos a seguir en el uso y disfrute de Internet.

Otro de los capítulos, de obligada aparición en el libro, es el relativo a la protección de los menores en la Red, tanto como víctimas potenciales de ciberdepredadores mediantes actividades delictivas encaminadas al acoso del menor en la Red para satisfacer las fantasías sexuales del pedófilo o pederasta, así como por ser los

[7] **Ingeniería social** es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar (ciertas) los ciberdelincuentes para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona comprometida a riesgo o abusos.

[8] ***Hacker:*** Especialista y apasionado de la seguridad informática. Esto concierne principalmente a personas que descubren, depuran y arreglan errores en los sistemas informáticos que auditan.

protagonistas principales de otras actividades muy dañinas en la lo el ciberacoso, entre otros, en los que el menor se convierte tanto en víctima como en autor de la actividad delictiva, con graves consecuencias en ambos casos.

Para finalizar se aportan seis diccionarios necesarios en el uso de Internet, éstos siempre estarán incompletos dada su continua evolución y aparición de nuevas terminologías.

5. RELATIVO A LOS CONTENIDOS

Muchos de los artículos, entradas, *post*, tanto de este libro como del propio blog son lo que se podría denominar "de cosecha propia", algunos de ellos están apoyados con información encontrada en Internet sobre el tema tratado. Otros, con la idea de hacer llegar el concepto de seguridad en la Red a todos los usuarios, podrían considerarse "traducciones" de textos existentes en la Red, traducciones de un lenguaje técnico a un lenguaje más próximo y cercano al usuario básico de Internet.

No obstante, siempre que es conocida la fuente de la información utilizada, es mencionada, y se aportan los créditos oportunos, en agradecimiento y reconocimiento, tanto en *El Blog de Angelucho* como en este libro.

Una vez leída esta introducción y "declaración de intenciones", deberíamos tener claras dos cosas relativas a lo que nos va a aportar este libro:

1. En este libro se va a tratar solamente de Internet desde el punto de vista del usuario básico, así como de los peligros que acechan en la Red. **NO ES UN LIBRO DE INFORMÁTICA.**

2. El lenguaje a emplear va a ser muy básico, explicando cada uno de los apartados de forma detallada y comprensible para todos. **EL LIBRO ESTÁ ESPECIALMENTE DIRIGIDO AL LECTOR SIN NINGÚN TIPO DE FORMACIÓN TÉCNICA.**

Queda claro que entre todos contribuimos a hacer de la Red un lugar más seguro, llevando a efecto el lema responsable de todo esto: ***hasthags***[9]: #elblogdeangelucho y *#X1red+segura.*

[9] **Etiqueta de almohadilla** (del inglés ***hashtag***, *hash*, 'almohadilla' y *tag*, 'etiqueta'), en servicios web tales como Twitter, Google+, FriendFeed o identi.ca, es una cadena de caracteres formada por una o varias palabras concatenadas y precedidas por una almohadilla (#). Representa un tema en el que cualquier usuario puede hacer un aporte y/o dar una opinión personal respecto al tema abierto con solo escribir la cadena de caracteres tras la almohadilla que dan nombre a ese tema. *Por ejemplo:* "Apenas aproveché el fin de semana y hoy tengo que volver al trabajo. #OdioLosLunes".

INFORMACIÓN
+
EDUCACIÓN
=
UNA RED MÁS SEGURA

X1RED+SEGURA

Angelucho

Comenzamos…

"Internet es positivo porque nos une, nos conecta. Incluso a las personas mayores. El estar conectado nos prolonga la vida y no solamente añade años a la vida, sino vida a los años."

Luis Rojas Marcos

I
INTERNET

Es obvio que para poder hablar de los peligros que nos acechan en la Red debemos conocer primero qué es Internet desde sus inicios. Quién lo creó y por qué, su definición, los usos de Internet y sobre todo cómo funciona.

Internet ha cambiado el modo en el que comprendemos las comunicaciones y, por lo tanto, el mundo. Tanto a nivel doméstico en nuestras relaciones personales o a nivel profesional o económico, la velocidad de la Red y las posibilidades que otorga han sido determinantes en los pocos años que llevamos de siglo XXI. Hoy en día es difícil encontrar a alguien que no haya oído hablar de Internet, pero no todo el mundo tiene claro lo que es exactamente ni cómo nace Internet, cuál es su origen ni quién invento la telaraña mundial a la que hoy se conecta medio planeta.

Internet puede entenderse de muchas formas. Del mismo modo que no es necesario conocer el funcionamiento interno de una televisión o la red de emisoras y repetidores para disfrutar de la programación, hoy en día también puede entenderse Internet de forma sencilla, por su utilidad, y también usarla sin tener grandes conocimientos técnicos.

Podemos definir a Internet como una "red de redes", es decir, una red que no solo interconecta ordenadores, sino que interconecta redes de ordenadores entre sí.

Una red de ordenadores es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos.

Internet es muchas cosas y sirve para fines infinitos; es un medio global de comunicación hoy día sumamente cotidiano en nuestras vidas.

Internet nos abre una inmensa ventana al mundo. Internet es, desde la imprenta, el mejor vehículo de difusión cultural conocido. Y desde su evolución a lo que se ha dado en llamar Web 2.0, las posibilidades se han multiplicado, ya que ahora es un medio donde el usuario no es pasivo, sino que puede interactuar con otras personas y crear sus propios materiales, al contrario que los medios de comunicación existentes hasta su aparición.

Desde el año 2010 la **Web 2.0**[10] ha cobrado un protagonismo especial, con cada vez mayor presencia en la forma de interrelacionarse los internautas.

Si hubiera que hacerlo, tal vez bastaría con decir que Internet es el mayor conjunto que existe de información, personas, ordenadores y *software* funcionando de forma cooperativa, publicando y organizando información e interactuando a nivel global.

Nunca ha existido nada igual a Internet y sus ramificaciones, pronto llegarán a todos los puntos del ciberespacio ideal: el conjunto de información y comunicación en el que estamos todos involucrados de una forma u otra.

Según el Instituto Nacional de las Tecnologías de la Comunicación (INTECO) a finales de 2011 se censaban cerca de 1.800 millones de usuarios de Internet en todo el mundo.

[10] **Web 2.0** está asociado a aplicaciones web que facilitan el compartir información. Un sitio Web 2.0 permite a los usuarios interactuar y colaborar entre sí como creadores de contenido generado por usuarios en una comunidad virtual, a diferencia de sitios web donde los usuarios se limitan a la observación pasiva de los contenidos que se ha creado para ellos. Ejemplos de la Web 2.0 son las comunidades web, las redes sociales, servicios de alojamientos de imágenes o videos, blogs, etc.

1. UN POCO DE HISTORIA. LOS INICIOS DE INTERNET

Pensamos que Internet es algo novedoso, pero estamos equivocados, los inicios de Internet datan de los años sesenta.

La historia de Internet se remonta al temprano desarrollo de las redes de comunicación y ante la idea de crear una red de ordenadores diseñada para permitir la comunicación general entre usuarios de varios ordenadores.

La historia de Internet apunta a Inglaterra donde se experimentó al principio con estos conceptos y así, durante 1968, el Laboratorio Nacional de Física de Gran Bretaña llevó a cabo la primera red experimental.

Pero los primeros textos en los que se documentan los inicios de Internet y de las interacciones sociales a través del *networking* (trabajo en red) están contenidos en una serie de memorándums escritos por **J.C.R. Licklider**[11], del Massachusetts Institute of Technology, en agosto de 1962, en los cuales Licklider discute sobre su concepto de *Galactic Network* (Red Galáctica), entonces era un sueño de ciencia-ficción porque no sería hasta 1974 cuando se comienza a utilizar la palabra "Internet".

Licklider concibió una red interconectada globalmente a través de la que cada uno pudiera acceder desde cualquier lugar a datos y programas informáticos. En esencia, el con-

[11] **Licklider:** Psicólogo, físico y matemático, que simple y sencillamente presagió Internet. Según el profesor Licklider el ser humano y las computadoras debían ser capaces de cooperar de forma flexible y eficiente para "tomar decisiones y controlar situaciones complejas" y expuso su visión para mejorar el diálogo hombre-máquina. Lo llamó "simbiosis hombre-ordenador" en una serie de artículos publicados en la década de 1960. La simbiosis hombre-computadora es un desarrollo previsto en la interacción entre hombres y computadoras electrónicas […].

cepto era muy parecido a la Internet actual. Licklider fue el principal responsable del programa de investigación en ordenadores de la **DARPA**[12] desde octubre de 1962. Mientras trabajó en DARPA convenció a sus sucesores Iván Sutherland, Bob Taylor y el investigador del MIT Lawrence G. Roberts de la importancia del concepto de trabajo en red.

Unos años más tarde, durante la denominada Guerra Fría, la ARPA (Agencia de Proyectos de Investigación Avanzados) del Departamento de Defensa de Estados Unidos, crea una red informática de ordenadores exclusivamente militar con el objetivo de que, en el hipotético caso de un ataque ruso, tener descentralizado el acceso a la información militar y que además se pudiera tener acceso desde cualquier punto del país. Esta red se creó en 1969 y se llamó **ARPANET**[13].

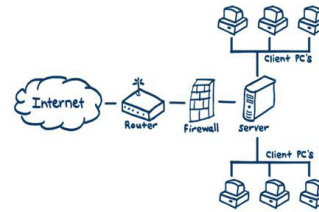
En sus orígenes, la red contaba con cuatro ordenadores distribuidos entre distintas universidades de los Estados Unidos. Dos años más tarde, ya contaba con cerca de cuarenta ordenadores conectados. Cada nodo de la red recibió una identificación numérica, conocida como "dirección", lo cual permitía que las computadoras se diferenciaran unas de otras para facilitar la puesta en marcha de procesos simultáneos. Pero fue a partir de 1972 cuando se comenzó a investigar la forma de que los paquetes de información puedan moverse a través de varias redes de diferentes tipos y no necesariamente compatibles. De esta manera se consiguen enlazar redes independientes consiguiendo que puedan comunicarse entre sí todos los computadores integrantes de la red. Este proyecto recibió el nombre de *Internetting*, y para referirse al sistema de redes

[12] **DARPA** (*Defense Advanced Research Projects Agency* o DARPA) es una agencia del Departamento de Defensa del Gobierno de los Estados Unidos, con sede en el Pentágono, responsable del desarrollo de nuevas tecnologías usadas en el área militar. Fue creada en 1958 ante el lanzamiento del SPUTNIK por los soviéticos. Su función era mantener la tecnología por encima de sus enemigos en plena Guerra Fría.

[13] **ARPANET** conectó los ordenadores centrales vía ordenadores de pasarela pequeños, o *routers*, conocidos como *Interface Message Processors* (IMP). El 1 de septiembre de 1969 el primer IMP llegó a UCLA. Un mes después el segundo fue instalado en Stanford. Despues en UC Santa Barbara y después en la Universidad de Utah.

funcionando conjuntamente y formando una red mayor se utilizó el nombre de Internet.

En 1975, ARPAnet comenzó a funcionar verdaderamente como red de información, uniendo centros de investigación militares y universidades estadounidenses. Tanto fue el crecimiento de la red que su sistema de comunicación se quedó obsoleto. Entonces dos investigadores crearon el Protocolo **TCP/IP**[14], que se convirtió en el estándar de comunicaciones dentro de las redes informáticas (actualmente seguimos utilizando dicho protocolo).



ARPANET siguió creciendo y abriéndose al mundo y cualquier persona con fines académicos o de investigación podía tener acceso a la red. Las funciones militares se desligaron de ARPANET y fueron a parar a MILNET, una nueva red creada por los Estados Unidos. La NSF (National Science Fundation) crea su propia red informática llamada NSFNET, que más tarde absorbe a ARPANET, creando así una gran red con propósitos científicos y académicos. La promoción y el desarrollo de las redes fue abismal, creándose nuevas redes de libre acceso que más tarde se unen a NSFNET, formando el embrión de lo que hoy conocemos como INTERNET.

Y la historia de Internet continúa...

Poco después de la adopción generalizada del protocolo TCP-IP ARPAnet fue desmilitarizada por completo, lo cual sucedió el 1 de enero de 1983, fecha que algunos mencionan como la de nacimiento de Internet. Para entonces ya estaba claro que las comunidades académicas eran las principales usuarias de la Red de redes y que su actividad principal era la de mandarse mensajes de correo electrónico. “En 1985 la Internet ya era una tecnología bien establecida”, afirma el documento de la Internet Society, pero era conocida solo para unos pocos y aún faltaban muchos años antes que comenzara a ser descubierta por la gente común, y ya ni hablar del sur del planeta.

Poco tiempo después, gracias a las literaturas de ciencia ficción, se comenzaron a utilizar términos para identificar esta nueva forma de comunicación. Poco a poco la palabra “ciberespacio” se consolidaba y empezaba a ser sinónimo de Internet.

[14] **TCP/IP** es un conjunto de protocolos. Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP). La noción de estándar de TCP/IP representa la manera en la que se realizan las comunicaciones en una red.

A esas alturas el futuro estaba desatado. En 1986 la Fundación Nacional de las Ciencias (NSF) de Estados Unidos estableció una *backbone* o troncal de Internet, con cinco nodos interconectados a altas velocidades. ARPAnet vivía sus últimos momentos, llegaba la hora de su extinción al borde de los noventa. En ese momento la acción se trasladó a Suiza.

2. NACE EL WORLD WIDE WEB (WWW)

Comúnmente se refiere indistintamente a Internet y a la WWW como si fuese lo mismo, cuando esto no es así y su aparición es posterior al de la red Internet. En efecto, la WEB o WWW es una parte que se encuentra englobada dentro de lo que es Internet (accesible y disponible su funcionamiento mediante la red Internet).

En el Centro Europeo de Investigaciones Nucleares (CERN), el físico inglés Tim Berners Lee dirigía la búsqueda de un sistema de almacenamiento y recuperación de datos. Berners Lee retomó la idea de Ted Nelson (un proyecto llamado "Xanadú") de usar **hipervínculos**[15]. Robert Caillau quien cooperó con el proyecto, cuenta que en 1990 deciden ponerle un nombre al sistema y lo llamaron World Wide Web (WWW) o Telaraña Mundial.

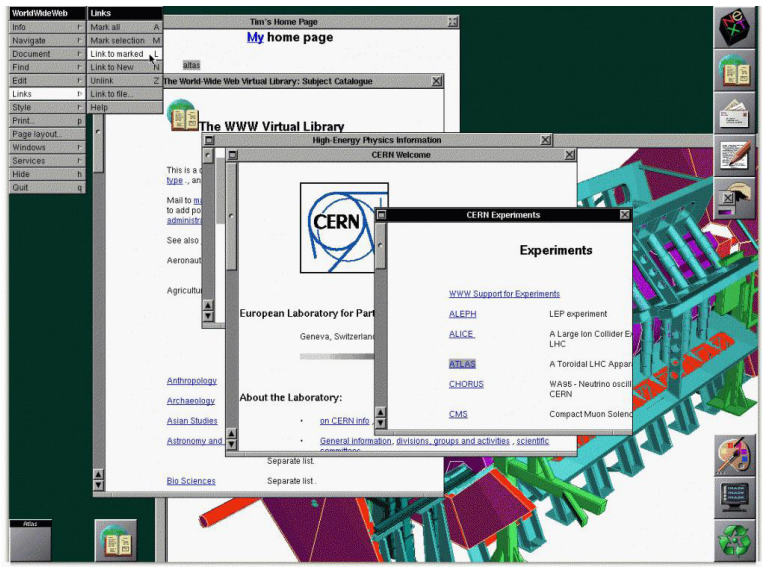
Fue el 6 de agosto de 1991, cuando Tim Berners-Lee publicó oficialmente la primera página de su proyecto en Internet, dando origen a la Web.

Berners-Lee tenía como finalidad intercambiar información entre científicos de todo el mundo. Esa primera web fue posteriormente actualizándose con nuevos documentos conforme evolucionaba el proyecto que fue creciendo poco a poco hasta convertirse, veinte años después, en un elemento esencial para cualquier usuario de la Red.

Desgraciadamente, en su momento, no se pudo capturar el aspecto que tenía la página de Tim, de nombre Info.cern.ch, el cual tuvo modificaciones constantes a

[15] **Hipervínculo** es un enlace, normalmente entre dos páginas web de un mismo sitio, pero un enlace también puede apuntar a una página de otro sitio web, a un fichero, a una imagen, etc. Para navegar al destino al que apunta el enlace, hemos de hacer *click* sobre él. También se conocen como hiperenlaces, enlaces o *links*.

lo largo de su existencia, siendo hasta el 3 de noviembre del 93, cuando se realizó el primer ***screenshot***[16].



Hasta ese momento, lo cierto es que Internet era una herramienta con muchas posibilidades, pero muy restringida, ya que todo se limitaba a universidades y otros centros estatales. De igual modo, si cualquier usuario común hubiese intentado participar, probablemente se encontraría con un lenguaje informático demasiado complicado y solo accesible a ingenieros preparados para ello.

La nueva fórmula permitía vincular información en forma lógica y a través de las redes de ordenadores. El contenido se programaba en un lenguaje de hipertexto con "etiquetas" que asignaban una función a cada parte del contenido. Luego, un programa de computación, hacía de intérprete, leyendo esas etiquetas para desplegar la información. Ese intérprete sería conocido como **navegador**[17].

WWW define al estándar que permite la visualización de todo tipo de contenidos en Internet, sean tanto textos como archivos multimedia (imágenes, gráficos,

[16] ***Screenshot*** es una captura de pantalla (también llamada pantallazo). Es una imagen tomada por un ordenador para registrar los elementos visibles en el monitor u otro dispositivo de salida visual.

[17] **Navegador** o **navegador web** (del inglés: *web browser*) es una aplicación que opera a través de Internet, interpretando la información de archivos y sitios web para que podamos ser capaces de leerla (ya se encuentre ésta alojada en un servidor dentro de la World Wide Web o en un servidor local).

textos, sonidos, etc.) siendo entonces un sistema basado en los protocolos anteriormente mencionados y no en la Internet en sí.

Tenemos entonces dos elementos importantes en esta comunicación, que son los hipertextos y los hipervínculos (también conocidos como hiperenlaces).

- **Hipertextos:** Está relacionado al HTTP *(Hypertext Transfer Protocol)* que corresponde al transporte de datos mediante estos hipertextos, interpretado por el HTML (*Hypertext Markup Languaje* que es la forma de crear estos textos).

- **Hipervínculos:** Permite realizar enlaces entre las distintas páginas web, ya que con tan solo "pinchar" el enlace en cuestión el usuario, permite visitar el sitio de destino, siendo entonces una especie de atajo con términos relacionados o con una palabra que indica el destino, o bien mediante la utilización de una imagen o botoneras especiales mediante aplicaciones web.

Era el detonador de una explosión. La nueva fórmula permitía vincular la información en forma lógica y a través de las redes. El contenido se programaba mediante un lenguaje de hipertexto con etiquetas que asignaban una función a cada parte del contenido. Y luego un programa de computación, un intérprete, era

capaz de leer esas etiquetas para desplegar la información. Ese intérprete sería conocido como *browser* o navegador.

En 1993 ocurrió algo muy importante: Marc Andreesen produjo la primera versión del navegador Mosaic, que permitió acceder con mayor naturalidad a la WWW. La interfaz gráfica iba más allá de lo previsto y la facilidad con la que podía manejarse el programa abría la Red a los menos expertos. Poco después, Andreesen encabezó la creación del programa Netscape.

Esta forma de enlazar siempre una información con otra llevó a Internet a relacionarse por completo entre sí mismo, y que con el aumento de público generó cientos de millones de páginas, buscadores, redes sociales y demás.

Internet comenzó a crecer más rápido que ningún otro medio de comunicación en la historia de la humanidad, convirtiéndose en lo que hoy conocemos todos.

3. INTERNET EN EL SIGLO XXI – LA WEB 2.0

Hoy en día Internet, como bien sabemos, es algo muy común en nuestras vidas y con presencia en la mayoría de los hogares. Es un medio de trabajo para muchas personas, también es un medio de comunicación que nos permite poder realizar una labor profesional o incluso particular desde la comodidad de nuestras casas o de cualquier lugar donde podamos encontrar señal inalámbrica wifi, o simplemente mediante nuestros *smartphones* de última generación.

Internet, en la actualidad, no es solo un medio necesario para nuestras rutinas profesionales sino que también es un fantástico medio de distracción ya que, gracias a la Red, encontramos mucha información y pasatiempos.

Es un "producto" que reúne las tres "B" de bueno, bonito y barato, además de una forma rápida y eficaz de comunicación inmediata con nuestro interlocutor, superando de muchas formas a los medios de comunicación convencionales.

Tal es el caso que, en cuanto a la velocidad, a la eficacia y a la eficiencia de Internet, los medios de comunicación convencionales han tenido que someterse a este monstruo que es Internet para poder seguir manteniendo vigencia y subsistir en este rápido mundo del siglo XXI. En la actualidad Internet significa llegar a un extenso mercado de necesidades de los consumidores.

Desde el año 2010 la Web 2.0 ha cobrado un protagonismo especial, con cada vez mayor presencia en la forma de interrelacionarse los internautas. Según el Instituto Nacional de las Tecnologías de la Comunicación (INTECO) a finales de 2011 se censaban cerca de 1.800 millones de usuarios de Internet en todo el mundo.

La Web 2.0 se caracteriza entre otras cosas por ser mucho más interactiva y dinámica, permitiendo una mayor participación y colaboración de los usuarios. Éstos dejan de ser meros lectores y se convierten en autores que tienen a su disposición una amplia serie de herramientas o plataformas de publicación, como los **blogs**[18], los **wikis**[19], los ***podcasts***[20], los portales de fotos y vídeos, las redes sociales, etc., donde poder expresarse, opinar, buscar y obtener información, construir el conocimiento, compartir contenidos, interrelacionarse, etc.

[18] **Blog** es un sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente.

[19] Un **wiki** o una **wiki** es un sitio web cuyas páginas pueden ser editadas por múltiples voluntarios a través del navegador web. Los usuarios pueden crear, modificar o borrar un mismo texto que comparten.

[20] El ***podcasting*** consiste en la distribución de archivos multimedia (normalmente audio o vídeo, que puede incluir texto como subtítulos y notas) mediante un sistema de redifusión (RSS) que permite suscribirse y usar un programa que lo descarga para que el usuario lo escuche en el momento que quiera.

4. EL CORREO ELECTRÓNICO

Conceptos básicos

El correo electrónico podríamos catalogarlo como el "servicio" estrella de Internet en cuanto a la comunicación directa entre personas.

Sin lugar a dudas, el servicio de correo electrónico (o *e-mail,* por *electronic mail)* es el más tradicional y el más utilizado por los usuarios de Internet. Algunos lo señalan como la versión más "humilde" de la Red. En la actualidad existen pocas posibilidades de mantener una comunicación actualizada y efectiva, ya sea laboral o personal, si no se cuenta con un correo electrónico o *e-mail*.

El nombre de **correo electrónico** proviene de la analogía con el correo postal: ambos sirven para enviar y recibir mensajes, y se utilizan "buzones" intermedios (servidores), en donde los mensajes se guardan temporalmente antes de dirigirse a su destino, antes de que el destinatario los revise.

E-mail o correo electrónico es un servicio de Red para permitir a los usuarios enviar y recibir mensajes y ficheros mediante sistemas de comunicación electrónicos.

Una dirección de *e-mail* se compone de dos partes:

- La parte de usuario **(Cyberusuario)**
- La parte del dominio **(hotmail.com)**

Ejemplo: **Cyberusuario@hotmail.com**

Funcionamiento de un *e-mail*

Un *e-mail* pasa por al menos cuatro ordenadores durante su período de vida:

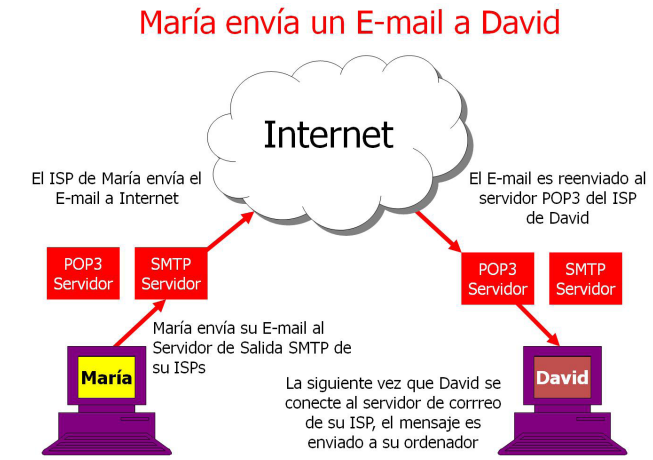
- Servidor de correo. Máquina dedicada exclusivamente a tratar el *e-mail*.
- El mensaje se confecciona en el ordenador del usuario, luego es enviado al servidor de correo de salida de su **ISP**[21] *(Simple Mail Transfer Protocol* o **SMTP**[22])

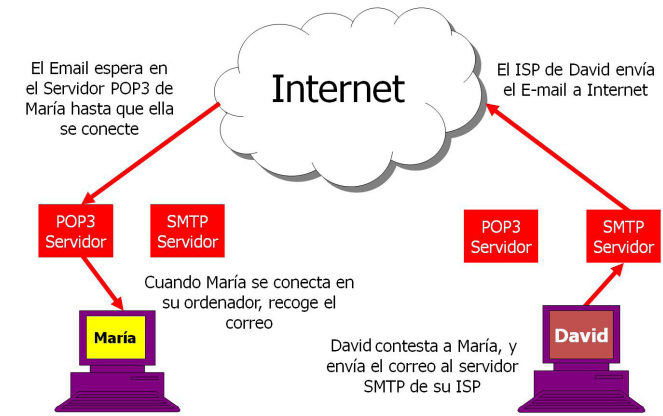
[21] **ISP** (*Internet Service Provider,* Proveedor de servicios de Internet).

[22] **SMTP (*Simple Mail Transfer Protocol*, Protocolo Simple de Transferencia de Correo)** Protocolo estándar de Internet para intercambiar mensajes de *e-mail*.

- El servidor de correo del ISP encuentra el servidor de correo de entrada del destinatario (**POP3**[23], **IMAP**[24], etc.) y envía el mensaje.
- El mensaje es obtenido por el ordenador del recipiente o destinatario.

Ejemplos:





[23] ***Post Office Protocol*** (**POP3**, Protocolo de Oficina de Correo o Protocolo de Oficina Postal) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto.

[24] **IMAP** ***(Internet Message Access Protocol)*** es un protocolo de aplicación de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.

Comparándolo con un correo postal **los mensajes de *e-mail* tienen:**

- **Cabecera o *header* (el sobre).**
- **Cuerpo del mensaje (la carta en sí) con los adjuntos *(attachment)*.**

Formato de un correo electónico (norma RFC 822)

El correo electrónico que se envía desde cualquier ordenador sigue una norma internacional con el objeto de ser legible desde cualquier otro ordenador que se reciba.

Básicamente un mensaje de correo electrónico se divide en tres partes:

1. **Encabezado o cabecera técnica *(header)***
2. **Cuerpo del mensaje**
3. **Archivos adjuntos *(attachment)***

Encabezado:

El encabezado del mensaje normalmente no está a la vista de quien lo recibe, no obstante es visible una vez habilitada la opción dentro de las propiedades de las opciones de configuración de los programas gestores de correo electrónico o *webmail.*

El encabezado o *header* es la parte más importante de un correo electrónico, dado que nos va a aportar la información desde donde nos enviaron el correo electrónico y por donde pasó hasta que llegó a nuestro ordenador, reflejando la cuenta de correo que nos lo envió, las fechas, las horas, e incluso por los servidores por donde pasó (los matasellos de las cartas postales).

Cuerpo del mensaje:

Es el mensaje en sí, tal como lo vemos en nuestras pantallas de ordenador o cualquier otro dispositivo conectados a Internet. Puede estar redactado en formato de texto plano *(Plain Text)* y/o HTML, es decir como una página web, lo que permite darle formato al texto, utilizando un gráfico de fondo, etc.

Archivos adjuntos *(attachments)***:**

La gran mayoría de los programas de correo electrónico actuales tiene la posibilidad de adjuntar al texto del mensaje un archivo, usualmente residente en el disco de nuestro ordenador. Este archivo puede ser de cualquier tipo, un programa ejecutable (*.exe), archivo comprimido (*.zip), una imagen gráfica (*.GIF, *.JPG, etc.), un archivo de texto o cualquier otro tipo de archivo informático.

Como consejo general, debemos cuidarnos de los archivos adjuntos a los correos que recibimos, no debiendo abrir nunca un archivo adjunto en un correo electrónico que provenga de alguien que no conocemos. Hoy en día el correo electrónico es una de las principales vías de difusión de virus.

5. SOCIALIZACIÓN EN INTERNET

La socialización "cara a cara" está siendo suplantada por la pantalla del ordenador. Ahora, cuando miramos a nuestros amigos a los ojos no vemos más que nuestro propio reflejo en el monitor. Las nuevas tecnologías ponen a nuestro alcance formas de crear relaciones personales con otros usuarios, de forma rápida y protectora. Necesitamos preguntarnos si las relaciones a través de la Red pueden ser consideradas reales o si solo se deben llamar así en el caso de haber un cara a cara entre los usuarios.

La Red ha conseguido ofrecer a la población mil maneras distintas de conocer a gente, hacer nuevos amigos e incluso iniciar relaciones sentimentales. Los chats, el Messenger y las redes sociales se nos presentan como fuertes herramientas de socialización. Éstas se han creado para conseguir una socialización más activa y amplia… parece increíble todos los amigos que puedes llegar a hacer en la Red durante un solo día, cuando en la vida normal no contamos ni con dos amigos de verdad. Lo más normal sería que todos usáramos estas herramientas para lo que realmente fueron creadas, reforzar y ampliar nuestra vida social desde el respeto, la simpatía y el deseo de conocer a nuevas personas. También es una realidad que hay muchos cibernautas que usan los chats y redes sociales para conocer gente nueva e introducirla en su vida real.

Gracias a esta socialización, el conocimiento se comparte con el uso de las Tecnologías de Información y Comunicación (TIC).

Las redes sociales

Ya se cumplieron los veinte años del aterrizaje de Internet en España. En aquellos tiempos, los que hacíamos de la comunicación un hobby, dejábamos atrás nuestras viejas emisoras de radioaficionado gracias a las cuales conseguíamos mantener conversaciones mediante voz (fonía) a largas distancias aprovechando los buenos días de propagación de las ondas hertzianas o a distancias inimaginables mediante el uso de la telegrafía (morse). Por aquel entonces también empezamos a dar nuestros primeros pasos en lo que se podría considerar como la antesala de Internet, mediante el denominado radio paquete *(ver nota al pie en página 17)* conectando nuestras emisoras de radioaficionado a los súper ordenadores "386" a 33 MHz y 4 MB RAM.

Entre 1992 y 1994 se produjo la implantación de Internet en la mayor parte de las universidades y la llegada de más servicios globales y proveedores de acceso. 1995 fue el año definitivo para la popularización de Internet en España.

Recientemente, una agencia de noticias española, especialista en análisis de tecnologías y tendencias web, se hizo eco del imparable crecimiento de una conocidísima red social en Internet que, en tan solo ocho años, está en el punto de alcanzar los mil millones de usuarios en todo el mundo.

Este sorprendente crecimiento llama la atención porque no solo se ha dado en regiones geográficas "lógicas", por su alto nivel de avance tecnológico, donde se observa que un elevado porcentaje de la población se encuentra de una u otra forma conectada a las nuevas tecnologías (el 58,3% en Europa y el 78,3% en Norteamérica) sino que se observa un potencial aumento de usuarios en países con menor desarrollo económico como en África y Asia.

En nuestro país, según las estadísticas de finales del año 2010, se censaban más de 21,5 millones de internautas (un 55% de la población de española), de los que el 73% hacían uso de Internet de forma diaria y desde su propio domicilio.

Con Internet llegaron nuevos vocablos que se hacen hoy en día imprescindibles en casi cualquier conversación, conceptos de comunicación inimaginables hace veinte años pero imprescindibles en nuestro día a día, tanto en el ámbito personal, como forma de contacto con amigos y familia, como en el ámbito profesional.

Las redes sociales tienen sus inicios entre los años 2001 y 2002, cuando aparecen ciertas redes de amigos, haciéndose populares en el año 2003.

Con ellas se deja atrás la conectividad tecnológica para dar paso a una conexión humana, podemos tener una reunión con los antiguos compañeros de instituto sin movernos de nuestro sofá o cerrar un negocio con un cliente en Taiwán desde nuestro propio despacho.

CONCEPTOS BÁSICOS

Antes de entrar en materia tenemos, y debemos, que tener claros ciertos conceptos que nos facilitarán no solo la lectura de este texto sino que también ayudarán a comprender el fenómeno de las redes sociales en la actualidad, presentes de forma latente en la vida de todos nosotros.

- **Red social en Internet:** Podríamos definir que redes sociales son estructuras sociales compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, aficiones, intereses comunes personales o profesionales…
- **Socialización:** La socialización es un proceso por el cual el individuo acoge los elementos socioculturales de su ambiente y los integra a su personalidad para adaptarse en la sociedad.

REDES SOCIALES EN INTERNET

Las redes sociales en Internet son sitios web en los que un grupo inicial de participantes invita a conocidos a formar parte de ella, de forma que cada nuevo miembro trae a nuevos miembros y el número de participantes y enlaces va creciendo.

En el año 2003 vieron la luz algunos de los sitios más populares que lograron hacer crecer exponencialmente el uso de Internet, comenzaron a denominarse comunidades y las más importantes eran MySpace, Friendster, Tribe y Xing, entre otras.

Fueron precisamente estos sitios los pioneros en lograr que las redes de interacción o círculos de amigos comenzaran a socializarse, llegando a captar la atención de miles de millones de usuarios de todo el planeta, añadiendo (gracias a las nuevas capacidades técnicas, como es la WEB 2.0 también denominada Web social)

la oportunidad de agregar comentarios en foros, mensajería instantánea y, eventualmente, listas de amigos, permitiendo interactuar al usuario en los contenidos del *site*.

Estos lugares se han convertido en lugares de negocio para empresas, pero sobre todo en lugares para los encuentros humanos. Son formas de interacción social, entendido como lugares de intercambio entre personas, grupos o instituciones, que poseen las mismas necesidades ofreciendo a sus usuarios un lugar común para desarrollar comunicaciones constantes.

Una red social permite, a sus usuarios, construir un perfil público o semipúblico dentro de los límites que cada plataforma ofrece. Se constituye por un grupo de personas ligadas, en general, por intereses comunes, abiertos a compartir pensamientos, pero también pedazos de la propia vida: desde enlaces a sitios que consideran interesantes hasta las fotografías o los propios vídeos personales.

Las redes sociales han irrumpido en la vida de millones de personas sin importar su edad, sexo, condición social, religión o preferencia política.

A comienzos del año 2012 podemos afirmar que las redes de interacción social se han convertido en uno de los elementos de Internet más difundidos, ya que ofrecen a sus usuarios un lugar común para desarrollar comunicaciones constantes. Esto es posible gracias a que los usuarios no solo pueden utilizar el servicio a través de su ordenador personal, sino que además en los últimos tiempos se puede participar en este tipo de comunidades a través de una gran variedad de dispositivos móviles, tales como teléfonos móviles u ordenadores portátiles, marcando la nueva tendencia en comunicaciones personales. Ahora Internet es igual a comunidad. Aprovechando sus ventajas, la Web social es también utilizada por las empresas como una manera efectiva, y muchas veces gratuita, de márketing, para estar en interacción con sus clientes actuales y potenciales.

A modo de ejemplo sirvan los números relativos a la archiconocida red social Facebook que, tras su aparición en el año 2004, cuenta con más de 1.000 millones de usuarios en 2012.

Funcionamiento

Estas redes sociales se basan en la teoría de los seis grados. Seis grados de separación es la teoría de que cualquiera en la Tierra puede estar conectado a cualquier otra persona en el planeta a través de una cadena de conocidos que no tiene más de seis intermediarios. Esta teoría defiende que las personas tienen un

contacto, que a su vez tiene otro y otro y así hasta seis que unen a cualquier persona. Cuando la teoría se formuló, en 1929, era difícil comprobar su validez, pero con Facebook sí se ha podido. Los investigadores han analizado las rutinas de amistad de los usuarios, dentro y fuera de Facebook. Según la Universidad de Milán, más del 50% de las personas tiene más de cien amigos y contactos.

Las herramientas informáticas para potenciar la eficacia de las redes sociales *on-line* ("*software* social"), operan en tres ámbitos, "las 3C", de forma cruzada:

- Comunicación (nos ayudan a poner en común conocimientos).
- Comunidad (nos ayudan a encontrar e integrar comunidades).
- Cooperación (nos ayudan a hacer cosas juntos).

Por tanto se podría resumir que el funcionamiento de una red social se basa en que un usuario invita a otros usuarios a que establezcan una conexión *on-line* por medio de una plataforma web o red social. Cada usuario que acepta la invitación pasa a formar parte de su red contactos. Cada uno de estos nuevos usuarios realiza la misma operación, invitando a otro número determinado de conocidos, esparciéndose de este modo las conexiones. Con las relaciones creadas, el usuario crea lo que hoy se conoce por red de contactos, pudiendo intercambiar información de diversa índole, en función del tipo de red social.

Tipología

En el presente texto vamos a centrarnos exclusivamente en las digitales o redes sociales *on-line* que son las que tienen su origen y se desarrollan a través de medios electrónicos e informáticos. Hay muchos tipos de redes sociales en Internet y sus servicios son diversos, hay redes sociales que son para ligar, hacer negocios, ponerse en contacto con antiguos compañeros de estudios o compartir. En cuanto a encuadrar a cada una de ellas en un "tipo" definido existen varios criterios de clasificación.

- **Redes sociales verticales:** Las redes sociales verticales se basan en un tema concreto y buscan congregar un gran número de usuarios en torno a esa temática o fin concreto. Se pueden distinguir tres tipos dentro de estas redes: las redes sociales verticales profesionales (Viadeo, Xing, Linked In), las redes sociales verticales de ocio (Wipley, Minube Dogster, Last.FM y Moterus) y las redes sociales verticales mixtas.

Algunos ejemplos:

- Fotografía:
  - **Flickr**: sitio web que permite compartir fotografías y vídeos entre usuarios. Se pueden dejar comentarios, crear grupos, etiquetarlas. Cuenta con una versión gratuita y con otra de pago, llamada pro. Fue adquirida por Yahoo.
  - **Panoramio:** lugar para subir imágenes y geolocalizarlas. Fue iniciada por dos jóvenes españoles y comprada posteriormente por Google.
  - **Picasa:** organizador de fotografías de Google.
  - **Fotolog:** es una red social donde cada usuario puede subir una foto por día, en las cuales los amigos registrados en la página web pueden dejar comentarios debajo de las imágenes.
- Música:
  - **Last.fm:** red social musical. Se comparte toda la música que cada usuario escucha (mediante una aplicación se envía a last.fm lo que pasa por nuestros reproductores), se forman comunidades y se generan de manera automática grupos similares que nos podrían gustar. Antes ofrecía *streaming* de canciones y radio personalizada, pero tras pasarlo a servicio de pago, han anunciado que de forma definitiva retiran esta funcionalidad. También cuenta con una importante sección de conciertos, donde indica al usuario los que se celebrarán cerca de su lugar de residencia y donde el usuario puede indicar si asistirá además de dejar comentarios al resto de asistentes.
  - **Blip.fm:** un lugar donde hacer recomendaciones musicales. El resto de usuarios valoran si les gusta la canción, pueden introducir mensajes cortos, enviar esas notificaciones a otras redes como Twitter, Facebook, etc. Las canciones no residen en la plataforma, sino que se utilizan otras web como YouTube, goear, etc..
  - **Spotify:** aunque no sea una red propiamente dicha, está generando multitud de ellas a su alrededor y supone toda una revolución para el mundo de la música. Es una plataforma para escuchar música vía *streaming* (ha firmado acuerdos con las discográficas Universal Music, Sony BMG, EMI Music, Hollywood Records y Warner Music entre

otras, por lo que cuenta con una colección enorme). No se pueden agregar contactos, pero sí crear listas de canciones y compartirlas.

- **Vevo:** es una ramificación de YouTube específica para vídeos musicales.

- **MySpace:** es un sitio web, de interacción social constituido por perfiles personales de usuarios que incluye redes de amigos, grupos, blogs, fotos, vídeos y música, además de una red interna de mensajería que permite comunicarse a unos usuarios con otros.

• Vídeo:

- **YouTube:** es la plataforma más conocida para compartir vídeos. Comprada por Google, permite subir vídeos de no más de 2 GB de tamaño ni diez minutos de duración. Hay canales institucionales y se organizan eventos en *streaming*. Algunos vídeos pueden ser "embebidos" en otras páginas.

- **Vimeo:** es similar a YouTube. Los usuarios con cuentas gratuitas (limitadas) pueden cargar hasta 500 MB de vídeos estándar y solo un vídeo de alta definición a la semana. Vimeo se ha hecho un lugar en el abultado mercado de alojamiento de vídeo simplemente por su elegancia.

- **Dailymotion:** lo mismo que los anteriores. Dailymotion apoya y patrocina el proyecto sin ánimo de lucro One Laptop Per Child.

- **Google Video:** es un servicio de Google que hasta enero de 2009 permitía subir vídeos. Inicialmente nació como competencia de YouTube, a la que terminó comprando el 10 de octubre de 2006. Finalmente, Google Video pasó a funcionar como un mero buscador de vídeos en la red.

- **Joost:** algo así como una televisión a la carta vía Internet.

• Plataformas para emitir un evento en *streaming* :

- **Ustream:** emite en directo (y permite grabar al mismo tiempo).

- **Mogulus:** te ayuda a crear tu propio programa televisivo fundiendo tu *webcam* con *clips* de YouTube o *webcams* de otras personas. El servicio es gratuito pero se sustenta de la publicidad, por lo que cada diez minutos, se corta la emisión para que aparezca un anuncio.

· **Cover It Live:** emite vídeo junto a un apartado de chat y también puedes agregar contenido de Twitter (usando *hashtags* o listas). Dispone de una versión de pago.

· **Chatroulette:** entre los jóvenes de Estados Unidos se ha puesto muy de moda y como su propio nombre indica consiste en una ruleta de chats. Te conectas a la plataforma con tu *webcam* encendida y te toca charlar con algún otro usuario que se ha conectado desde cualquier parte del mundo. Hasta la mismísima Ashley Tisdale (actriz muy conocida entre los adolescentes por ser parte del reparto de High School Musical) se ha atrevido con esta ruleta.

- Otros:

  · Presentaciones: **slideshare.**

  · Marcadores sociales: **del.icio.us.**

  · Sistemas de promoción de noticias: **menéame, aupatu, zabaldu.**

  · Red de lectura: **anobii, librarything, entrelectores.**

- **Redes sociales horizontales:** Son transversales en cuanto temáticas y se centran más en los contactos: las redes sociales horizontales se dirigen a todo tipo de usuario y no tienen una temática definida ni un fin concreto. Las redes de este tipo más conocidas son Facebook, Orkut, Identi.ca, Twitter.

  - Redes de contactos: **Facebook, Tuenti, Orkut, Hogetti.**

  - Redes profesionales: **LinkedIn, Xing, Plaxo.**

  - *Microblogging* (aunque los creadores de Twitter digan que no se trata de una red social...): **Twitter, Jaiku, Plurk.**

  - Redes de conocimiento: **Zutagu** es una nueva red social para compartir el conocimiento entre internautas. Entre esas herramientas destacan un blog, un archivo, un lugar para guardar las direcciones, páginas tipo wiki o *microblogging.* Además, también se pueden crear grupos de interés.

Las redes sociales más conocidas son: MySpace, Facebook, Hi5, Tuenti, Orkut y otras más recientes como Twitter que se utiliza para comunicar al mundo lo que estás haciendo en cada momento, resumido en una pequeña frase de un máximo de 140 caracteres.

En definitiva,

esto no es el futuro

¡¡¡ES EL PRESENTE!!!

Los chats

Los chats han entrado de lleno en nuestras cibervidas y más allá. Da igual si participamos en ellos como forma de intercambio de conocimientos, como forma de relacionarnos con otras personas o los utilizamos como medio de comunicación entre nuestros contactos. Es un medio de sobra conocido por todos nosotros, los internautas. Presentes en cualquier web o marca que se precie, independientemente de su temática, pero indispensables para ser un punto de reunión para los seguidores donde comentarán sus inquietudes y pareceres sobre un tema en particular.

Todo el mundo utiliza la palabra chat como sinónimo de charla en Internet para comunicar a dos o más personas. El chat puede ser considerado como un espacio en común para conversar por Internet. Es un medio de comunicación ampliamente utilizado siendo utilizado por personas de la misma localidad, región o país, pero también es tan abierto que da la posibilidad de comunicación, y en tiempo real, con personas que se encuentran en puntos distintos del planeta.

Solamente necesitamos acceder vía web a cualquier sala de chat, con nuestra temática preferida, cualquier persona que conozca su existencia, podrá acceder y comunicarse con nosotros para compartir nuestras aficiones o intereses.

Existen tantos tipos de chats como temáticas posibles, negocios, cultura, música, amistad, relaciones personales, sexo, uno para cada una de las temáticas posibles.

La primera conversación mediante un chat, ordenador a ordenador, surgió en el año 1972. Esta conversación fue muy famosa, puesto que participaron en ella un paciente y su psiquiatra.

Posteriormente, en 1988, el científico Jarkko Oikarimen, crea el IRC o Internet Relay Chat. Para mí el padre de los chats al hacer posible el chat como lo conocemos hoy en día. Gracias a este programa se puede conversar de forma simultánea entre varias personas.

Los chats suelen estar divididos en *chat rooms* o *channels* (en español "salas de charla o canales"), normalmente organizados por temas.

Técnicamente se puede decir que una sala de chat es un lugar virtual que se encuentra alojado en un "espacio virtual" de un servidor de Internet que administra su funcionamiento.

Un chat, por norma general, se rige por unas normas básicas de "convivencia" en la Red, conocida como **NETIQUETA**, que se compone de un conjunto de reglas y consejos para favorecer la comunicación en el chat en orden como por ejemplo:

- **No escribir en mayúsculas,** puesto que se considera como el hecho de gritar.
- **No repetición de texto** de forma reiterada para evitar molestar al resto de usuarios.
- **No utilización de colores** en los textos al considerarlos molestos.
- **No insultar,** esto parece obvio, pero muchos chats se han malogrado por los continuos insultos que había en ellos, gracias al anonimato que proporciona la Red.

Todos los que chateamos somos conscientes de que no se escribe igual en un chat que como se escribe en una carta, en un documento, en nuestro trabajo o incluso en un correo electrónico. Por norma general en los chats nos olvidamos de las normas lingüísticas para darle mayor fluidez y rapidez a nuestra conversación. Los usuarios de chat usan casi siempre abreviaturas o simplemente utilizan la "fonética". *(Ver Capítulo VII. Diccionarios).*

Algunos ejemplos de este tipo de "lenguaje":

- ¿Por qué? o porque: "xq", "porq".
- Hola: "hla", "hl".
- ¿Qué tal estás?: "q tal?", "k tal?", "qtl?".
- ¡Saludos!: "salu2".
- "vns a mi qmple? :-P MK? :-) a2" . Traducción: "¿Vienes a mi cumpleaños? Me relamo de gusto. ¿Me quieres? Estoy contento. Adiós".

La mensajería instantánea

La mensajería instantánea es una forma de comunicación en tiempo real entre dos o más personas utilizando las nuevas tecnologías, y se identifica con las siglas I.M. (del inglés: *Instants messaging*).

Es un servicio de comunicación en tiempo real, mediante Internet, y utilizando distintos dispositivos como ordenadores, tabletas, *smartphones*, etc. La mensajería instantánea, desde sus inicios, ha ido sumando adeptos y evolucionando de forma sorprendente, hoy en día forma parte de la vida cotidiana de cualquier internauta que se precie.

¿CÓMO FUNCIONA LA MENSAJERÍA INSTANTÁNEA (IM)?

Para comunicarnos mediante mensajería instantánea con nuestros contactos debemos utilizar programas específicos, a estos programas se les conoce como

clientes de mensajería y que normalmente deben de ser instalados en nuestros dispositivos al igual que nuestros contactos para poder mantener la comunicación.

Gracias a la mensajería instantánea, y a diferencia de los primeros chats, no solo podemos compartir mensajes de texto sino que además podemos disfrutar de videoconferencias (audio y vídeo) y en tiempo real con nuestros contactos sin que la distancia sea impedimento. Además, otra de las bondades de ellos, es que algunos permiten incluso la multiconferencia, pudiendo mantener conversaciones con varias personas en la misma conversación o varias conversaciones privadas.

Además nos permiten el envío y la recepción de archivos de audio/vídeo y otro tipo de documentos.

En la actualidad existe la tendencia de incorporar mensajería instantánea en otros servicios de Internet, normalmente en redes sociales como por ejemplo Facebook o Tuenti, pero también y desde la llegada de la Web 2.0 este tipo de mensajería podemos encontrarlas en servicios web en incluso en servicios ***webmail***[25] (MSN, Gmail, etc).

Los clientes de mensajería instantánea más populares son:

- **Windows Live Messenger.** Perteneciente a la empresa Microsoft y posiblemente el más popular puesto que es utilizado por millones de usuarios en todo el mundo. Es conocido popularmente como **MSN** o **Messenger**, nombre usado por su antecesor.

- **Yahoo! Messenger.** Muy popular hace unos años aunque ha ido perdiendo puestos en el *ranking,* su utilización y funcionamiento es muy similar al Windows Live Messenger.

- **Google Talk.** Popularmente conocido como **Gtalk**, en auge en los últimos años y es el utilizado por los usuarios de Gmail.

- **Skype.** Es un *software* que permite comunicaciones de texto, voz y vídeo sobre Internet. También perteneciente a la empresa Microsoft. Este servicio absorberá, en el primer trimestre de 2013, a todos los usuarios de MSN que desaparecerá.

[25] Un ***webmail*** o **correo web** es un cliente de correo electrónico que provee una interfaz web por la que acceder al correo electrónico.

Todos estos clientes de mensajería instantánea están disponibles también en versión para ser instalados en *smartphones*.

Los blogs

¿QUÉ ES UN BLOG?

No cabe duda de que la palabra "blog" o *"weblog"* sea la más repetida en los últimos "cibertiempos". Existe una explosión de apariciones de esta forma de comunicación en Internet aunque realmente los blogs vieron la luz a finales de los años noventa.

¿Pero qué diferencia a los blogs de otros servicios de la Red?, ¿qué es exactamente un blog, *weblog* o bitácora?, ¿qué lo distingue de cualquier otro tipo de sitio web?

La diferencia es clara, un blog es una publicación *on-line*, al igual que otro tipos de servicios como la Web, con la salvedad de que las noticias, historias o artículos son presentadas en orden cronológico, lo primero que vemos cuando entramos en un blog es la publicación más reciente.

Los "blogueros" o editores de los blogs, tienen una periodicidad de publicación muy alta, atendiendo con ello a sus "ansiosos" seguidores quienes además pueden comentar su parecer sobre lo leído en el blog y así compartir su opinión con otros lectores. En ocasiones, estos comentarios son moderados y filtrados por el *webmaster* del sitio, en este caso el bloguero. El autor tiene la opción de darles respuesta, de forma que es posible establecer un diálogo entre el lector y el autor del artículo.

El uso o temática de cada blog es particular, los hay de tipo personal, periodístico, tecnológico, educativo, etc.

Crear y editar un blog es muy sencillo, tanto como utilizar cualquiera de los demás servicios que nos ofrece la Red. No se necesitan conocimientos técnicos, tan solo es necesario tener ganas de escribir, de contar historias o de opinar sobre un tema determinado.

Es tanto el auge de este servicio que incluso en el mundo empresarial se está extendiendo, pudiendo encontrar blogs específicos para clientes, para usuarios de

un determinado producto o incluso como medio de información para sus empleados.

Lo que está claro es que la presencia de los blogs se ha convertido en algo indispensable para los internautas que quieren estar informados, haciendo uso de los **RSS**[26] para estar al día sobre las noticias de sus temas preferidos haciéndose un servicio indispensable y complementario al periodismo tradicional.

6. INTERNET Y SUS MORADORES

"El acceso a Internet es una realidad ya para el 32,5% de las personas que pueblan el planeta, según un informe presentado por la ONU, que sitúa a Islandia, Noruega, los Países Bajos, Suecia, Luxemburgo y Dinamarca como los únicos países con más del 90% de sus habitantes conectados a la Red. España, en el puesto 39 con un 67,6%." (Periódico *Cinco Días*: http://www.cincodias.com, 14 de octubre 2012)

[26] **RSS** son las siglas de *Really Simple Syndication*, un formato XML para indicar o compartir contenido en la Web, de forma sencilla y recibiendo las noticias directamente en nuestros ordenadores.

Existen varios tipos de usuarios dependiendo de los estudios analíticos realizados o de la persona que exponga su opinión.

Unos dirán que los usuarios se dividen en **"usuarios profesionales"** o **"usuarios aficionados"** dependiendo de si dedican largos períodos de su tiempo de trabajo al uso de las TIC o si solo están interesados en la Red simplemente como afición con el único fin de informarse o como forma de relacionarse y socializar.

Otros van más lejos, llegando a crear glosarios con la terminología empleada para identificar a los usuarios de Internet de acuerdo a su actitud durante su paso por la Red *(ver Diccionario de usuarios de la Red, Capítulo VII. Diccionarios).* En estos diccionarios encontramos términos como:

Lamer: Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender. La palabra también viene del inglés *lame* ('cojo').

Newbie: Usuario principiante que acaba de integrarse en un grupo, comunidad o actividad *on-line.*

Hacker: Este término, frecuentemente utilizado de forma errónea, ha sido muy desprestigiado con el tiempo a través de la prensa, los medios de comunicación y de los propios usuarios de la Red para identificar a los cibercriminales. El término *"hacker"* normalmente denomina a personas expertas en alguna de las materias de la informática.

Cracker: Procede del inglés ***crack*** ('romper') y hace juego con las palabras ***criminal hacker.*** Son usuarios que, generalmente, se encargan de (solo y exclusivamente) "romper" sistemas de seguridad de aplicaciones mediante ***cracks, seriales*** (números de serie) o ***keygen*** (generadores de claves). El término también engloba a aquellos usuarios que violan **sistemas de seguridad** en beneficio propio o en perjuicio del sistema comprometido, pudiendo o no, robar información.

Sin embargo, aún estando de acuerdo con, al menos, algunas de estas "clasificaciones" yo quisiera hacer otra acorde a la filosofía de este libro; mi clasificación se enfoca de acuerdo a la denominada **"brecha digital".**

La **brecha digital** se define como la separación que existe entre las personas que utilizan las Tecnologías de Información y Comunicación (TIC) como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas y que aunque las tengan no saben cómo utilizarlas.

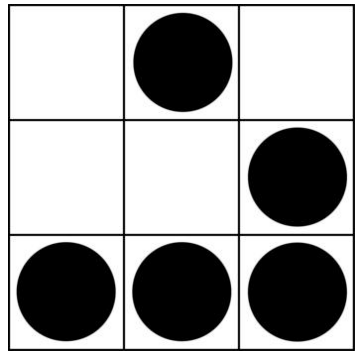
En definitiva, la brecha digital, no es otra cosa que el reflejo de la brecha social en el mundo digital y que enfrenta a dos generaciones, **los nativos y los inmigrantes digitales.** Una brecha que deja al margen de las nuevas tecnologías a muchas personas mayores en favor de aquellas que ha crecido "en paralelo" con dispositivos digitales y que ya no puede entender el mundo sin ellos. Una brecha entre los que se criaron con los libros y los profesores tradicionales y los que manejan con total naturalidad ordenadores, *tablets* o *smartphones*.

La mayoría de los niños, adolescentes y jóvenes actuales que tienen acceso a la Red (Internet, móviles, etc.) son los actuales nativos digitales porque reúnen una serie de características propias que les diferencian de las generaciones precedentes, son interactivos, multifuncionales y multitareas; se trata de una generación creativa que produce sus propios contenidos. ¡Siempre están conectados! Incluso crean sus propios lenguajes como ya hemos visto en páginas precedentes *(ver Capítulo Diccionarios). Ejemplo:*

X1Red+Segura

A estas dos "generaciones digitales" añadiría un grupo más para completar mi clasificación. Este nuevo grupo es el **colectivo responsable, con su contribución, de que hoy conozcamos Internet como tal, los "inventores" y guardianes de la Red de redes, los "padres de la criatura", los expertos que con su talento han permitido que Internet sea el inicio de una nueva era, la Era Tecnológica. Los *hackers.*** Por todo ello, tienen un protagonismo muy especial en este libro.

Los *hackers:* ¿héroes o villanos?



En una ocasión, un intrépido "jabato", me llamó "maldito", y os reproduzco la prueba que publicó en el artículo **"Mi experiencia en Blogger"** publicado en su blog ***Seguridad Informática "A lo Jabalí…".***

> "Hace poco más de un año que comenzamos el Loco Proyecto de ***Seguridad Informática "A lo Jabalí..."*** y no dejamos de sorprendernos. Cuando comenzamos a escribir el blog **la única pretensión** era poner nuestro granito de arena para mejorar la seguridad en la Red, publicar de forma comprensible algunos detalles técnicos (luego apareció el **"maldito"** ***Blog de Angelucho*** para **dejarnos por los suelos** ja, ja, ja) y dar a conocer sitios, que en nuestra opinión son interesantes para aprender seguridad informática."

Y por su "osadía" prometí vengarme y desenmascarar a los peligrosísimos *"jaquers"* como él (espero que me sigas llamando "maldito" mucho tiempo, total… ¡Ya hay un ***Maligno***[27]**…!**).

Quiero aprovechar este rinconcito del libro para dar mi opinión sobre el concepto que tengo del término o calificativo *hacker* y por fin desenmascarar a estos "oscuros personajes".

Dicen, las falsas creencias, que la gente de la comunidad *hacker* también denominada ***"underground"*** son una especie muy solitaria, que no tiene amigos, con

[27] ***Maligno*** es el pseudónimo utilizado por Chema Alonso, experto en seguridad informática y uno de los máximos referentes en este campo a nivel mundial, escribe en el blog http://www.elladodelmal.com/ y es consultor de seguridad en Informática64.

granos en la frente, antisociales... pero no, no es así, y os lo voy a explicar ***(espero que te reconozcas en tu frase).***

La definición de *hacker* ha tenido, a lo largo de su historia, muchas interpretaciones y connotaciones, casi siempre negativas.

Hacker es asimilado casi siempre con el "pirata informático", con el "ciberdelincuente", con el responsable de los delitos más sofisticados cometidos en Internet o valiéndose de la Red para cumplir sus objetivos delictivos.

Hay que ser realistas y en honor a la verdad tengo que decir que no le falta razón a quien en alguna ocasión lance estas afirmaciones, pero exactamente la misma razón que tendrían si afirmasen que todos los conductores son unos delincuentes porque son los responsables de los accidentes producidos por algunos conductores que se dedican a realizar carreras "kamikazes" en las carreteras, o que todos los *rockeros* son unos macarras descerebrados y drogadictos, o más común todavía, los falsos estereotipos, como por ejemplo sobre las chicas rubias, la forma de ser de los residentes en una determinada región y cientos de ejemplos más. Por supuesto estas afirmaciones no son más que falsedades.

Posiblemente en más de una ocasión habrá algún *hacker* delincuente, o una rubia sosa, o un *rockero* adicto a las drogas, pero queda claro que es algo que no se puede ni se debe generalizar. La mayoría de todos estos tipos de estereotipos son falsos y por ello no debemos juzgar a una persona en particular o un colectivo en general sin conocimiento suficiente sobre quien opinamos.

> "Saber romper medidas de seguridad no hacen que seas *hacker*, al igual que saber hacer un puente en un coche no te convierte en un ingeniero de automoción."
>
> **Eric Raymond**

La realidad, según mi humilde punto de vista y opinión, es otra muy distinta a este falso estereotipo. La persona que se dedica al *hacking,* el *hacker,* es una persona entusiasta de la seguridad informática en alguno de sus múltiples campos, una persona que dedica su vida, sus aficiones, su profesión a la seguridad informática, es un científico de la seguridad informática que no cesa en su empeño en investigar con el objetivo de encontrar las múltiples vulnerabilidades que nos regalan los sistemas operativos de nuestros ordenadores o programas más utilizados por los usuarios informáticos.

Estas personas, a las que vilipendiamos asiduamente en los medios o en nuestras conversaciones cada vez que los aludimos, son ciertamente los responsables de los mayores avances tecnológicos de los últimos tiempos, incluso podemos en-

contrarlos como investigadores en cuerpos policiales, o como profesores de las más prestigiosas universidades del mundo, y en entre ellas incluimos las españolas.

Los *hackers* son responsables del nacimiento de Internet, y del progreso tecnológico, son responsables de la securización de una central nuclear, de un banco, de un hospital o de una planta potabilizadora de agua.

Hackers, a los que yo denomino ***GRANDES (ellos se reconocerán),*** luchan contra la pornografía infantil y la pederastia en la Red, además de colaborar con las Fuerzas y Cuerpos de Seguridad del Estado, y con policías de otros países, creando herramientas para detectar a estos ciberdepredadores en la Red.

Los *hackers* investigan para encontrar los fallos de seguridad en los distintos sistemas informáticos, con el fin de evitar que sean atacados por los verdaderos ciberdelincuentes, los "piratas informáticos", los *crackers…*

Como se puede observar en los pocos ejemplos que he detallado, en ninguno se ha descrito al *hacker* como responsable de actividades delictivas, sino todo lo contrario, os he presentado a este "protagonista" de Internet como el responsable de este nuevo "mundo tecnológico" cada vez más necesario y más presente en nuestras vidas.

Existen muchas clasificaciones para definir el mundo del *hacking* que catalogan a los *hackers* dependiendo de su "finalidad", pero la más conocida y utilizada suele ser:

- ***Hacker, White Hat* o Sombrero Blanco:** son aquellos que utilizan su conocimiento para el bien, para mejorar los sistemas de seguridad, *hardware, software,* etc.

- ***Cracker, Black Hat* o Sombrero Negro:** son aquellos que utilizan su conocimiento para aprovechar de los errores de los sistemas para destruirlos, robar información, programación de virus, troyanos y todo tipo de actividad delictiva en la Red, en beneficio propio, de terceros o simplemente por dar-

le publicidad al hecho de hacerlo. Responsables del falso estereotipo atribuido a los *hackers*, por lo que no deberían ser considerados como tal.

- ***Grey Hat* o Sombrero Gris:** se emplea para referirse a aquellos *hackers* que ocasionalmente traspasan los límites entre ambas categorías.

- ***Lammer:*** se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender. Un *hacker* sería el opuesto de un *lamer* al tener gran cantidad de conocimientos y no presumir de ello.

Incluso el verbo *hackear* se utiliza de manera incorrecta, siguiendo con mi opinión, no es correcto decir "me *hackearon* el correo", cuando alguien accedió de forma fraudulenta a nuestro correo o nos robó las credenciales, en vez de "me *crackearon* el correo" dicen "han *hackeado*"…

Sinceramente, lo que aquí he intentado trasladar es algo mucho más complejo y largo de explicar y entrar en tecnicismos y complejidades no es la finalidad de este libro. Simplemente quiero transmitiros ciertos conceptos, los que yo tengo sobre estos "personajes" a los que tanto maltratamos pero que tanto hacen por nosotros, incluso desde su anonimato, y me gustaría haber contribuido a que al menos los lectores de este libro, si es que existe alguno, utilicen correctamente el término *hacker* y no los confundan con los "otros" que ni se merecen ostentar el calificativo de *hacker*.

A lo mejor alguno pensáis que escribo estas opiniones porque soy uno de ellos, porque soy un *hacker*, siento el deciros que os confundís al pensar que soy un *hacker*, aunque **¡ya me gustaría ser GRANDE!**

Si pones un *hacker* en tu vida, solo tendrás que decirle… **"Securízame"** y estoy seguro de que tendrás junto con la **Seguridad por Defecto (sbD),** un plus más en seguridad y lo que ello conlleva. La mal llamada **Seguridad del Mal,** fluye en una línea muy **delgada,** te protegerá con sus conocimientos, te sentirás seguro como un **Jabalí,** aquí y en **Tr1ana,** y podrás mantener, siempre a salvo, tu más de **1Gbdeinfo,** aún teniendo un **Snifer** o una **Conexión Inversa.** Sí, sé que este párrafo os resultará muy raro, y sin sentido, pensaréis que o **mi Equipo está Loco,** o que soy un ***Informático en el lado del Mal*** *(aunque una vez me llamaron* hacker, *¡y lloré! ¡Ojalá me dije!),* pero no es así, todo esto tiene sentido, y mucho, al final del artículo lo entenderéis, os dejo un **Av4t4r** de lo que os quiero explicar.

¿Que no sabéis dónde encontrarlos? Tenéis que mirar bien a vuestro alrededor, están en la sombra de la Red, pueden ser cualquiera, vuestro amigo, vuestro padre

o vuestro hijo (un ***cómplice de la Red***), aunque a veces, salen de sus guaridas y se reúnen, *como los humanos.* ¡A mí no se me escapan!, porque *¿sabéis quién soy yo, verdad?,* conozco sus secretos, sé que en otoño se reúnen en la Ciudad Condal en una especie de cónclave que ni le ponen nombre, ***"No Con Nombre",*** podéis acercaros y preguntar por **el hijo del GRAN Comandante.** Después, cuando llega la primavera, salen de su letargo y se reúnen en ***Madrí,*** donde vive la ***Keka,*** en una especie consejo de ancianos muy **"Arraigado Con"** su cultura en la que imparten doctrina y conocimientos a los que elijen el camino de la Grandeza, **capitaneados por un pato que lucha por limpiar la Red de maldades,** y me consta.

¡Va por vosotros!, los Grandes ejemplos a seguir.

Y muchísimos otros más…

A continuación os relato una "crónica", un "hecho real", una de las muchas "experiencias" que he tenido con estos "ciberdelincuentes" y que publiqué en *El Blog de Angelucho.*

Diario de Angelucho: *hackers* al descubierto

Os voy a contar una historia, algo que sucedió recientemente y que quiero compartir con vosotros. **Una historia contada en tono de humor,** espero que nadie se moleste, y con la que quiero concienciaros sobre ciertos conceptos erróneos que tenemos de alguna comunidad.

No voy a citar nombres ni *nicks,* por dos motivos, el primero por miedo a olvidarme de alguno, que seguro que me pasará puesto que no tuve la oportunidad de poder hablar y conocer a todos con los que compartí esta vivencia, y el segundo porque me han dicho que Internet es como las Vegas, y lo que subes a Internet queda en Internet, o sea por privacidad.

El caso es el siguiente…

Recientemente, en una ponencia a la que asistí sobre seguridad informática en una universidad, uno de los ponentes, profesor universitario, terminaba su ponencia con la imagen que antecede a este párrafo. ¡Madre del amor hermoso! ¿Qué me cuentan?

Poco después, un buen amigo me envió un *e-mail* personal, muy personal, en el que me expresaba muchas cosas que no voy a desvelar, pero en esencia terminaba diciéndome, ***¡el muy canalla!,*** que **yo era un *"hacker",*** pero es que además fundamentaba la calificación hacía mí de forma muy detallada, vamos que me lo llamó sin tapujos y por distintas razones. Me describía el sentido de *hacker* que tiene la gente como **"… una especie muy solitaria, que no tiene amigos, con granos en la frente, antisociales... pero no, no es así…"** y me explicaba el porqué.

Yo, como siempre me documento, busqué en "el Internet que tengo grabado en mi casa", pregunté al "oráculo" Google para que me desvele lo que es un *hacker*.

En una de las entradas de respuesta leo **"en la actualidad, el término *hacker,* se usa de forma corriente para referirse mayormente a los criminales informáticos".**

¿Yo, un delincuente? ¿En qué me estoy convirtiendo? ¡El término *hacker* me perseguía y me asustaba!

Algún día después me invitan a una "fiesta *hacker*", una reunión de "delincuentes informáticos" donde se reuniría la *"crème de la crème"* de ese mundo ***"underground".***

La fiesta se celebraba en honor a un "delincuente" que dejaba nuestro país y se marchaba a delinquir a muchos kilómetros de España, sería vecino del mismo Michael Dundee *"Cocodrilo Dundee".*

La verdad que "la ocasión pintaba calva" para conocer a estos personajes oscuros de la Red, tan escurridizos y que tan mala fama tienen para la mayoría de los mortales. No me lo pensé dos veces y asistí a la fiesta. ¡Total, yo era uno de ellos!

El primer problema surgió cuando llegué al lugar de la reunión, era un lugar público, un bar lleno de gente, ¡algo estaba fallando!, en ese entorno no podría dar lugar una reunión de esa índole. El siguiente problema fue que en la barra de ese bar, y nada más llegar, **reconocí a dos personas, y además GRANDES personas humanas.** Uno de ellos había sido profesor mío en algún curso de informática forense, además de los buenos, y que me había ayudado con algún problemilla técnico en mi día a día profesional, me recibió con un fuerte abrazo. El otro un referente en el mundo de la seguridad informática, ponente en los más prestigiosos eventos, con el que había coincidido en algún curso y quien me animó a continuar con este blog, un tío GRANDE y estrenando empresa con la que le auguro mucha suerte en el mundo de la seguridad informática.

Con ellos se encontraban dos promesas de la seguridad informática, que acababan de organizar, desde sus blogs, un concurso en el que se premiaría un trabajo. Este trabajo sería una guía para que cualquier persona, sin ningún tipo de conocimiento pudiera instalar un sistema operativo en su ordenador, siguiendo el criterio de compartir información y educar, para evitar los problemas que nos encontramos diariamente en la Red, aprendiendo a evitarlos o mitigarlos.

Poco después se presentó otro **GRANDE** de la seguridad informática, otro que me había deleitado, enseñado y divertido en las numerosas ponencias y cursos suyos a los que yo había asistido. Una persona que ostenta el **MostValuable Professional (MVP)** por **Microsoft** en el área de Enterprise Security, una distinción que tienen muy pocos informáticos en el mundo. Nos comentaba, durante la primera

cerveza, su discurso improvisado en su nombramiento como embajador de una universidad española.

Mientras nos contaba la anécdota de su discurso se presentó otra persona, amigo de éstos, **otro GRANDE de la seguridad informática,** y que había quedado con ellos para despedirse puesto que se iba a probar fortuna profesional a Australia como responsable de seguridad de una importante empresa en el país de los canguros.

¡Qué fastidio! Para una vez que voy a una reunión clandestina de delincuentes informáticos me encuentro, por casualidad, con verdaderos científicos de la seguridad informática. **Así, estando con esta gente, no voy a tener la oportunidad de conocer a esos "delincuentes" de los que tanto he oído hablar.**

Me voy fuera, a la terraza del bar, seguro que es donde voy a encontrar a mis ***targets***[28], casualidades de la vida, nada más salir me encuentro con **otro GRANDE acompañado de su esposa,** a ambos los conocí en el último Security Blogger Summit en Madrid, un tipo autodidacta como él mismo reconoce en algún artículo que he leído sobre él: "Siempre he sido autodidacta. El secreto está en cuestionarte todo... ¿Cómo o por qué funciona tal cosa? ¿Qué ocurre si modifico...? ¿Cómo se podría mejorar...? Lo podría resumir en tres palabras: 'leer', 'cacharrear' y 'tiempo'". Un tipo que hoy en día se encuentra en el *ranking* de GRANDE entre los grandes y participante de los retos de seguridad informática más prestigiosos.

Pues parece ser que no voy a tener suerte, me voy a quedar sin conocer a esos delincuentes, porque ahora veo que llega **otro GRANDE, otro gran referente dentro de la seguridad informática, una persona a la que llevo leyendo desde hace tiempo, de quien he aprendido el significado de virus, antivirus y heurísticas, entre muchas otras cosas,** del que he aprendido que informando se puede evitar muchos problemas en la Red a otras personas menos "preparadas" técnicamente, el único que levantó la mano en un congreso a la pregunta de ¿quién se siente seguro en Internet? por parte de un ponente.

Como el objetivo de mi visita a ese bar estaba claro que no iba a hacerse realidad, decidí quedarme con estas personas con quienes el azar había hecho que coincidiera. Hablando con mi profe, el de Triana, o mejor dicho escuchando alguno de sus chistes, se nos acercó una persona que no conocía, un amigo del sevillano. ¿Os imagináis a que se dedica? Efectivamente, a la seguridad informática, con su empresa en Galicia, tentado por dejar el país como tantos profesionales que se

[28] ***Target:*** Término del inglés, significa 'objetivo'. *Ejemplo:* "El *target* de este libro son usuarios sin conocimientos técnicos".

han marchado de España a buscar fortuna en otros lugares, como el de los canguros.

Este GRANDE, y gallego de pro, rápido empezó a transmitirme su interés por luchar contra lacras como la pedofilia en la Red, su interés en colaborar altruistamente en la lucha contra los ciberdepredadores, me contaba sus logros en la creación de herramientas para geolocalizar conexiones de estos "elementos". Un verdadero cerebro.

Otro GRANDE se acerca a nosotros, grande también de altura, otra persona que también conocí en un evento de seguridad, a quien también he seguido en la Red por sus interesantes aportes. **Otro grande que me animó a continuar con este blog y que me anunció, para desgracia nuestra, que también abandonaría próximamente nuestro país** para gestionar la seguridad informática de una conocidísima empresa multinacional de telefonía. ¡Otro cerebro que nos deja!

Cuando daba por perdida la noche en mi búsqueda de delincuentes informáticos, aparece **otro GRANDE, acompañado de su pareja (que es la que realmente manda).** Este GRANDE pertenece al **CoreTeam** de uno de los mayores congresos de seguridad informática en Madrid y en España, como responsable y organizador al mejor estilo americano de un congreso tipo DEFCON (LA CONFERENCIA *HACKER* MÁS GRANDE DEL MUNDO), con el propósito de **promover el intercambio de conocimiento entre los miembros de la comunidad de seguridad informática.**

Bueno, pues parece que al final tendría suerte, si este GRANDE organiza este tipo de eventos, **seguro que algún *hacker* de esos se acerca, por supuesto, yo estaría "ojo avizor" para poder identificarlos.**

Al poco de comenzar la conversación con esta persona y comentar lo cortos que se nos hacen los días con nuestros trabajos, vidas sociales y familiares, me comenta que **además de todo lo que hace se dedica a luchar de forma personal y particular contra los peligros de los menores en la Red, pornografía infantil y todo lo relativo a lo que de forma directa o indirectamente afecta a los críos en la Red.** No tardaron en aparecer propuestas de colaboración en esta lucha de la que ambos compartíamos puntos de vista en cuanto a nuestro aporte a la sociedad para poder ayudar a mitigar estos problemas y sobre todo a cambiar ciertos conceptos.

Durante nuestra conversación se unió a nosotros la persona que se iba con los canguros, me lo volvieron a presentar, "mira éste es por el que se ha organizado todo esto, es un *hacker* y nos deja para irse a Australia a trabajar en seguridad informática".

Ahora lo entendía todo, no había ninguna casualidad, desde el primer momento estuve con ellos, eran ellos los *hackers.* Los científicos de la seguridad

informática que con su trabajo y esfuerzo ayudan a todos a que tengamos una vida digital más segura y ayudan en la lucha de las lacras sociales que proliferan en la Red.

Me dejo en el tintero a muchos que asistieron a la "fiesta *hacker*", pero como suele pasar en las grandes reuniones, no todo el mundo tiene la oportunidad de conocerse pero oportunidades tendremos.

Terminamos nuestra "reunión" pasadas las cuatro de la mañana, hablamos de todo y de las grandes cosas que se tienen que hacer todavía en este país por la seguridad informática, pero **lo peor de todo, me fui sin ver ningún "delincuente informático", ahora *hackers… Hackers* vi unos cuantos.**

Solo me queda deciros…

"*HAPPY HACKING…* y cuidadín (por el buen camino)."

7. ENTREVISTAS

EXPERTO EN SEGURIDAD EN INTERNET

Hace un tiempo conocí, en un evento de seguridad en Internet, a un GRANDE en el panorama de la seguridad informática de nuestro país. Una persona que me hizo ver de otra forma la seguridad en Internet. Hablo de Yago Jesús.

En ese congreso Yago estaba como público junto con al menos doscientas personas más, la mayoría también expertos en seguridad, en un momento dado uno de los ponentes lanzó una pregunta al "respetable": ¿Quién de los presentes se sentía seguro en Internet?

Solo una persona levantó la mano. ¿Adiviná is quién? Efectivamente, **Yago Jesús.**

Como presentación de este GRANDE, decir que es uno de los editores y responsables, junto con otros **GRANDES (Lorenzo Martínez, Alejandro Ramos y José A. Guasch),** de uno de los blogs de referencia sobre seguridad informática en lengua española, *Security By Default,* precisamente en el evento participaba, en la mesa

redonda, el amigo Lorenzo Martínez junto con miembros de las Fuerzas y Cuerpos de Seguridad del Estado, abogados y otros especialistas en seguridad.

Gracias a ellos y a gente como ellos aprendí el verdadero concepto de seguridad en Internet, aprendí el verdadero concepto del *hacking*, y por ello espero que cada vez que me dirijo a los *hackers* como GRANDES se sienta identificado, al igual que todos sus compañeros de bien pertenecientes al mismo "gremio".

He leído a Yago y escuchado en infinidad de entrevistas y conferencias, sobre todo en temas relativos a virus, antivirus y *malware,* y por ello es uno de los responsables de que *El blog de Angelucho* exista, porque muchas de las entradas y artículos del blog y de este libro no son otra cosa que meras traducciones de sus propios artículos, conferencias y por supuesto enseñanzas.

Sé a ciencia cierta que Yago se ha prestado a infinidad de entrevistas cuya temática principal es la seguridad, pero en esta ocasión le he pedido el favor de hablar de seguridad en "cristiano" para que me pueda enterar "hasta yo".

- ¿Qué es para ti Internet?

Opino que Internet es un nuevo paradigma, he leído a mucha gente compararlo con la invención de la imprenta, y creo que me adhiero a esa opinión.

Internet lo ha cambiado absolutamente todo. De hecho, creo que todo invento que aspire a ser revolucionario ha de hacer que pienses ¿cómo hubiera sido mi vida si hubiese tenido esto antes? Y creo que Internet cumple al 100% con eso.

Uno lo piensa, trata de extrapolar el concepto Internet a la época en la que no existía y piensa ¡uff, si hubiera tenido esto!

- ¿Es posible hablar de seguridad y de Internet sin tecnicismos?

Claro que sí, siempre hay niveles. Por ejemplo, si me tocase leer un tratado de genética estoy seguro que no podría comprender ni un 5%.

Sin embargo, uno lee a Mendel y sus guisantes y los conceptos generales quedan bastante bien explicados.

- ¿Cómo llegaste al mundo de la seguridad informática?

Siempre he tenido inquietud por la informática, en mi casa mi padre fue pionero en ese mundo y desde que era pequeño siempre hubo un Mac (de los de antes, los pequeños con mini-pantalla) en casa.

Luego llegó el PC y con él, un módem para conectarse a IBERTEXT (precursora de Internet en España) eso me fascinó, lo de estar sentado frente a una pantalla y comunicarme con un montón de gente a la vez

que leían lo que escribía, era algo cautivador (las facturas de teléfono, no tanto...).

De ahí di el salto a Internet y dado que me había "movido" tanto previamente, eso de quedarme en un usuario normal no iba conmigo. Así que empecé a investigar, con aquellas páginas web *under* de Isla Tortuga, ciertos canales de irc... Hice amigos, y sobre todo gente de la que pude aprender mucho, creo que ese es el principal activo de cualquier persona: tener cerca gente que sepa más que tú.

- ¿Eres *hacker*?

En algún *ezine* o web de los 90 leí algo como "tú no puedes autodefinirte como *hacker*, te lo tienen que llamar".

Así que, supongo que compete a otros responder esa pregunta

- Antes de entrar en materia, define *hacker:* ¿héroe o villano?

Yo creo que esas cuestiones semánticas deben ser superadas cuanto antes. Está claro que el término ha mutado, no tiene el significado original, se ha vuelto demasiado comercial: "*hacking* ético", "*hackers* malos", "un *hacker* ha roto ...".

Me quedo con la parte de persona ingeniosa capaz de superar obstáculos, y en esa categoría encajo no solo a personas relacionadas con la informática. En general se puede ser *"hacker"* en todos los aspectos de la vida.

- Desde el punto de vista de un experto en seguridad, ¿cuáles son los principales peligros a los que nos enfrentamos los internautas "base"?

Pese a que mucha gente se siente tentada en generalizar y divagar respuestas, yo creo que no existen las generalidades.

La respuesta tiene que ir en función de tu perfil. No es lo mismo lo que te puede suceder si tienes quince años y estás todo el día en el MSN/Tuenti, que si tienes cincuenta y haces operaciones bancarias e incluso "juegas" en bolsa.

No obstante, sí que existe un axioma que se cumple siempre: a menor sentido común → mayor riesgo.

Para un adolescente el peligro puede estar en la sobre-exposición en redes sociales o acciones de compañeros/as orientadas a su hundimiento social.

Para una persona de un perfil más "señor", sin duda verse envuelto en alguna página-timo que a base de advertencias falsas les cuele algún troyano bancario en forma de supuesto antivirus.

- ¿Crees que es posible el binomio Internet y seguridad en los hogares españoles?

Creo que se puede alcanzar un porcentaje alto de seguridad, pero no existen las estadísticas del tipo "100%".

No creo que existan fórmulas mágicas. Siempre habrá delincuencia en Internet o gente con el suficiente tiempo libre como para hacer daño, y por ende, siempre habrá víctimas.

- Los "agujeros" de seguridad en la Red, en los niveles de usuario básico, ¿crees que pueden ser tapados?

Siempre hay que utilizar el principio del mínimo privilegio. Si tuviera que explicarle el concepto a una señora de sesenta años, le diría que se imaginase en el supermercado, a punto de coger un carro. Ese carro acepta monedas de cincuenta céntimos o un euro para ser desbloqueado.

Aplicar el principio del mínimo privilegio sería el optar por la moneda de cincuenta céntimos frente a insertar un euro, de esa forma, si la moneda se pierde o te olvidas de cogerla, la pérdida es menor.

Y este principio tan ajeno a la informática es 100% extrapolable al mundo virtual.

Si vas a comprar por Internet, hazlo desde una tarjeta de crédito SOLO para ese menester, con un límite bajo. Si vas a usar Windows, usa siempre cuentas no privilegiadas de usuario normal, nunca cuentas administrativas.

De esa forma estás limitando el riesgo y haciendo que un incidente tenga consecuencias menores.

- ¿Estamos preparados los internautas españoles para navegar seguros?

Claro que sí, todo es cuestión de voluntad, de tener ganas de aprender y aceptar las reglas del juego.

- Niños e Internet ¿están seguros? ¿Qué consejos les darías? ¿Y a sus padres?

Personalmente creo que el control parental es la mejor herramienta, por mucho que se venda eso de "tener derecho a la privacidad", estimo que unos buenos padres no deben quitar el ojo a su hijo. Y si eso significa "violar" su privacidad, bien hecho está.

- En líneas generales, ¿qué consejos darías X1Red+Segura?

Cautela, mesura y ante la duda: preguntar, siempre preguntar. Hay muchos y muy buenos foros en Internet donde la gente está dispuesta a echar una mano.

- Yago, ¿te sientes seguro en Internet?

Tomando como ejemplo los coches y la carretera, yo me siento seguro cuando conduzco, pero me siento así principalmente porque, pese a que me han "dicho" la cantidad de adelantos en seguridad que tiene mi coche (ABS, ESP, etc., etc.), yo entiendo que, una curva señalizada a ochenta, no la voy a poder tomar a doscientos, principalmente porque comprendo que la carretera es en sí un medio hostil y el vehículo en el que viajo no deja de ser un montón de hierro incapaz de aguantar un impacto (con seguridad) a más de 30km/h.

Internet es igual, puedes estar seguro en él, pero eso implica que debes conocer los riesgos y limitaciones.

¡Interesante el último párrafo de la entrevista! ¿Verdad?

HACKERS VS CIBERDEPREDADORES

Otra persona que tiene que tener presencia en este libro, sin ningún lugar a duda, es Juan Antonio Calles.

Juan Antonio es consultor senior en Seguridad de la Información en el Centro Hacking de Everis, Ingeniero en Informática de Sistemas, Postgrado en Tecnologías de la Información y Sistemas Informáticos y Postgrado en Ingeniería de Sistemas de Decisión.

Además, este peligroso *"hacker"* es el responsable, junto con Pablo González, de Flu Project, un proyecto que nació con el objetivo de enseñar y concienciar a los usuarios sobre los problemas producidos por el *malware* y para colaborar en los procesos de auditoría de seguridad de la información y el *hacking* ético.

Estos GRANDES, con su proyecto, se dedican a combatir la pedofilia y pederastia en la Red, con el desarrollo de una de sus herramientas orientada a la obtención de información de estos criminales, permitiendo identificarles e incriminarles por los delitos cometidos. Expusieron su colaboración, bajo el título **Técnicas oscuras para combatir la pederastia en Internet** en congresos como la No cON Name (NcN, es uno de los GRANDES congresos de seguridad informática y *hacking* más importante en España).

Esta estrecha colaboración la realizan con Anti-Depredadores.org, proyecto colombiano colaborativo y sin ánimo de lucro de la Corporación HackLab que apoya técnicamente a instituciones gubernamentales de cualquier país en la identificación y rastreo de predadores (pedófilos), que ponen en riesgo la integridad y seguridad de los menores y jóvenes en Internet.

Con el amigo "Juanan" he compartido largas charlas en las que hemos intercambiado ideas y opiniones de cómo luchar contra los ciberdepredadores y sobre todo, de cómo poder concienciar sobre el problema. Tal vez en alguna ocasión, no muy lejana, surja una colaboración real ;-)

Para esta entrevista, con el permiso del entrevistado, voy a realizar mi trabajo lo mejor posible y para ello voy a continuar con el espíritu del libro y os intentaré traducir las ideas o conceptos más técnicos que Juan Antonio nos transmite en su mensaje.

- ¿Flu Project es…? ¿Cómo, cuándo, motivaciones?

Flu Project es un proyecto que nació de una idea. Allá por el verano de 2009, Pablo me propuso desarrollar un **troyano**[29] educativo, para contarlo en los cursos y charlas que impartimos y por el mero hecho de aprender algo nuevo, ya que hasta el momento el ***malware***[30] era una rama de la seguridad que no habíamos tocado mucho. Tuvimos un año complicado de trabajo y hasta el verano de 2010 no llevamos a cabo la idea. El núcleo de **Flu**[31] lo desarrollamos realmente en dos tardes, y la primera versión estable en una semana. Decidimos hacerlo en **.Net**[32] y **PHP**[33] ya que eran lenguajes que todo el mundo iba a entender fácilmente, por su fin educativo (actualmente tenemos una versión en **C**[34] bastante potente que quizás liberemos algún día, aunque por el momento la versión oficial seguirá siendo la actual). Era un troyano verde aún (y todavía no teníamos el logotipo ☺) y se nos ocurrió montar una

[29] **Troyano.** En informática, se denomina **troyano** o **caballo de Troya** a un *software* malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños. Todo en clara alusión al histórico Caballo de Troya.

[30] ***Malware:*** *Software* malicioso con el objetivo de dañar el equipo informático.

[31] **Flu** es el nombre que recibe el troyano desarrollado por la Comunidad Flu Project.

[32] **.Net** es un *software* que aporta soluciones para el desarrollo de aplicaciones.

[33] **PHP** es un lenguaje de programación.

[34] **C** es un lenguaje de programación.

comunidad *online* para desarrollarlo con otras personas que estuviesen interesadas. Así surgió Flu Project en Diciembre de 2010. Durante el primer mes de vida ya se fueron definiendo el resto de cosas que componen Flu Project, como su blog, que hasta el momento es lo más valorado por la gente, el desarrollo de otras herramientas cómo Flunym0us, FluBlocker, Liberad a Wifi y otros proyectos que iremos presentando próximamente, nuestros foros, los retos *hacking*, las secciones de utilidades, libros, etc.

A las pocas semanas de lanzar la comunidad Flu Project en la Red, contactó conmigo David Moreno, de la Asociación Anti-Depredadores, para una colaboración con el desarrollo de **Flu-AD**[35], una versión especial de Flu orientada a perseguir casos de *cibergrooming* en Colombia. Y no pudimos rechazarla, desde pequeño por temas familiares siempre he estado muy ligado a asociaciones sin ánimo de lucro y la verdad que nos pareció tanto a Pablo como a mí una manera genial de poder colaborar con nuestros conocimientos en la materia y hacer algo por la causa. En la actualidad seguimos colaborando con ellos, la verdad que hacen un trabajo excepcional y digno de admirar y el apoyo que les damos es incluso poco en muchas ocasiones, así que aprovecho para hacer un llamamiento a todos los que quieran colaborar en la causa: http://www.anti-depredadores.com/. Y de esa primera colaboración han ido surgiendo varias nuevas con otras asociaciones y cuerpos policiales. ¿Qué te voy a contar que no sepas? ☺

- *Hackers,* ¿héroes o villanos?

Desde mi punto de vista ni héroes, ni villanos. El término *hacker* se ha devaluado mucho en los últimos años. Por desgracia, es habitual que salgan en telediarios y periódicos noticias que ponen el término *hacker* para contar un caso, cuando en realidad quieren decir delincuente. Además, en los últimos años ha sido habitual que saliesen muchas noticias de casos como los de **Anonymous**[36], **Wikileaks**[37] o Kim

[35] **Flu-AD** es la versión del troyano Flu específica para Antidepredadores.org.

[36] **Anonymous** es un seudónimo utilizado mundialmente por diferentes grupos e individuos para (poniéndose o no de acuerdo con otros) realizar en su nombre acciones o publicaciones individuales o concertadas a través de Internet.

[37] **Wikileaks** es una organización mediática internacional sin ánimo de lucro que publicaba a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.

"Dotcom"[38], y los periodistas han tenido muchas oportunidades para utilizar ese término que tanto les gusta estropear.

Un *hacker* no es ni más ni menos que un especialista en seguridad de la información, un investigador como el de otras ramas. Por ello existe la coletilla "ético" en la expresión "*hacker* ético", para definir el tipo de *hacker* que se es, un investigador con fines considerados éticos o un investigador con fines maliciosos.

- ¿Sois/eres *hackers*?

Cuando me preguntan a qué me dedico, antes solía decir "informático" a secas, pero me cansé de arreglar ordenadores de amigos y familiares ☺. Luego decía que me dedicaba a temas de *hacking* ético, y comenzaron a pedirme que "piratease" cuentas de MSN entre otras cosas. Ahora prefiero definirme como auditor de seguridad, así evitamos problemas :P

Contestando a la pregunta, yo creo que todos los que nos dedicamos al mundo de la seguridad tenemos alma *hacker*, nos gusta trastear, ir más allá de lo que ven los ojos y eliminar esa magia por la que parece que funcionan las cosas a veces. Todos somos un poco *hackers* ☺

- ¿Qué es para ti Internet?

Es más fácil definir qué no es Internet, que definir qué es. Internet ha sido el sistema que ha revolucionado el mundo de las comunicaciones. Para no extenderme mucho daré tres aspectos que me han parecido claves de la aparición de Internet. En primer lugar ha sido un soplo de aire fresco para la empresa tradicional, que le ha permitido llegar a clientes de una manera económica y que se encontraban a mucha distancia. Antes si tenías una pequeña empresa de chapuzas de albañilería, fontanería, etc. te dabas a conocer por el boca a boca, anuncios en guías o carteles por la calle, ahora tienes tu página web y es fácil darte a conocer en el mercado. Ello ha hecho que haya mucha más competencia y por tanto una carrera por el **SEO**[39] abismal por tener su web en los primeros resultados de Google. En segundo lugar ha sido una manera de evitar los aislamientos comunicativos con el resto del mundo que tenían ciertos países (los que tenían la suerte de tener

[38] **Kim "Dotcom".** Fundador de Megaupload, sitio web de servicio de alojamiento de archivos, fundado el 21 de marzo de 2005 por Megaupload Limited en Hong Kong. El 19 de enero de 2012 fue cerrado por el FBI por supuesta infracción de derechos de autor.

[39] **SEO.** Posicionamiento en buscadores (en inglés: *Search Engine Optimization*).

acceso a Internet), y redes sociales como Twitter han ayudado a que la población se una en una única voz, aunque por desgracia en los últimos años se ha convertido en un gran arma política, y son muchos los países que están montando "grandes ***firewalls***[40]" por los que canalizan las comunicaciones de sus ciudadanos, que contratan ***botnets***[41] para realizar **DDoS**[42] a otros gobiernos o que intentan controlar sistemas rivales con software malicioso. Sin duda Internet ha sido la revolución del siglo XXI tanto para lo bueno como para lo malo.

- Desde el punto de vista de un experto en seguridad, ¿cuáles son los principales peligros a los que nos enfrentamos los internautas "base"?

Creo que un ejemplo será la mejor manera de explicarlo. Tengo un familiar muy cercano con pocos conocimientos en informática y una base de Internet, pero que le gusta mucho navegar, chatear, etc., como a cualquier persona, vamos, y de vez en cuando voy a revisarle el ordenador. Cada mes que voy, me encuentro que tiene tres o cuatro barras instaladas en el navegador (babylon, etc. ya sabéis), tiene dos o tres iconos con accesos directos a páginas de todos los colores, el antivirus desactualizado, las actualizaciones de Windows esperando, servicios sospechosos corriendo en la máquina, ciertas ralentizaciones temporales, páginas de inicio en los navegadores que simulan ser de Google plagadas de anuncios, ***plugins***[43] extraños en los navegadores que muestran anuncios por pantalla, algún que otro *spyware,* troyanos… vamos, que se ve las ofertas del mercado con solo iniciar Windows ☺. La verdad que siempre que lo veo no sé si meterle un formateo y aplicar fuero purificador o remangarme, sacar el **Encase**[44] y ponerme un buen copazo…

El mayor peligro de los usuarios base es precisamente la falta de una base que les forme en lo que se puede hacer, y lo que se debe hacer en

[40] Un cortafuegos (***firewall*** en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado.

[41] ***Botnet*** es un término que hace referencia a un conjunto de robots informáticos o *bots,* que se ejecutan de manera autónoma y automática.

[42] **Ataque de denegación de servicios,** también llamado ataque **DDoS** (de las siglas en inglés: *Denial of Service),* es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima debido a la sobrecarga.

[43] ***Plugins*** son complementos de los navegadores.

[44] **Encase** es un programa muy utilizado en informática para el análisis forense.

Internet. Mi madre cuando comenzó en Internet me llamaba diciendo cosas cómo que le había tocado un coche por ser la usuaria 1.000.000, tras unas pocas clases ya navega tranquilamente por la Red y sabe dónde se puede clicar y dónde no. Cosas que a nosotros nos pueden parecer lógicas, como mirar si un *link* se dirige a donde indica el texto, para evitar tragarnos un ***phishing***[45], a ellos, que no saben **HTML**[46], ni cómo funcionan las cosas internamente les cuesta bastante más y hay que tener paciencia a la hora de enseñarles. Creo que haría falta en los colegios una asignatura que tratase sobre seguridad en Internet. Ahorraríamos muchos disgustos.

- ¿Y los menores? ¿A qué peligros se enfrentan?

Los menores por desgracia se encuentran bastante indefensos en las redes. Aún les falta cierta madurez que les permita discernir entre situaciones que pueden ser peligrosas y acceden a ciertos contenidos con la falsa seguridad de estar sentados tranquilamente en su habitación tras un PC. Por ello siempre recomiendo a los padres colocar el PC en el salón o en zonas de paso donde puedan echar un vistazo a lo que hacen los menores, al menos hasta que tenga la edad suficiente para comprender lo que ve y los peligros que esa responsabilidad conlleva.

Cuando era pequeño y no teníamos Internet mi madre me decía siempre "si te dicen algo por la calle no te pares", "no cojas caramelos de extraños en el parque" y un largo etc.; siempre he tenido una madre protectora ☺. Simplemente hay que aplicar los consejos de siempre a Internet, aunque ahora cambian los caramelos por fotos y el parque por un chat.

- ¿Cómo piensas que podrían paliarse estos peligros?

Concienciación, formación desde pequeños en seguridad de Internet (al igual que debería haber una clase de seguridad vial) y sobretodo endureciendo las penas en España para los casos de *cibergrooming, ciberbullying,* pedofilia…. Durante la NcN del 2011 Pablo y yo hablamos largo y tendido sobre la comparativa del Código Penal español y el colombiano, y se vio cómo hace falta aplicar urgentemente unas medidas más agresivas para evitar que los delincuentes reincidan.

[45] ***Phishing.*** *(Ver artículo específico en el libro: Capítulo III. Amenazas en la Red, punto 5.)*

[46] **HTML.** Lenguaje informático para la elaboración de páginas web.

- Flu Project *vs* ciberdepredadores, ¿nos explicas cómo?

Flu Project no se dedica a la caza de ciberdepredadores, al menos directamente. Nosotros únicamente desarrollamos herramientas que pueden ser de utilidad a los cuerpos policiales en ciertos casos determinados y les ofrecemos nuestros conocimientos técnicos en caso de que les sean necesarios. Son los cuerpos policiales los que realizan todo el trabajo, el esfuerzo y los que sufren realmente cada batalla que se encuentran diariamente. Tengo amigos de varios cuerpos policiales, tanto en España como en América Latina y la verdad que me cuentan que lo pasan mal cada vez que se encuentran casos de abuso a menores o pornografía infantil. Hay que estar muy preparado para llevar este tipo de casos y ellos tienen ayuda psicológica y legal. El problema es que a veces no suelen tener los recursos técnicos necesarios para la ejecución de los casos y cuando no la tienen es cuando suelen contactarnos. Un sistema de monitorización de redes, localización de IP, e incluso si la ley se lo permite, *kits* de explotación de vulnerabilidades o troyanos, pueden ser clave para cazar a un depredador.

- Queda claro que es mucho el trabajo que realizáis luchando contra esas lacras, ¿es buena la compensación económica?

Pues la compensación económica suele ser cero, porque son colaboraciones sin ánimo de lucro, pero la compensación de saber que has hecho algo por alguien, y has logrado brindar las herramientas a los cuerpos policiales para que una persona deje de sufrir no tiene precio.

- Sois *hackers* y no delinquís, estáis en lucha contra los peligros de la Red de forma altruista ¿sabes que estás rompiendo un mito?

Sí, lo estamos rompiendo y sirve para concienciar a cierta gente que ya nombré más arriba, me alegro de romperlo. La verdad que es fácil no delinquir cuando nunca me han ofrecido 10.000€ por una cuenta de Hotmail… es broma, si no viene el Dioni con un furgón no me vendo ;)

- ¿Crees que es posible el binomio Internet y seguridad en los hogares españoles?

Pues como decía un anuncio de una conocida marca deportiva, *"Impossible is nothing"* y la verdad que casi nada es imposible. Pero para ello hay que mostrar cierto interés en que las cosas se hagan como se debe hacer. Si quieres que tu hijo no se meta, aun siendo sin querer, en páginas con contenido no recomendado para menores (ya demostramos en la NcN que buscando "pokemon" en Google y con 3 clics de

ratón accedías a vídeos pornográficos), aplica un control parental en el equipo y obliga a los pequeños que se autentiquen con cuentas poco privilegiadas, instala un buen antivirus, actualízalo regularmente, no instales *software* pirata descargado de sabe dios dónde y lo peor, *crackearlo* con sabe dios que *keygen…* El problema es que ahora los niños saben más que los padres, por ello los padres deben asistir a charlas y formaciones para actualizarse en temas tecnológicos e intentar ir un paso por delante de los hijos.

- En líneas generales, ¿qué consejos darías X1Red+Segura?

En Flu Project, Pablo publicó una ***checklist***[47] con una serie de consejos y buenas prácticas para usuarios base que son muy útiles para conseguir 1Red+Segura, si me permites, te cuelo un ***black seo***[48] con los links a los artículos ☺

http://www.flu-project.com/buenas-practicas-para-usuarios-novatosmedios.html

http://www.flu-project.com/buenas-practicas-para-usuarios-novatosmedios-parte-ii.html

http://www.flu-project.com/buenas-practicas-para-usuarios-novatosmedios-parte-iii.html

http://www.flu-project.com/buenas-practicas-para-usuarios-novatosmedios-parte-iv.html

http://www.flu-project.com/buenas-practicas-para-usuarios-novatosmedios-parte-v.html

- Juanan, ¿te sientes seguro en Internet?

La verdad que yo vivo con el modo paranoico. Cada vez que tengo que entrar al banco *on-line,* tengo una cuenta de usuario poco privilegiada y un navegador con el modo seguro activado. Para el uso normal siempre tengo al menos un antivirus instalado, el *firewall* levantado, el navegador en modo seguro y de vez en cuando miro la tabla **ARP**[49], para ver si me están ***spoofeando***[50]. Nunca utilizo wifis públicas, y en el trabajo evito entrar a sitios personales y, si no tengo más remedio, siempre lo hago bajo una conexión segura por http. Y lo más importan-

[47] ***Checklist*** es un listado.

[48] ***Black seo*** es una lista de *links.*

[49] **Tabla ARP** contiene las direcciones físicas MAC (es un identificador que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física) de cada equipo.

[50] ***Spoofing,*** en términos de seguridad de redes, hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos.

te, no instalo *software* pirata en el equipo, siempre intento usar *software* original o libre descargado de los repositorios oficiales. Tampoco suelo navegar por sitios peligrosos y soy muy restrictivo con las políticas de ***SPAM***[51] del correo, me fio poco de todo. Con todo esto, aún sigo sin sentirme seguro al 100%, pero al menos sé que estoy aplicando las medidas necesarias para vivir las menores situaciones de peligro.

Inmigrante digital adaptándose a las TIC

Una las inmensas bondades que ofrece la Red es algo que ya hemos explicado en este libro, la socialización, el conocer personas, el compartir información y conocimiento.

Este libro está dirigido a los internautas menos técnicos, a los que sufren la conocida "brecha digital" para contrarrestar sus efectos, adaptándose a las nuevas tecnologías.

Y como ejemplo de esta adaptación os presento a una joven internauta sevillana, que además es madre y abuela, merecedora de una mención especial en este libro como ejemplo de adaptación de los "inmigrantes digitales" a las nuevas tecnologías.

Es muy sencillo encontrarla por Twitter ayudando a difundir mensajes solidarios sobre cualquier causa, ***retwitteando***[52] mensajes con ofertas de trabajo, mensajes con alertas o amenazas en la Red, mensajes para la movilización social ante injusticias, en definitiva, colaborando en difundir información y en tener una Red más segura.

Me estoy refiriendo a mi ciberamiga Elena, internauta, usuaria de redes sociales y *twitera,* quien se prestó a una pequeña "entrevista" para explicar su singladura en la Red de redes.

Un ejemplo a seguir.

[51] ***SPAM.*** *(Ver Capítulo III. Amenazas en la Red, punto 3).*

[52] ***Retwittear*** es reenviar un mensaje que se recibe en Twitter a nuestros contactos.

ENTREVISTA A UNA INMIGRANTE DIGITAL

- Elena, ¿qué es para ti Internet?

Información. Distracción. Últimamente también una forma de hacer algo por los demás.

- ¿Cómo conocíste Internet?

Por mis hijos.

- Antes de convertirte en usuari@ de Internet, ¿qué conocimientos previos tenías sobre las Tecnologías de la Información y Comunicación (TIC)?

Ninguna. Aún hoy sé muy poco, entre otras cosas por miedo a meterme en algún sitio no deseable o cargarme el PC.

- ¿Cómo ha sido tu aprendizaje en Internet?

Prácticamente sola, poco a poco y preguntando.

- ¿Qué uso das a la Red?

Sobre todo leo mucho, periódicos, artículos que me envían o ponen en Twitter y un poco de cotilleo.

- ¿Cómo y desde dónde utilizas Internet?

Desde mi casa

- ¿Qué beneficios encuentras en Internet?

Mucha información y buenas personas.

- ¿Consideras que existen peligros en Internet?

Sí.

- ¿Cuáles son los peligros que conoces en la Red?

Pederastia. Estafa y la facilidad para levantar calumnias.

- En caso de encontrarte ante un peligro o amenaza en la Red, ¿cómo reaccionas?

Nunca me he sentido en peligro. Llegado el caso denunciaría.

- Seguridad e Internet ¿Qué opinas?

Pienso que la seguridad en Internet depende de cada uno. En sí misma no considero que la Red sea segura.

- ¿Para ti qué es una red social?

Conocer gente, intercambiar opiniones.

- ¿Qué redes sociales conoces?

Facebook, Tuenti y Twitter.

- ¿Utilizas alguna red social? ¿Qué criterios tienes para aceptar una nueva "amistad"?

Facebook y Twitter. Acepto a gente que conozco por medio de amig@s. A los que llevo viendo tiempo y me gustan sus mensajes etc. Acepto gente que piensa distinto a mí.

- ¿Utilizas Internet como medio de comunicación con tu familia y amigos?

Familia y amigos de fuera de la Red, NO.

- Privacidad y redes sociales (Internet) ¿Qué opinas?

No creo que la Red permita mucha privacidad. Yo no me fío.

- ¿Tienes o has tenido algún menor a cargo y que sea usuario de Internet?

Hasta ahora no. Dentro de poco empezará a entrar mi nieto.

- ¿Cómo piensas actuar en el momento que tengas que responsabilizarte del uso de Internet por tu nieto?

Ya estoy intentando hacer que comprenda las trampas que puede encontrar en la Red, que son muchas. Cuando llegue el momento y esté en mi casa solo utilizará el PC. Delante mía. Sé que hay maneras de bloquear páginas y temas, llegado el caso lo haría pero creo más interesante que sea él mismo, con nuestra ayuda, el que se haga responsable. Es mi opinión, no sé si equivocada. Tanto mi hija como yo estamos trabajando ya en eso.

- ¿Qué es para ti el control parental en Internet?

Es fundamental que los padres vigilen de cerca. Que hablen mucho con los hijos y adviertan de los peligros que pueden correr.

- ¿Te sientes segur@ en la Red?

Pues no debo sentirme muy segura cuando no entro en *link* que recomiendan en algunos sitios, que no son sospechosos pero no conozco.

- Elena, ¿qué es para ti un *hacker*?

La palabra *hacker* solo verla me da miedo. Pero a través de tus escritos y poco a poco, me doy cuenta que dentro de los *hackers* pueden existir de todo tipo. Gente buena y menos buena. De todas formas la palabra sigue echándome hacia atrás.

Elena, tú sí que eres un "ángel en la Red" y fuera de ella, estoy seguro de que tu familia y amig@s estarán muy orgullosos de ti, sobre todo tu/s niet@/s cuando lean estas líneas, además de que se sentirán más protegidos en la Red gracias a su súper "ciberabuela".

II
SEGURIDAD EN LA RED

"La desconfianza es la madre de la seguridad."

Aristófanes

Internet nos aporta un mundo de grandes posibilidades, nos abre de par en par una ventana al mundo que normalmente es demasiado lejano para que podamos acceder a él, pero gracias a la Red de redes se hace accesible desde la comodidad de nuestras casas, trabajos o centros de ocio.

En seguridad hay un dicho que dice que la seguridad plena no existe, que la seguridad nunca es completa. Internet no es diferente en ese sentido. Recientemente, en una conferencia sobre seguridad en Internet, escuché afirmar a uno de los ponentes, especialista en seguridad informática, que los principales agujeros de seguridad se encontraban en los propios sistemas operativos de nuestros ordenadores y sobre eso no podemos hacer demasiado. Se estima que un 50% de los internautas podría tener comprometida la seguridad de sus equipos en mayor o menor medida.

Estoy totalmente de acuerdo con esta afirmación, es algo obvio, aun sin tener, ni por asomo, el conocimiento en cuanto a seguridad informática que demostró el ponente en su intervención. Pero de lo que estoy seguro es de que, incluso aceptando la afirmación del especialista informático, podemos mitigar esos riesgos de

forma sencilla. Simplemente debemos adoptar unas medidas básicas de seguridad cuando nos encontremos en la Red, medidas que no son, en absoluto, complejas de llevar a cabo puesto que no tienen nada que ver con la programación informática ni es necesario tener los más mínimos conocimientos técnicos.

Estas normas básicas de "navegación" segura se sintetizan en una única palabra, **LÓGICA.**

> "El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados."
>
> **Gene Spafford**

1. SEGURIDAD BÁSICA EN LA RED

¿Existe la seguridad plena en Internet? Sinceramente creo que no, ya expliqué los motivos, pero creo firmemente que la mayor parte de esa falta de seguridad la generamos nosotros mismos, solemos poner las cosas demasiado fáciles a los "cibermalos".

Ningún internauta está exento de los peligros de la Red y menos si no pone los mínimos medios de protección para evitarlos.

Como desarrollaremos más adelante en el apartado de *Ingeniería social,* ha quedado demostrado que el primer fallo de seguridad es el propio usuario dado que **"los usuarios son el eslabón débil en la cadena de la seguridad de cualquier sistema".** Y en Internet no va a ser diferente.

La primera medida básica para combatir los peligros de la Red es la concienciación de su existencia, conocerlos, conocer su origen, conocer su funcionamiento y cómo actúan sus responsables.

Debemos ser conscientes de que en la Red también existen cibercriminales capaces de lanzar ataques indiscriminados con el fin de controlar los ordenadores que se topen en su "camino". Cibercriminales que, si no encuentran ninguna traba,

serán capaces de robar nuestros secretos más preciados, nuestra privacidad, e incluso nuestras cuentas corrientes.

El delincuente ha mutado, ha dejado de un lado las ganzúas para utilizar programas informáticos para obtener nuestras **credenciales**[53], ha dejado de hacer tirones, butrones y alunizajes para utilizar su "fuerza bruta" en "romper" las contraseñas robadas. Ahora realiza otras actividades tan fructíferas o más pero sin embargo menos expuestas para ellos.

Ahora el delincuente se ha convertido en ciberdelincuente, desarrolla distintos tipos de *malware,* virus, gusanos o troyanos, que lanzados mediante campañas de *spam* y *phishing,* combinadas con distintas técnicas de ingeniería social logran "entrar hasta la cocina" del internauta menos precavido o simplemente menos informado y concienciado de los peligros que acechan en la Red.

Publicidad engañosa, falsas ofertas de trabajo, anuncios de compra/venta, que nos ofertan gangas impensables e irrechazables, *scam, smishing,* timos, fraudes y estafas.

Una de las mayores vías de "infección" a las que nos exponemos, y de forma "gratuita", son los conocidos programas *"peer to peer"* o **P2P**[54]. Programas de intercambio de todo tipo de archivos, generalmente lo más común es el intercambio de películas, programas, música. Esa última versión del deseado programa de retoque fotográfico, la nueva película recién estrenada en las salas de cine, o el nuevo disco de nuestro grupo o cantante favorito, todo lo tenemos al alcance de la mano y completamente gratis.

Esa gratuidad ha convertido a los programas tipo Emule, Ares, etc. en una de las mayores vías de infección y propagación de *malware,* virus y troyanos, poniendo en peligro nuestra seguridad y privacidad y eso en el mejor de los casos.

Lanzar un ataque valiéndose de las redes P2P es de lo más sencillo y seguro para los cibercriminales. Simplemente conectándose a cualquiera de los conocidísimos programas P2P y compartiendo un archivo cuyo nombre se encuentre en el "top de búsquedas", la última versión de cualquier programa, esa última película recién estrenada o último disco de nuestro cantante favorito. Posiblemente incluso tengamos suerte, en el menor de los casos, y consigamos el ansiado archivo, pero para

[53] **Credencial:** Que acredita en Internet credenciales. Son los datos, usuario y contraseña, que necesitamos para autentificarnos en un servicio *on-line* (bancos, correo electrónico, redes sociales, etc.).

[54] **P2P:** siglas en inglés para *peer to peer,* en español algo similar a 'de persona a persona' o de 'igual a igual'. En el P2P los que interactúan, comparten un interés específico compartiendo información "digital" de forma directa.

nuestra desgracia en la mayoría de los casos puede venir con "premio" escondido tras el verdadero archivo que trae incrustrado cualquier tipo de *malware* que nos ponga en un verdadero aprieto.

Posiblemente muchos de las "palabrejas" que acabamos de mencionar, en los párrafos anteriores, os suenen a "chino mandarín" pero no os preocupéis, a lo largo de este libro iréis descubriendo su significado y su similitud con los peligros que nos acechan en la vida real.

Y hablando de la vida real, la vida virtual no difiere de la real, y ahí está el "*quid* de la cuestión", la respuesta a la pregunta de cómo protegernos en la Red, se sintetiza en una única palabra, **LÓGICA.**

A lo largo de la lectura de este libro, la palabra lógica estará presente en cada uno de los mensajes que se pretenden transmitir, o el sentido de ella, puesto que considero que es el principio básico de seguridad a tener en cuenta desde el momento en el que encendemos nuestros *routers* u otros medios para proveernos de Internet en nuestros equipos informáticos, ya sean ordenadores, *tablets* o *smartphones.*

La seguridad en la Red no diferencia los medios de conexión, el peligro nos puede llegar sin importar el dispositivo que utilicemos para conectarnos.

¿Cómo emplearemos la lógica en Internet para evitar los peligros que nos acechan? Es una pregunta importante a tener en cuenta, evidentemente no existe ningún programa informático que nos permita controlar el "nivel de lógica" que tenemos que utilizar en cada momento, pero la respuesta es sencilla. Tenemos que olvidarnos de la virtualidad de la Red y pensar que nos estamos moviendo en un mundo real, tan real como los peligros que se nos pueden llegar a presentar en este mundo tan "virtual".

No pensemos que la seguridad en Internet es cosa de expertos informáticos, lo único que tenemos que hacer es actuar como lo haríamos en la vida real: "No voy a cruzar por aquí porque hay mucho tráfico, voy a buscar un paso de peatones, o un semáforo". En Internet es igual, si no estás seguro de algo, si piensas que puede ser un sitio web comprometido, un correo que no conoces su remitente, un archivo poco fiable… simplemente, y por lógica, ¡óbvialo!

Una vez teniendo clara la falsa virtualidad de los peligros, debemos comenzar a tener buenos hábitos en el uso de Internet y para ello debemos estar informados de los peligros que nos pueden acechar.

El principal foco de peligrosidad con el que nos encontramos en Internet, como ya hemos visto, es el que viene potenciado por la ciberdelincuencia. También hemos

visto que los ciberdelincuentes no difieren de los delincuentes convencionales salvo en la forma de llevar a efecto sus actividades delictivas.

Un ciberdelincuente puede robar, estafar, emplear nuestra identidad, hacerse pasar por un banco o utilizar nuestra propia identidad en nuestro banco, comprar un producto con nuestros datos personales y bancarios, e infinidad de actividades delictivas más, pero todas ellas con un denominador común: utilizar la Red como herramienta o como forma de hacer efectiva su "fechoría".

Las distintas técnicas que emplean para sus cibercrímenes van evolucionando y adaptándose a las circunstancias y a los momentos, por eso es necesario estar informados de sus "andanzas" y conocer sus técnicas para acceder a nuestra "ciber-vida", sobre todo conocer sus formas de engañarnos y sus artes de manipulación con el fin de obtener nuestra información personal y confidencial.

Los bienes más preciados que pueden peligrar en la Red son nuestra propia seguridad, nuestra privacidad y nuestra economía.

No facilitemos gratuitamente información sobre nuestros "tesoros" a proteger, no compartamos con desconocidos datos personales, nuestras fotografías o informaciones sobre nuestra vida privada o social. En el Internet social es muy sencillo hacerse "falsos" amigos. Volviendo a la lógica, no compartáis con vuestras "amistades virtuales" ningún tipo de información o contenido que no harías con vuestro círculo real de amistades o familia, piensa que esa información puede volverse contra tu propia seguridad, privacidad e incluso contra tu economía si es utilizada de forma inadecuada por esos "falsos amigos".

Según la agencia Europa Press, el 8% de los internautas españoles reconoce que ha sido víctima del robo de su identidad en Internet en los últimos meses, de los cuales el 1% asegura que ha sido víctima de este tipo de delito con frecuencia.

No caigáis en la creencia errónea de pensar que un ordenador comprometido o infectado se detectaría fácilmente porque se bloquearía, funcionaría más despacio o crearía ventanas emergentes indiscriminadamente. En la mayoría de las ocasiones el cibercriminal elude todo esto intentando hacer pasar totalmente desapercibida su acción.

2. DIEZ MANDAMIENTOS PARA UNA NAVEGACIÓN SEGURA

Una vez que conocemos los riesgos a los que nos enfrentamos es hora de pasar a la protección de nuestros equipos y para ello también vamos a utilizar unas normas básicas:

1. Utilizar un **antivirus de confianza,** no de los que se descargan de cualquier página web (los hay incluso gratuitos y muy efectivos), y sobre todo tener en cuenta la importancia de tenerlo actualizado. Los virus van apareciendo y los antivirus necesitan estas actualizaciones para desempeñar su función.

2. Mantener **actualizados los sistemas operativos** de nuestros ordenadores así como los programas más sensibles de infección o propicios para facilitar la entrada a nuestros equipos por nuevas vulnerabilidades detectadas y que no han sido actualizadas.

3. No bajar la guardia pensando que al tener instalado un antivirus o actualizado nuestro sistema operativo estamos exentos de ser víctimas de cualquier ataque. **Los virus realmente son peligrosos en su "nacimiento" cuando todavía no han sido detectados ni se conocen las "puertas falsas" por donde entran en nuestros equipos (vulnerabilidades aún desconocidas)**, ni el *malware* catalogado por las compañías de seguridad informática. A esto se le denomina "ataque del día cero (0Day)".

4. Si nuestros conocimientos no son demasiado apropiados para poder apreciar un ataque por algún tipo de ***malware*** deberíamos **utilizar una cuenta de usuario con permisos restringidos,** evitando usar la cuenta de administrador que utilizamos por defecto en nuestros ordenadores, de esa manera evitaremos que estos virus modifiquen o manipulen nuestro ordenador.

5. **Elegir contraseñas seguras** y distintas para cada uno de los servicios de Internet que utilicemos.

6. **Usar sentido común** y no hacer *click* en cualquier "cosa" que veamos en la Red.

7. **Desconfiar** de los enlaces o descargas que nos aparecen en páginas web de poca confianza o correos electrónicos enviados por desconocidos.

8. **Nunca abrir mensajes de usuarios desconocidos** o que no se hayan solicitado, eliminarlos directamente y no contestar en ningún caso a estos mensajes.

9. No hacer operaciones bancarias **desde ordenadores que no sean de tu confianza,** como los de los cibercafés o utilizando conexiones wifis que no controles. Lo ideal sería utilizar un ordenador específico para "operaciones sensibles" en la Red y no mezclar la navegación de ocio.

10. Ser muy cautelosos con la información **que se decide compartir en la Red** y con quien se comparte, porque Internet es como Las Vegas, **lo que se sube a Internet queda en Internet** y no será fácil su borrado total. Por supuesto solo se debe aceptar a gente conocida tanto en los clientes de mensajería instantánea como en redes sociales.

3. LA IMPORTANCIA DE LAS CONTRASEÑAS

Una contraseña segura es tu primera línea de defensa contra los intrusos e impostores y por eso se convierte en uno de los mayores puntos flacos en nuestra seguridad en la Red.

Recientemente apareció en el blog de **ESET**[55] la entrada *Las contraseñas siguen siendo un punto débil de los usuarios.* De su lectura se puede extraer el preocupante mensaje de que los usuarios de Internet no ponemos los medios suficientes para reforzar nuestra propia seguridad en la Red, por lo que nos convertimos en nuestra principal vulnerabilidad y por tanto generamos inconscientemente nuestro principal punto débil.

Aspecto preocupante es que un **42,3% de los usuarios asegura utilizar una palabra o frase real** como parte de la contraseña. Aunque esto facilita que la misma sea recordada fácilmente, también permite que sea vulnerada e incluso adivinada en menor tiempo y utilizando pocos recursos.

[55] **ESET** es una compañía que desarrolla soluciones de seguridad para usuarios domésticos y empresas, encaminadas a la protección de los equipos informáticos ante las amenazas víricas en la Red.

Como quedó de manifiesto en la edición **de la Security Blogger Summit,** del 2012, organizada por **Panda Security** y en la que se abordó como uno de los temas principales **la seguridad y privacidad en la Red,** los cibercriminales explotan las vulnerabilidades tanto de los propios equipos informáticos como de las redes sociales en búsqueda de sus víctimas.

Si además de todo esto el usuario les pone en bandeja de plata el acceso a los perfiles privados o cuentas de correo, eligiendo contraseñas débiles o comunes (la típica *password* 1234) fácilmente deducibles (nombre de pila) o fáciles de obtención como números de documento, fechas de nacimiento, o por fuerza bruta al utilizar palabras demasiado "lógicas" o "evidentes", podríamos decir que dejamos abiertas la puerta de nuestra casa de par en par, incluyendo en el "paquete" nuestros datos más personales (bancarios, personales, ideológicos, etc.).

Por todo esto, y si no queremos utilizar un programa generador/gestor de nuestras contraseñas, creo que se hace conveniente la utilización de ciertas pautas a la hora de elegirlas y que se podrían resumir brevemente en:

- **No reveles jamás tu contraseña a nadie.** No se la digas a tus amigos, por muy buenos que sean. Un amigo se la podría revelar por accidente a otra persona o incluso utilizarla para fastidiarte si se rompe vuestra amistad.
- **No utilices la misma contraseña para sitios web distintos.** Si alguien se entera de cuál es esa contraseña, podría usarla para entrar también en tus cuentas de los demás sitios.
- **Crea contraseñas que sean fáciles de recordar pero que resulten difíciles de adivinar a los demás.** *Por ejemplo,* imagínate una frase como "**T**erminé **d**e **e**studiar **e**n **e**l **c**olegio **e**n **2004**" y usa las iniciales de cada palabra de este modo: "Tdeeece2004".
- **Crea contraseñas que tengan al menos 8 caracteres.** Cuanto más largas mejor, así resultarán más difíciles de descubrir.
- **Incluye números, mayúsculas y símbolos.** Si el sitio web lo permite, usa $ en vez de S o cambia las vocales por números o símbolos (A-4, E-3, I-1, O-0, U->) o incluye "&" o "!". Sin embargo, ten en cuenta que $01t3r0 (Soltero) NO es una contraseña segura, pues los ladrones de contraseñas ya se saben este truco. En cambio, M4$3>gtyb4 (MASEUGTYBA, iniciales de: "Mi amigo Salvador es un gran tipo y buen amigo") podría ser una buena contraseña.
- **Estudia la posibilidad de usar un gestor de contraseñas.** Hay varios programas y servicios web que permiten crear una contraseña distinta y segura

para cada sitio. En cambio, tú solo tienes que acordarte de la contraseña que te permite acceder al programa o al sitio seguro donde están guardadas las demás. Dos de estos programas son RoboForm (para Windows solamente) y Lastpass (para Windows y Mac).

- **No te dejes engañar por los ataques de *phishing.*** Asegúrate bien antes de hacer *click* en un vínculo que te pida iniciar sesión, cambiar la contraseña o proporcionar cualquier tipo de información personal, aunque parezca proceder de un sitio legítimo. Podría ser un mensaje fraudulento de *phishing* y que la información que proporciones la reciba un ciberdelincuente. Si dudas, inicia sesión manualmente escribiendo en la ventana del explorador la dirección URL que tú conoces del sitio en cuestión.

- **Asegúrate de que tu ordenador sea seguro.** La mejor contraseña del mundo no te servirá de nada si hay alguien que mira por encima del hombro mientras la escribes (ya sea en la vida real o en el entorno virtual) o si te olvidas de cerrar la sesión en un ordenador compartido (en un cibercafé por ejemplo). El *software* malintencionado, incluidos los ***keyloggers*** (programas registradores de pulsaciones de teclas) que graban todas las pulsaciones de teclas, pueden robarte las contraseñas y otra información. Para aumentar la seguridad, asegúrate de usar un *software* antivirus actualizado y que el sistema operativo esté al día.

- **Estudia la posibilidad de usar una contraseña también en el teléfono móvil.** Muchos teléfonos se pueden bloquear de tal forma que solo puedan utilizarse si se escribe un código. La gente puede encontrar o robar teléfonos desbloqueados y usarlos para adquirir información personal, realizar llamadas o enviar mensajes de texto como si fueses tú. Usando tu teléfono, alguien podría enviar mensajes de texto de tal forma que parezca que estás acosando a gente que figura en tu libreta de direcciones enviándoles palabras o imágenes desagradables.

Otra cuestión sería que los "malos" obtengan nuestras contraseñas mediante ingeniería social o mediante la utilización de programas con "código malicioso" (*keyloggers,* etc.), pero eso ya sería tema de otra cuestión.

4. EL MEJOR ANTIVIRUS DEL "CIBERMUNDO"

Está claro que para muchos internautas la protección de sus ordenadores, *tablets* o *smartphones* no es un tema que les inquiete. En su "cibermundo" son ajenos a los peligros que nos podemos encontrar en la Red y, por consiguiente, también lo son a sus graves consecuencias.

Son de los que desoyen las sabias frases del refranero español como ***"más vale prevenir que curar".***

Esto me recuerda una histórica frase, según una extendida leyenda, en la que se cuenta que Boabdil "el Chico", último rey moro de Granada, al salir de la ciudad tras ser reconquistada por los Reyes Católicos, y camino de su exilio, volvió la cabeza para ver su ciudad por última vez y lloró, por lo que su madre se dirigió a su hijo con esta histórica frase *(de forma bastante machista, por cierto):*

"Llora como mujer lo que no supiste defender como hombre…"

Esta cita, hoy en día, se utiliza dándole un significando a la inutilidad de las lágrimas derramadas a destiempo, y que en nuestros "ciberdías" podríamos adaptarla y versionarla como:

"Llora como 'inconsciente' lo que no supiste defender como
'internauta' seguro…"

Bien, como sabéis, desde este libro se pretende informar de los peligros potenciales que existen en la Red para poder evitarlos con medidas preventivas o mitigarlos una vez afectados para que sus consecuencias sean los menos "molestas" posibles.

En el caso de las vulnerabilidades, que afectan a nuestros equipos aprovechándose de los conocidos y molestos "ciberbichitos" de todo tipo que aprovechan el más mínimo "agujerito" *(bug)* en nuestros sistemas informáticos, disponemos de infinidad de soluciones antivirus, tanto comerciales como gratuitas.

Se ha realizado un exhaustivo estudio, de las principales soluciones antivirus, desde el "Departamento Técnico" de *El blog de Angelucho* en colaboración con las más prestigiosas universidades de cuya cantera nacen los mejores y más preparados ingenieros "sociales", así como la participación activa de los *"juakes"* más peligrosos y prestigiosos del "mundo mundial".

Una vez terminado el estudio, tras un análisis minucioso de los pros y los contras de cada una de las soluciones *antimalware* analizadas, queremos hacer público el resultado final del mismo aportando la mejor solución para evitar ser "infectados".

El mejor antivirus es…

Mira detrás de tu teclado

¡EL MEJOR ANTIVIRUS ERES TÚ!

Como veis y en tono de humor, no quiero más que reforzar lo que siempre os digo:

Nosotros mismos somos nuestra peor vulnerabilidad pero también somos nuestro mejor antivirus.

5. CÓMO NAVEGAR DE FORMA SEGURA DESDE UN ORDENADOR QUE NO ES EL NUESTRO

Muchas veces sucede que estamos de viaje o sencillamente lejos de casa y necesitamos tener acceso a Internet para revisar nuestro correo o comunicarnos con algún contacto o solo obtener alguna información.

Para ello debemos acudir a un cibercafé o si disponemos de un dispositivo portátil (ordenador, *tablet* o *smartphone*) tenemos la posibilidad de conectarnos mediante wifi a un ***hotspot***[56] de los muchos que hay en sitios públicos.

En estos casos es totalmente necesario que tomemos algunas medidas de precaución básicas para preservar nuestra privacidad y seguridad, al igual que lo haríamos si utilizásemos un ordenador público (de un ciber, por ejemplo).

Cuando navegamos por Internet, **los navegadores suelen guardar nuestras contraseñas** para que no tengamos que teclearlas cada vez que nos metamos en nuestra cuenta de correo electrónico o cualquier otro servicio que necesite de nuestras credenciales. Esto es muy **cómodo,** cuando utilizamos ordenadores "de confianza", en casa, por ejemplo.

[56] ***Hotspot*** es un acceso wifi, que suele ofrecerse en lugares públicos (restaurantes, centros comerciales, etc.) y que puede ser aprovechados especialmente por dispositivos móviles para acceder a Internet.

Pero esta "cómoda" opción no es recomendable para ser utilizada en ordenadores compartidos por otros usuarios que no sean de nuestra total confianza (casi ninguno) o en ordenadores públicos (un ciber, un ordenador público, etc.)**.**

Con este artículo se pretende informar y enseñar a navegar, de forma más segura, desde un ordenador que no es nuestro o no sea de nuestra "confianza" (el de un amigo, en un cibercafé, en un centro público, etc.) **sin poner en riesgo nuestra "confidencialidad" y privacidad,** tanto por las páginas que hayamos visitado, como por las contraseñas que hayamos tenido que introducir. En cualquier caso, y esto es **muy importante,** para navegar por páginas **muy comprometidas** (bancos *on-line,* trabajos, etc.) lo mejor es **hacerlo desde un ordenador seguro de nuestra propia confianza, por ejemplo desde casa (aquí los GRANDES[57], ellos se reconocerán, pensarán, "¡¡sí, sí, seguro!!" ;_) y esbozaran una sonrisa), nunca desde un ordenador público.**

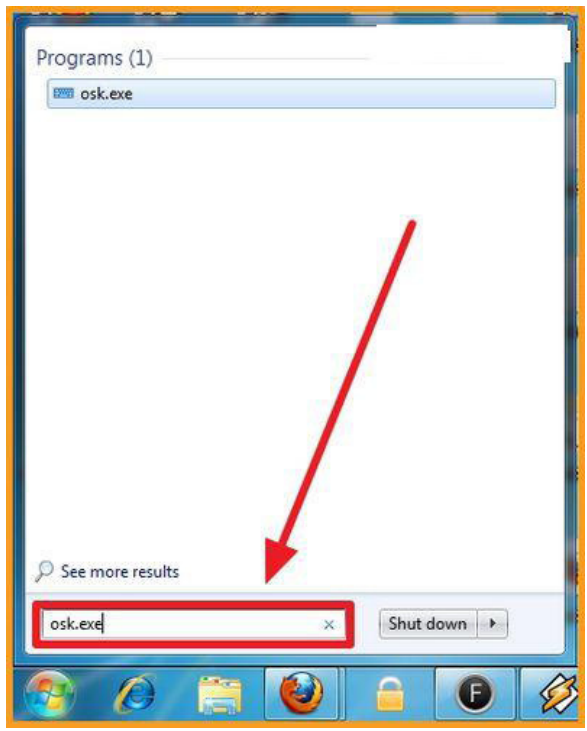
Cuando utilicemos un ordenador público JAMÁS, y digo JAMÁS, guardéis vuestra información de acceso o *logueo*[58], esto quiere decir que nunca se os ocurra marcar esos casilleros que dicen "recordarme en este ordenador" o "no cerrar sesión" o cosas similares:

[57] En las diferentes entradas de *El Blog de Angelucho,* o en los distintos artículos de este libro el autor denomina **GRANDES** a los *hackers* que se dedican a hacer el bien *(Ver artículo sobre* hackers *en el libro).*

[58] ***Loguearse*** es identificarse para ingresar a un sitio restringido de acceso con usuario y contraseña.

Nunca escribir información personal sensible en un ordenador que no sea nuestro, esto incluye número de tarjetas de crédito, *passwords* de cuentas correo personal o corporativo, de acceso a webs personales o profesionales, servidores.

Cuando escribamos nuestras contraseñas o información "sensible", utilicemos el **teclado "virtual" en pantalla (ejecuntando "osk.exe" desde Inicio de Windows).**



Las transacciones bancaria realizarlas siempre desde casa o punto de acceso de confianza, de lo contrario nuestra información privada puede ser usada por ciberdelincuentes, en puntos de acceso públicos pueden tener instalados algún tipo de del tipo ***Keylogger***[59] que graban todo cuanto escribimos en el teclado y aparece en el monitor, sin que nos demos cuenta.

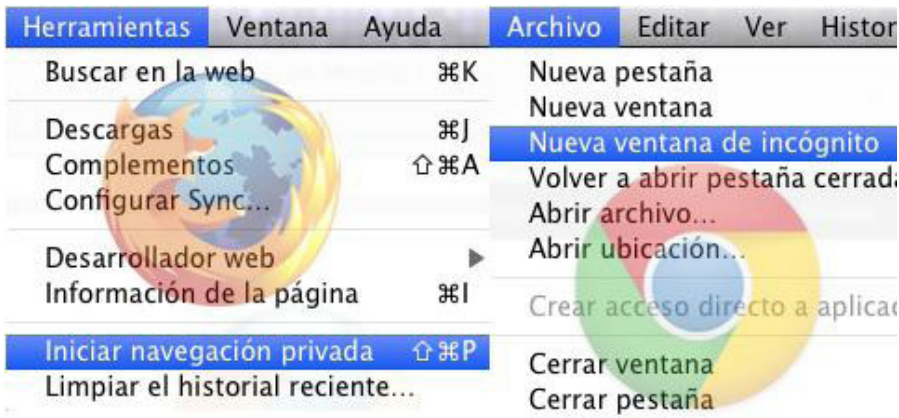
Una vez que finalicemos de utilizar el ordenador debemos eliminar el historial de la navegación, y si fuera posible reiniciar el PC.

[59] ***Keylogger*** es un tipo de *software* o un dispositivo *hardware* específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de Internet.

La mayoría de los ordenadores públicos tienen instalados distintos navegadores, **Mozilla Firefox** por ejemplo, un navegador que junto con **Google Chrome, se encuentra entre los más extendidos y que se consideran razonablemente "seguros".** Para empezar a navegar de forma privada, solo tendremos que decirle al navegador que, temporalmente, **deje de guardar toda nuestra información.** Esto suele conocerse comúnmente como **modo privado o modo de incógnito.**

También podemos ahorrarnos algún paso de los explicados hasta ahora, sencillamente **teniendo una navegación anónima o privada,** existen varios métodos, alguno de ellos incluso los podemos llevar en una memoria USB con nuestro propio navegador "portable", posiblemente un poquito más técnico que todo esto, pero si os ponéis veréis que es muy sencillo.

Otra forma, posiblemente la más válida para los que no "sabemos mucho de esto", es **configurar el navegador** que utilicemos. Cada navegador tiene su forma de activar este modo como podéis ver a continuación.



- En Firefox (Herramientas > iniciar navegación privada) como en Chrome (Archivo > nueva ventana de incógnito). Al activar esta función, **en Firefox desaparecen todas las pestañas que estuvieran abiertas** y esto indica que el navegador ya está listo para el modo privado.

- **En Chrome aparecerá una nueva ventana** (con un borde más oscuro, como en la primera imagen de esta nota), desde la cual podremos navegar de forma privada.

Para desactivar el modo privado del navegador y que vuelva a guardar toda la información, es muy sencillo.

- En Google Chrome, simplemente hay que **cerrar la nueva ventana** que nos ha aparecido.
- En Firefox tendremos que **hacer *click* en el mismo sitio** que antes, con la diferencia de que ahora en vez de poner Iniciar navegación privada, pondrá detener (Herramientas > Detener navegación privada)

Sencillo, ¿verdad? ¡¡¡Pues ya sabéis!!!

Recordemos que…

Nosotros mismos somos nuestra peor vulnerabilidad pero también nuestro mejor antivirus.

6. PRECAUCIONES AL UTILIZAR UNA WIFI "GRATUITA"

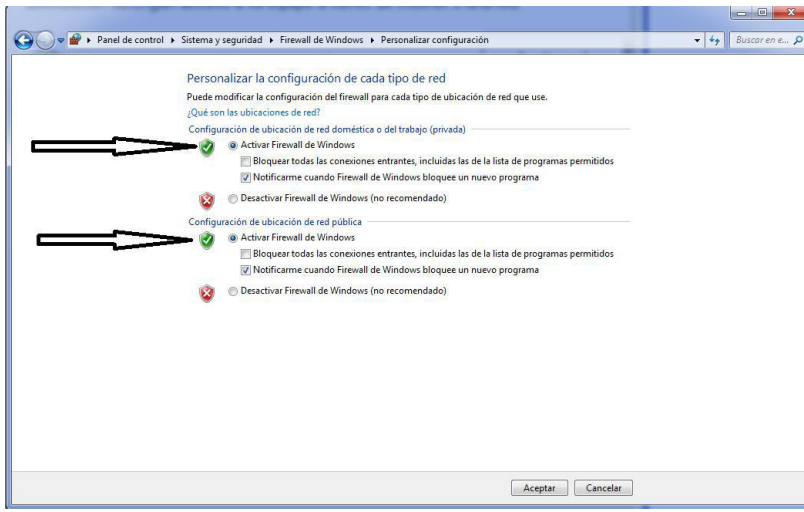
Voy a continuar con la misma línea que en los artículos anteriores encaminados a concienciar sobre las medidas básicas de seguridad que debemos adoptar cuando nos conectemos a Internet fuera de nuestro entorno habitual.

Muchas veces sucede que estamos de viaje o sencillamente lejos de casa y necesitamos tener acceso a Internet para revisar nuestro correo o comunicarnos con algún contacto o solo obtener alguna información.

Para ello debemos acudir a un cibercafé o si disponemos de un dispositivo portátil (ordenador, *tablet* o *smartphone*) tenemos la posibilidad de conectarnos mediante wifi a un *hotspot* de los muchos que hay en sitios públicos (un *hotspot* es una zona en la que tenemos acceso gratuito a una conexión inalámbrica de Internet por cortesía de un local como un café, hotel, o simplemente de un "alma caritativa").

En estos casos es totalmente necesario que tomemos algunas medidas de precaución básicas para preservar nuestra privacidad y seguridad, al igual que lo haríamos si utilizásemos un ordenador público (de un ciber, por ejemplo). Estas medidas se pueden resumir en:

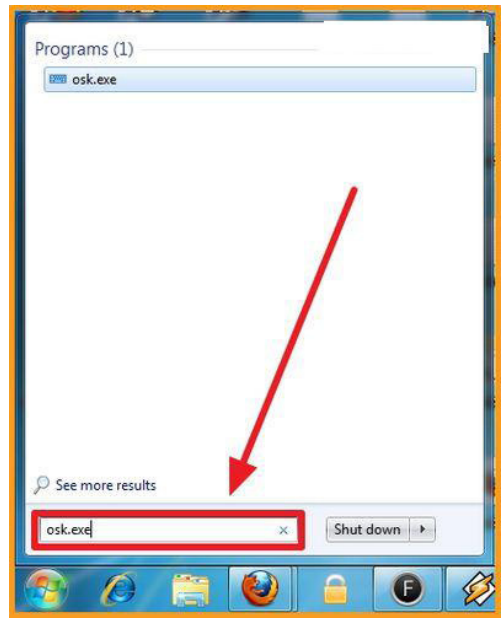
- Debemos usar un *Firewall* (programa que bloquea acceso externo no autorizado a nuestras computadoras). Hay muchos *firewalls* gratuitos :
  - ZoneAlarm
  - Comodo Personal Firewall (muy recomendable).
- Si no queréis uno pueden usar el que viene incluido con su Windows XP, Vista o Windows 7:



- Apagar el wifi cuando no lo estemos usando, jamás conectarnos a una red pública y dejar nuestro dispositivo encendido y conectado vía wifi, siempre nos desconectaremos (*smartphones, tablets,* etc.) o apagaremos (ordenadores portátiles, etc.). Con esta medida evitaremos que se nos "enganchen" a nuestro equipo, aprovechando cualquier vulnerabilidad que tenga nuestro sistema operativo o mediante cualquier tipo de *malware.*
- En caso de tener que enviar información que pudiera ser importante, **encriptaremos los archivos antes de enviarlos,** hay muchos programas gratuitos que sirven para encriptar archivos. Por ejemplo **Truecrypt,** que es una aplicación gratuita (**descarga en** http://www.truecrypt.org).

- **No "trasmitir" información que no nos interese que otros vean,** como transacciones bancarias, accesos a webs o servicios que pudieran verse comprometidos. Tenéis que saber que alguien puede estar "escuchando" todos los paquetes del tráfico que transmitimos y "leer" todas nuestras conversaciones, *passwords,* información, mensajes, etc.

- Cuando escribamos nuestras contraseñas o información "sensible", utilicemos el **teclado "virtual" en pantalla (ejecutando "osk.exe" desde Inicio de Windows).**



- Si no nos queda más remedio que realizar una transacción conectados a una wifi pública, **al menos asegurémonos que la página donde estamos haciendo la operación use el protocolo SSL.** Sabemos que una web usa SSL cuando una vez en ella, vemos el icono de un candado en la parte inferior derecha, y la dirección en la barra de la URL comienza con "http://" .

Cómo comprobar si el sitio web usa una conexión segura (SSL).

Cuando introduzcas información personal confidencial en una página, busca el icono con forma de candado a la izquierda de la URL del sitio en la barra de dirección para ver si el sitio usa SSL.

SSL es un protocolo que proporciona un túnel encriptado entre tu ordenador y el sitio que estás viendo. Los sitios pueden usar SSL para evitar que terceros interfieran con la información que viaja por el túnel.

Ejemplos de SSL con Google Chrome:

Icono	¿Qué significa?
	El sitio no usa SSL. La mayoría de los sitios no necesitan usar SSL porque no solicitan información confidencial. Evita introducir información confidencial, como nombres de usuario y contraseñas, en la página.
https://	**Google Chrome ha establecido correctamente una conexión segura con el sitio.** Busca este icono y asegúrate de que la URL tenga el dominio correcto si tienes que acceder al sitio o introducir información confidencial en la página. Si un sitio utiliza un certificado SSL con validación ampliada (EV-SSL), al lado del icono también aparecerá el nombre de la organización escrito en color verde.
https://	**El sitio usa SSL, pero Google Chrome ha detectado contenido que no es seguro en la página.** Si vas a introducir información confidencial en esta página, ten cuidado. El contenido peligroso puede ser una puerta de acceso para que alguien cambie el aspecto de la página.
https://	**El sitio usa SSL, pero Google Chrome cree que el riesgo de que la página incluya contenido que no es seguro es alto o que puede haber una incidencia en el certificado del sitio.** No introduzcas información confidencial en esta página. Un certificado que no es válido o la existencia de irregularidades graves en la https podrían indicar que alguien está intentando manipular tu conexión al sitio.

¿Os parecen muchas medidas de seguridad? Vosotros sois los únicos que podéis valorar vuestra privacidad.

Bueno, pues ya sabéis lo que toca deciros, ¿verdad?

Nosotros mismos somos nuestra peor vulnerabilidad, pero también nuestro mejor antivirus.

III
AMENAZAS EN LA RED

"Pienso que los virus informáticos muestran la naturaleza humana: la única forma de vida que hemos creado hasta el momento es puramente destructiva."

Stephen Hawking

La seguridad en la Red, al igual que en la vida real, no puede asegurarse al 100%. Decíamos en el anterior capítulo sobre seguridad en la Red, que el 50% de los internautas podría tener comprometida la seguridad de sus ordenadores, y seguramente por fallos, muchos de ellos no conocidos, de los propios sistemas operativos y navegadores.

Pero de lo que sí estoy plenamente convencido es de que podemos evitar pequeños problemas que nos pueden afectar, o incluso graves amenazas, simplemente conociendo su origen o de donde podría surgir, su funcionamiento, y sobre todo conociendo nuestras propias vulnerabilidades. Y todo ello acorde a una de las afirmaciones más repetidas en las entradas del blog y por consiguiente en este libro:

Nuestra peor vulnerabilidad somos nosotros mismos, pero también somos nuestro mejor antivirus.

En este capítulo haremos un recorrido por las entradas al blog relativas a las amenazas que nos acechan en Internet. No solo a las distintas amenazas virales reportadas o no y que nos "atacan", sino también a otro tipo de amenazas dirigidas por ciberdelincuentes para obtener sus "beneficios" en contra de nuestro bienestar, sobre todo económico, pero también en muchas ocasiones, esas actividades afectan a nuestra propia seguridad y privacidad.

Gracias a que conocemos y aprendemos sus formas de actuar, hemos podido aprender a defendernos y evitarlos.

Ya hemos hablado en el primer capítulo de este libro, de forma obligada, de una comunidad bastante castigada a lo largo de su historia, me refiero a la comunidad *hacker,* a la cual no hay que culpabilizar de los males de la Red. Ellos no son la amenaza, la amenaza son los ciberdelincuentes entre los que habrá ladrones, estafadores, timadores, incluso algún que otro *hacker,* ¡claro que sí! Ya he dejado clara mi opinión al respecto y espero que la compartáis conmigo: *hacker* no debemos asociarlo a delincuente aunque algún delincuente sea *hacker.*

Entre las principales preocupaciones de los internautas españoles se encuentran los temores a la realización de las transacciones dinerarias o compras por Internet ante el temor de un "robo" de sus identidades bancarias digitales.

Igualmente, los españoles se encuentran entre los europeos más preocupados por encontrarse de forma accidental en Internet con contenidos racistas o que inciten a la violencia religiosa o contenidos de pornografía infantil.

1. LA CIBERDELINCUENCIA Y LOS INTERNAUTAS

Para este apartado tengo la gran suerte de contar con dos puntos de vista, dos perspectivas totalmente distintas, pero ambas confluyentes en mi propio conocimiento. Uno es el punto de vista personal, pues si recordáis soy internauta desde la llegada de Internet a los hogares españoles. El segundo es el punto de vista profesional, dado que me dedico de forma activa a la lucha contra los distintos tipos de ciberdelincuencia, concretamente como agente del Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Guardia Civil (y de lo que me siento

muy orgulloso) y quiero que este libro sea en parte un homenaje a todos mis compañeros en agradecimiento por todo lo que me han aportado y enseñado.

Según **INTERPOL**[60] la ciberdelincuencia, tal y como aparece en su propia página web, constituye uno de los ámbitos delictivos de más rápido crecimiento. Cada vez más delincuentes se aprovechan de la rapidez, la comodidad y el anonimato que ofrecen las tecnologías modernas para llevar a cabo diversos tipos de actividades delictivas. Éstas incluyen ataques contra sistemas y datos informáticos, usurpación de la identidad, distribución de imágenes de agresiones sexuales contra menores, estafas relacionadas con las subastas realizadas a través de Internet, intrusión en servicios financieros en línea, difusión de virus, *botnets* (redes de ordenadores infectados controlados por usuarios remotos) y distintos tipos de estafas cometidas por correo electrónico, como el *phishing* (adquisición fraudulenta de información personal confidencial).

Supongo que ya os habréis dado cuenta que no existen prácticamente actividades delictivas nuevas, simplemente han evolucionado, se han adaptado a las nuevas tecnologías. Utilizan un ordenador para robar en lugar de una pistola, o un correo electrónico para timar en vez de las "estampitas de Lina Morgan".

En el siglo XXI es evidente el alcance que tiene Internet a nivel mundial. Esta expansión ha obligado al delincuente a mutar y a convertirse en ciberdelincuente, pudiendo conseguir sus propósitos desde el falso anonimato que otorga la Red. Sin embargo, Internet permite que estas actividades no conozcan fronteras.

Cuando hablamos de delincuencia en Internet rápido nos viene a la cabeza, y de forma equivocada, el término *hacker* directamente vinculado con la piratería informática. Pero queda lejos, muy lejos de la realidad, al menos desde mi humilde opinión y mis "distintos" puntos de vista, y por eso no se va a hacer alusión, en este capítulo, a la palabra *hacker* con connotaciones negativas ni como ciberdelincuente.

La virtualidad de Internet no existe, Internet no es un juego que termina cuando apagamos nuestro ordenador, es una extraordinaria forma de comunicación que influye muy positivamente en nuestras vidas gracias a los beneficios y bondades que nos aporta. Sin embargo, la cara "B" de la

[60] La **Organización Internacional de Policía Criminal (INTERPOL)** es la mayor organización de policía internacional, con 190 países miembros, por lo cual es la segunda organización internacional más grande del mundo, tan solo por detrás de las Naciones Unidas.

Red es peligrosa, muy peligrosa. Peligrosidad potenciada por el desconocimiento y potenciada por la imprudencia del internauta.

Sin querer ser alarmista, simplemente realista, quiero haceros llegar el mensaje de que las consecuencias de la ciberdelincuencia pueden ser irreparables.

Cuando hablamos de delincuentes, hablamos de forma genérica de los distintos protagonistas dentro de la gran variedad de actividades delictivas, así nos referimos a ladrones, estafadores, asesinos, timadores, violadores, pederastas, acosadores, etc. Bien, pues en Internet existen también todas esas figuras del ámbito delincuencial, en muchas ocasiones las encontraremos con otros nombres derivados del inglés, ¡es la moda!, pero no dejan de ser eso, delincuentes, ladrones, estafadores, pederastas, acosadores, etc., etc., etc.

Hace unos años llegaban a nuestros buzones, de correo postal, cartas anunciándonos que habíamos sido agraciados con un extraordinario premio de lotería o que éramos los únicos beneficiarios de una herencia multimillonaria, las conocidas como cartas nigerianas. Para llevar a efecto esta conocida estafa era necesario desarrollar un laborioso trabajo mecánico para escribir, fotocopiar, imprimir, hacer sobres, timbrar todas las cartas y enviarlas por correo postal. Hoy en día una única persona es suficiente para realizar esta actividad delictiva que puede llegar a miles y miles de internautas de una sola tacada, con el simple envío masivo de esas "cartas" mediante correo electrónico o SMS, todo ello con un par de *clicks* de ratón o de "botón" de teléfono móvil.

Ahora la delincuencia o ciberdelincuencia se ha vuelto mucho más sofisticada y no solo pretende llegar a nuestros hogares a través de nuestros ordenadores, sino que también aprovecha nuestros teléfonos móviles y *smartphones* para vulnerar nuestra privacidad o atacar nuestra economía.

En los casos de pedofilia, el ciberdepredador se conformará con visualizar y obtener imágenes, para alimentar sus fantasías, de niños en aptitudes sexuales. Sin embargo, un pederasta no se quedará simplemente en el visionado de esas imágenes, intentará por todos los medios "engatusar" al menor, valiéndose de su ingenuidad, para conseguir contactar con el niño y llevar a la realidad sus más oscuras fantasías.

Actividades delictivas novedosas, con la llegada de las nuevas tecnologías, son los conocidos como sabotajes informáticos que alteran el buen funcionamiento de los ordenadores "centrales" de una empresa u organismo público, acceso a información privada o confidencial de empresas para comerciar con los datos con la competencia.

Con ello podemos hacer una clara diferenciación de objetivos, por un lado las conductas con el ánimo de causar daños técnicos lógicos y físicos, ocasionados por fallos de programación en los servidores víctima conocidos como "agujeros" o *"bugs"* o simplemente por la utilización de cualquier tipo de *malware* o troyano. Por otro lado daños dirigidos a la obtención de información confidencial y sensible de personas o empresas para traficar con los datos obtenidos, bien personales o bien empresariales, para ofertárselos a la competencia.

Queda claro que ambas conductas tienen un único fin común, el beneficio económico del ciberdelincuente.

Rapidez, comodidad y anonimato. Son las tres ventajas que ofrece Internet a los delincuentes que, cada vez en mayor medida, deciden desarrollar sus actividades criminales a través de la Red.

Estas tres ventajas, combinadas con una buena preparación técnica por parte del ciberdelincuente pueden asegurar un éxito seguro ante el internauta desinformado y descuidado.

Sin embargo, y aunque parezca una batalla perdida contra los ciberdelincuentes, podemos poner de nuestra parte y ganar la batalla. Ellos, los ciberdelincuentes, ponen todo de su parte para conseguir sus fines, son meticulosos, y siguen su "cadena" en la que aparecemos nosotros, los internautas, como el eslabón más débil. Para vencerles, lo único que necesitamos es romper su "cadena", reforzándonos. **Ellos no cuentan con nuestro "plan de defensa".**

Podemos derrotarles con la simple instalación de:

- **Antivirus de confianza**
- **Parches de seguridad de nuestras aplicaciones.**

Y por supuesto, siempre empleemos la lógica, NUNCA bajemos la guardia. Estando concienciados de la existencia de las amenazas, conociendo la forma de llegar a nosotros y conociendo su forma de actuar, tendremos el éxito asegurado.

Los ciberdelitos

Todos los internautas podemos ser víctimas de un ciberdelito y por consiguiente, objetivo de la ciberdelincuencia.

Con este libro se quiere potenciar el disfrute de las innumerables ventajas que nos ofrece la Red y para ello debemos conocer sus "desventajas". Internet es un mundo maravilloso, pero no perfecto como muchas veces nos quieren "vender". Las Tecnologías de la Información y Comunicación (TIC) también puedan ser utilizadas para atacar a la sociedad, convirtiéndose en un soporte más para delinquir.

Desgraciadamente, los ciberdelitos están teniendo cada vez mayor presencia en la vida "virtual" llegando a transformarse en un problema global y real atravesando con sus consecuencias las pantallas de nuestros ordenadores.

Los ciberdelitos son una nueva realidad en nuestra vida cotidiana, las amenazas, las injurias y el, cada vez más nombrado, *ciberbullying* o ciberacoso están cada vez más a la orden del día en los medios de comunicación.

El ciberdelito, como hecho delictivo, no es algo novedoso aunque no lo encontremos en nuestra legislación como tal. Estas actividades delicuenciales nos acompañan desde antes del nacimiento de Internet. El delito ha mutado a ciberdelito dado que, al igual que el delito tradicional, puede cometerse utilizando las ya conocidas y variadas casuísticas delictivas añadiendo la utilización de la Red para ser cometidos o simplemente cometerlos directamente en Internet. Delitos contra la intimidad, estafas, daños por intrusión en sistemas ajenos, distribución de pornografía infantil, entre otros.

El ciberdelincuente toca todos los palos delincuenciales, los más conocidos y mediáticos dada su gravedad y crueldad son los relacionados con la corrupción de menores y la pornografía infantil. Sin embargo, los ciberdelitos que están teniendo mayor presencia son los relacionados con los delitos de carácter económico, las estafas financieras y suplantaciones de identidad con el fin de utilizar las credenciales de los usuarios para accesos a sus cuentas corrientes para transferir dinero o realizar compras.

Los principales delitos que tienen presencia en la vida virtual se podrían clasificar dentro de los siguientes grupos:

- **Protección de la juventud y la infancia:**
  - Pornografía infantil
  - Captación y tráfico de menores
  - Amenazas o acoso y hostigamiento a menores
  - El acoso escolar o *bullying*
- **Protección de la dignidad humana:**

- Propagación de los materiales que inciten al odio, racismo, antisemitismo u otro tipo de discriminación en función del sexo, religión, origen u orientación sexual
- Propagación de materiales y discursos con violencia extrema o sangre desmesurada *(gore)*
- Incitación al suicidio
- Incitación a la anorexia y bulimia

- **Derecho al honor, a la intimidad o a la imagen propia:**
  - La difamación en Internet
  - La transmisión no autorizada de datos
  - El envío de correo no autorizado o *spam*
- **Propiedad del mercado, consumidores y seguridad económica:**
  - Estafas electrónicas
  - Fraudes informáticos
  - Falsificaciones documentales
- **Protección de la privacidad y al servicio de las comunicaciones:**
  - Obtención ilícita de datos personales
  - Interceptación de correos electrónicos
- **Seguridad de la información:**
  - Accesos no autorizados a sistemas informáticos
  - Daños en sistemas informáticos
  - Revelación de secretos
- **Seguridad nacional:**
  - Actividades terroristas
  - Instrucciones sobre preparación de bombas
  - Producción y venta de drogas a través de la Red
- **Propiedad Intelectual:**
  - Distribución no autorizada de obras registradas

- Copia ilegal

La vida virtual y las leyes

Los delitos que se comenten a través de Internet o que utilizan la Red para cometer la actividad delictiva no quedan impunes.

El **Convenio de Ciberdelincuencia del Consejo de Europa,** promulgado el 23 de noviembre del 2001 en Budapest, surge como consecuencia del desarrollo y utilización cada vez mayor de las Tecnologías de la Información y la Comunicación, así como de la necesidad de aplicar una política penal común, encaminada a proteger a la sociedad frente a la ciberdelincuencia, adoptando la legislación adecuada y manteniendo una política de cooperación internacional.

El Convenio señala los delitos informáticos en los siguientes grupos, y define los tipos penales que han de considerarse para cada uno ellos:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de los anteriores delitos.

2. Delitos informáticos:

- Falsificación informática mediante la introducción, alteración, borrado o supresión de datos informáticos.

- Fraude informático mediante la introducción, alteración o borrado de datos informáticos o la interferencia en sistemas informáticos.

3. Delitos relacionados con el contenido:

- Producción, oferta, difusión, transmisión, adquisición o tenencia, en sistemas o soportes informáticos, de contenidos de pornografía infantil.

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Posteriormente, en el año 2003, se promulgó la firma del **Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa** para criminalizar actos de racismo y xenofobia.

España, que participó en el amplio debate que dio lugar al Convenio, recientemente ha solicitado su ratificación, que será efectiva a partir del 1 de octubre de 2010. Ello obligará a trasponer a nuestro ordenamiento las conductas que define el Convenio.

Actualmente, los tipos penales de nuestro Código Penal que más se aproximan a lo que refleja el Convenio son (con expresión del artículo donde se encuentran reflejados):

- De los delitos relativos a la prostitución y la corrupción de menores *(Artículo 189.1,2,3,7* y *8).*
- Del descubrimiento y revelación de secretos *(Artículo 197, 199* y *200).*
- De los delitos relativos al mercado y a los consumidores (descubrimiento de secreto de empresa) *(Artículos 278* y *279).*
- De los daños *(Artículo 264.2).*
- De las estafas *(Artículo 248* y *249).*
- De los delitos relativos a la propiedad intelectual *(Artículo 270).*
- De los delitos relativos a la propiedad industrial *(Artículo 273* y *274).*
- De los delitos relativos a las falsedades documentales *(Artículos 390.1, 2* y *3, 392, 395* y *400).*
- De los delitos contra la comunidad internacional (apología del racismo y la xenofobia) *(Artículo 607).*
- De los delitos relativos a la prostitución y la corrupción de menores *(Artículos 187.1* y *189.4).*
- De los abusos sexuales *(Artículo 181.1* y *2).*

- De los delitos de exhibicionismo y provocación sexual *(Artículo 186).*
- De las amenazas *(Artículo 169* y *171).*
- De la calumnia *(Artículo 205* y *206).*
- De las injurias *(Artículo 208* y *209).*
- De fluido eléctrico *(Artículos 255* y *256).*

¿Qué hacer si he sido víctima de un ciberdelito?

- Al igual que ocurre en la "vida real" en la "vida virtual" podemos ser víctimas de cualquier delito cometido a través de Internet, y como víctimas debemos de interponer denuncia ante el Cuerpo Policial o Judicial competente.

- A la denuncia adjuntaremos toda la información que consideremos de interés y que pueda ayudar, en una posible investigación, a identificar al ciberdelincuente: documentación, correos electrónicos, conversaciones de mensajería instantánea, páginas webs, etc.

- Esta información deberemos conservarla en formato digital y sin alterarla. Si la imprimimos puede servir a los investigadores como guía, pero las verdaderas pruebas o trazas del delito se van a encontrar en la información "oculta" de los archivos informáticos.

www.gdt.guardiacivil.es

La denuncia telemática (a través de Internet) no es viable actualmente en la legislación española. La denuncia, conforme a nuestra Ley de Enjuiciamiento Criminal *(artículos 265 y 266)* exige la personación del denunciante o su representante legal, en un juzgado o centro policial, donde debe acreditar su identidad.

El Grupo de Delitos Telemáticos de la Guardia Civil, a través su página web, ofrece la posibilidad de rellenar un formulario con todos los datos necesarios que se deben acompañar a la denuncia de un delito telemático (exclusivo para este tipo de delitos). Una vez relleno, nos generará un documento que podremos presentar en la unidad policial que corresponda.

En el *Capítulo VII. Diccionarios,* podréis encontrar un diccionario de terminología relacionada con los delitos telemáticos o informáticos.

2. VIRUS INFORMÁTICOS

Virus informáticos, qué son, cómo se propagan

Como siempre, voy a intentar no utilizar "palabros raros" para procurar que sea una lectura lo más sencilla posible para todo el mundo. (Que me perdonen los que saben, y los técnicos también).

Además de conocimientos y opiniones personales voy a intentar transmitiros una recopilación de información totalmente libre y disponible en Internet, en páginas web, vídeos, etc., por lo que no siempre es sencillo hacer alusión a la fuente de la información.

La temática de la entrada, por su importancia, requiere que no escatimemos a la hora de escribir, podríamos habernos extendido muchísimo más, pero al menos espero que os sirva para tener las cosas un poquito más claras.

Para empezar a hablar de los virus informáticos debemos tener claros algunos conceptos.

- **DEFINICIÓN DE PROGRAMA INFORMÁTICO:** Un **programa informático *(software)*** es un conjunto de instrucciones **(código fuente)** que una vez ejecutadas realizarán una o varias tareas en un ordenador.

- **DEFINICIÓN DE SISTEMA OPERATIVO:** El sistema operativo de un ordenador es el es el *software* encargado de ejercer el control del mismo y coordinar el uso del *hardware* (distintos componentes físicos de un ordenador) entre diferentes programas de aplicación y los diferentes usuarios. Es un administrador de los recursos de *hardware* del sistema. En definitiva el programa "madre" para que un ordenador pueda funcionar correctamente.

- **DEFINICIÓN DE CÓDIGO FUENTE:** El código fuente de un programa informático es un conjunto de líneas de texto que son las instrucciones que debe seguir el ordenador para ejecutar dicho programa.

Una vez que vamos teniendo claro qué es un programa informático podemos empezar a hablar de los virus informáticos.

¿QUÉ SON LOS VIRUS INFORMÁTICOS?

Un **virus informático,** es un programa malicioso *(malware)* que puede infectar a otros programas o sistemas operativos, modificándolos, borrándolos o simplemente dañándolos, pudiendo afectar en mayor o menor medida al funcionamiento y la propia seguridad de nuestro ordenador y lo que en él tenemos almacenado.

La infección consiste en incrustar su código malicioso dentro del propio código fuente del programa "víctima" o del archivo que se va a utilizar para infectar (normalmente un archivo ejecutable, los que tienen la extensión "exe") de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección.

Como los virus humanos, los virus de ordenador pueden propagarse. Algunos virus solo causan efectos ligeramente molestos mientras que otros pueden dañar tu ordenador, tus programas o la información que en ellos guardas.

Casi todos los virus se unen a un fichero ejecutable, lo que significa que el virus puede estar en tu ordenador pero no puede infectarlo a menos que ejecutes o abras el programa infectado. Es importante observar que un virus no puede continuar su propagación sin la acción humana, por ejemplo ejecutando un programa infectado.

La gente contribuye a la propagación de los virus, muchas veces sin saberlo, al compartir archivos infectados o al enviar *e-mails* con virus como archivo adjunto en el *e-mail.*

Los virus se propagan más rápido de lo que se tarda en solucionarlo, incluso para las propias compañías que proveen de programas antivirus.

DIFERENTES TIPOS DE *MALWARE*

A la hora de hablar de **virus de ordenador** la mayoría de la gente se refiere equivocadamente a los gusanos y a los caballos de Troya como si fueran virus.

Aunque los términos troyano, gusano y virus se utilizan a menudo alternativamente, no son iguales. **Los virus, los gusanos y los caballos de Troya son programas malévolos que pueden causar daño a tu ordenador,** pero hay diferencias entre los tres, y saber esas diferencias puede ayudarte a proteger mejor tu ordenador contra sus efectos, a menudo, muy perjudiciales. Ya hemos visto al principio de este documento la definición de virus pero que son los:

- **Gusanos:** un ***worm*** o **gusano informático** es similar a un virus por su diseño y es considerado una subclase de virus. Los gusanos informáticos se propagan de ordenador a ordenador, pero a diferencia de un virus, tiene la **capacidad a propagarse sin la ayuda de una persona.**

  - **Lo más peligroso de ellos** es su capacidad para replicarse en tu sistema, por lo que tu ordenador podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador enorme.

- **Troyanos:** un **troyano informático, caballo de Troya** o ***Trojan Horse,*** está tan lleno de artimañas como lo estaba el mitológico caballo de Troya del que se ha tomado el nombre.

  - A primera vista el troyano parece ser un programa útil, pero en realidad hará daño una vez instalado o ejecutado en tu ordenador. Los que reciben un troyano normalmente son engañados para abrirlos porque creen que han recibido un programa legítimo o archivos de procedencia segura.

  - Cuando se activa un troyano en tu ordenador, los resultados pueden variar. Algunos troyanos se diseñan para ser más molestos que malévolos (como cambiar tu escritorio agregando iconos de escritorio activos tontos), mientras que otros pueden causar daño serio, suprimiendo archivos y destruyendo información de tu sistema.

  - También se conoce a los troyanos por crear **puertas traseras** o ***backdoors*** en tu ordenador permitiendo el acceso de otros usuarios a tu sistema, accediendo a tu información confidencial o personal.

¿CÓMO FUNCIONA UN VIRUS?

Cuando un virus lleva a cabo la acción para la que había sido creado, se dice que se ejecuta la carga. Pueden ser bastante maliciosos e intentan producir un daño irreparable al ordenador personal destrozando archivos, desplazando/sobrescribiendo el sector de arranque principal, borrando los contenidos del disco duro o incluso escribiendo sobre la **BIOS (instrucciones más elementales para que**

puedan funcionar un ordenador) dejando inutilizable el equipo. La mayoría de los virus no borran todos los archivos del disco duro. La razón de esto es que una vez que el disco duro se borra, se eliminará el virus, terminando así el problema.

- Un virus se inicia como cualquier programa informático, pero al estar escondido generalmente dentro de otro programa el virus se ejecuta cuando "arrancamos" el programa infectado, en la mayoría de las ocasiones sin ser conscientes de que lo hacemos.
- El código del virus queda presente en la memoria de nuestro ordenador (RAM), estando presente incluso después de finalizar el programa que lo "escondía".
- El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, los archivos ejecutables (.exe., .com, .scr, etc.) que sean llamados para su ejecución.
- Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

Algunos virus tienen una carga retrasada que a veces se llama bomba. Por ejemplo, un virus puede exhibir un mensaje en un día o esperar un tiempo específico hasta que ha infectado cierto número de hospedadores. Sin embargo, el efecto más negativo de los virus es su auto reproducción incontrolada, que sobrecarga todos los recursos del ordenador.

¿CÓMO SE TRANSMITEN LOS VIRUS?

La inserción del virus en un programa se llama infección, y el código infectado del archivo (o ejecutable que no es parte de un archivo) se llama hospedador *(host).*

Los virus se reproducen al infectar "aplicaciones huésped". Esto significa que copian una parte del código ejecutable en un programa existente. Los virus se programan de tal manera para no infectar el mismo archivo muchas veces y asegurarse de que funcionan como se espera. Para hacerlo, incluyen una serie de *bytes* en la aplicación infectada, los cuales verifican si ya ha se ha producido la infección. Esto se denomina **firma de virus.**

Hasta no hace mucho la principal vía de infección eran las propias vulnerabilidades de los sistemas operativos, las cuales siguen existiendo, pero hoy en día la principal vía de infección es la propia navegación o bien por las vulnerabilidades de los distintos navegadores o simplemente por el "descuido" de los mismos usuarios.

La forma más común en que se transmiten los virus es por transferencia de archivos, descarga o ejecución de archivos adjuntos a correos. También pueden encontrarse simplemente visitando ciertos tipos de páginas web que utilizan un componente llamado ActiveX o Java Applet. O siplemente podemos ser infectados leyendo un *e-mail.*

Las principales vías de infección son:

- Redes sociales
- Sitios webs fraudulentos
- Redes P2P ***(descargas con regalo)***
- Dispositivos USB/CDs/DVDs infectados
- Sitios webs legítimos pero infectados
- Adjuntos en correos no solicitados *(spam)*
- Copias de programas ***(con regalo como en el P2P)***
- Fallos de seguridad de los propios sistemas operativos

¿Ya tenemos claros los conceptos sobre los bichitos informáticos? Pues ahora nos toca utilizar la lógica para evitar infectarnos. Sin olvidarnos que podemos utilizar ciertos programas antivirus y *antimalware* para intentar protegernos de ellos.

Virus informáticos, ¿cómo protegernos?

¿QUÉ ES UN ANTIVIRUS?

Un antivirus es un programa encargado de detectar y eliminar posibles amenazas en nuestro ordenador y que cuenta generalmente con una lista de virus conocidos y formas de reconocerlos (llamadas firmas), por lo que un antivirus se encargará de comparar esas firmas con los archivos enviados y recibidos y de detectar si alguno de ellos puede poner en peligro nuestro equipo informático.

Existen varios métodos de "desinfección":

- Eliminación del código en el archivo infectado que corresponde al virus.
- Eliminación del archivo infectado.
- Puesta en cuarentena del archivo infectado, lo cual implica su traslado a un lugar donde no pueda ejecutarse.

¿CÓMO FUNCIONA UN ANTIVIRUS?

Un antivirus realiza varias funciones para proteger nuestro ordenador que podemos clasificar en:

- **Función de búsqueda de las firmas de virus conocidos:** escanean el disco duro en busca de virus específicos, de encontrarlo lo eliminan o lo ponen en cuarentena. Este método solo es fiable si la base de datos del virus del programa antivirus está actualizada e incluye las firmas de todos los virus conocidos, por lo que no cubre la seguridad al 100% al no detectar los nuevos virus o los que no figuran en su base de datos.
- **Función de cuarentena:** esta función aísla permanentemente un archivo potencialmente peligroso. Si el programa lo necesita el antivirus lo restaura y éste vuelve a su lugar original.

- **Función desinfectar:** sirve para eliminar un virus cuando ya está dentro del sistema.
- **Actualizaciones:** continuamente están saliendo nuevos virus.

Algunos antivirus, si tienen la sospecha de que un programa pudiera ser un virus, extraen las firmas del programa sospechoso, su "ADN", y son remitidas al fabricante del antivirus. Si se confirma el positivo, el "nuevo" virus es añadido a la base de datos.

DETECCIÓN DE VIRUS BASÁNDOSE EN LA HEURÍSTICA

Aunque el término heurística parezca un "palabro" tiene una sencilla explicación.

Los nuevos antivirus, así como otro tipo de programas específicos, usan otra forma de detección de virus llamada detección proactiva, que consiste en detectar virus no comparándolos con una base de datos sino detectándolos por sus comportamientos, esto permite detectar amenazas antes de que hayan podido ser añadidas a una base de datos.

Para detectar la presencia del *malware* no "controlado", el programa antivirus estudia las acciones que pretende realizar el archivo sospechoso, avisando al usuario de la acción al estar catalogada como una acción típica en el funcionamiento rutinario de cualquier *malware*, como por ejemplo:

- Que un archivo pretenda unirse a un programa instalado en el ordenador.
- Que intente modificar cualquier archivo esencial del sistema operativo.
- Que su finalidad sea renombrar carpetas o archivos.
- Que accione la aparición de ventanas emergentes *(pop-ups)* con información no solicitada.
- Que su ejecución envíe al usuario a sitios web no solicitados.

¿CUÁL ES LA MEJOR PROTECCIÓN CONTRA LOS VIRUS INFORMÁTICOS?

Una vez teniendo claros los conceptos de virus informáticos, programas antivirus y formas de detección de virus, es hora de ver cuál es la mejor forma de protegernos.

Recapitulemos:

- Sabemos que un virus informático es un "programa" que puede estar incluido en otro programa para infectar nuestros equipos.
- Sabemos que un antivirus es un programa informático.
- Sabemos que la seguridad de los antivirus no es plena al no detectar los virus no conocidos.
- Sabemos que existen otra forma de detectar virus no conocidos basándonos en comportamientos anómalos de archivos potencialmente sospechosos.

Así pues, ya sabiendo el funcionamiento de los virus y de las herramientas que disponemos para protegernos, podemos decir que l**a mejor forma de protegernos es** siguiendo las siguientes normas:

Mantener los programas y el sistema operativo actualizados.

Tener un antivirus actualizado instalado en nuestro ordenador y que este antivirus, como programa informático que es, tenga un origen conocido, no sea una descarga de cualquier programa de intercambio o que me lo haya dejado un amigo que se lo ha descargado. Recuerda cómo se extienden los virus.

Además disponer de otros programas ***antimalware, antispyware*** que detecten los comportamientos rutinarios de un virus que al no estar "fichado" no lo detecta nuestro antivirus.

No descuidarnos a la hora de compartir archivos, mediante descargas en Internet **(P2P)** o por soportes informáticos (discos duros externos, *pendrives*, tarjetas de memoria, etc.) y realizar un escaneo siempre de todos los que vayamos a utilizar en nuestro equipo y no hayan sido controlados previamente por nosotros, no confiando en los correos electrónicos desconocidos y con archivos adjuntos ejecutables.

Los mensajes de nuestros contactos en mensajería instantánea también nos pueden traer *links* a *malware* al estar el remitente infectado.

Evitar el usuario "administrador" para el uso general del sistema, ya que no suele ser necesario.

Prestad atención cuando se navega por Internet, evitando aceptar la descarga de archivos de origen dudoso o que ofrecen soluciones de seguridad falsas.

Ahora sí, ya toca decirlo:

Siempre tenéis que emplear la lógica y recordar que vosotros mismos sois vuestra peor vulnerabilidad, pero también sois vuestro mejor antivirus.

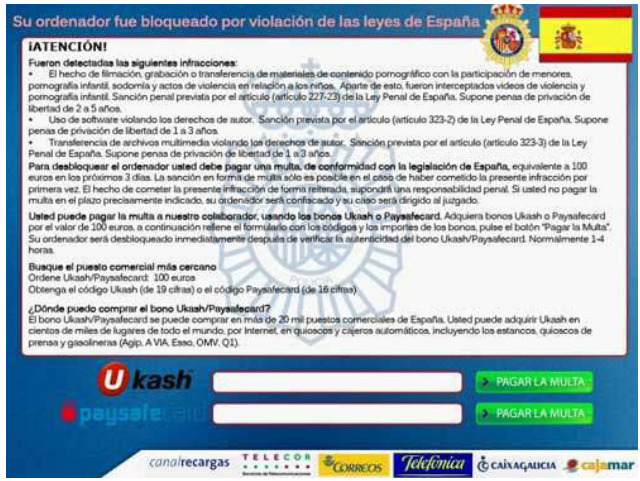
Historia de un virus: "El virus de la Policía"

RANSOMWARE. SU HISTORIA

Ya hace tiempo que tuvimos la desgracia de conocer al que fue denominado en *El Blog de Angelucho* como "**El virus Mortadelo"**, en clara alusión al personaje de Francisco Ibáñez y a sus disfraces. Este virus es conocido como "El virus de la Policía", "Virus de la SGAE", "Virus UKASH", "Virus de la Gendarmería Nacional Francesa" e incluso "Virus del FBI".

A nivel mundial han sido muchos los ordenadores que han sido infectados por el conocido virus **Ransomware**[61], que una vez bloqueados tras la infección, sus asustados usuarios no han dudado en efectuar, y sin perder tiempo, el pago electrónico solicitado para conseguir tanto eludir la denuncia del falso cuerpo policial.

[61] **Ransomware** es un tipo de virus informático *(malware)* que se caracteriza por secuestrar el acceso al sistema o archivos a cambio de un pago.



El falso mensaje argumenta que, además, la dirección IP ha sido registrada en las webs ilegales con contenido pornográfico orientadas a la difusión de la pornografía infantil, zoofilia e imágenes de violencia contra menores o temáticas similares.

Jamás llegaron las denuncias con las que amenazaba el mensaje que aparecía en la pantalla, sin embargo sí llegaron las de algún indefenso usuario que, aunque temeroso, sí se atrevió a denunciar los hechos a la verdadera policía de su país, pero el mal ya estaba hecho y casi de forma irreparable.

Lo que sí llegaron son los beneficios a los cibercriminales, según se calcula, las ganancias se han estimado en 33.000 dólares al día que se reembolsaba el cibercriminal que manejaba el *malware*. Imaginaos el "negocio" redondo, y sin moverse de casa.

Según Symantec se han llegado a detectar dieciséis "disfraces" o variantes del Ransomware, todos desarrollados de forma independiente en los dos últimos años. El "bicho" vió la luz en Rusia y Europa del Este, donde se iniciaron los ataques a usuarios de esos países, pero el beneficio era tan grande que terminó extendiéndose por el resto de Europa, España incluida, llegando incluso a Estados Unidos y Canadá.

Este *malware*, el Rasonware, ha sido utilizado por pequeños grupos de ciberdelincuentes, que según se estima han podido llegar a obtener con su actividad más de cinco millones de dólares procedentes de sus víctimas. Víctimas de las que se tiene conocimiento, de las que no se tiene conocimiento…

Al ver la facilidad de uso del *malware,* con riesgo casi cero para el malo, se potenciaron los grupos que de forma indiscriminada comenzaban a experimentar el nuevo "filón de oro" para la ciberdelincuencia.

Esta estimación posiblemente se quede demasiado corta, pero lo que sí quedó de manifiesto en todos los análisis de los investigadores de Symantec es que el número de ordenadores infectados iba *in crescendo* por lo que las cantidades obtenidas de forma fraudulenta podrían considerarse como **¡¡¡INCALCULABLES!!!**

RANSOMWARE: SU *MODUS OPERANDI*

El Ransomware, dentro de sus múltiples "disfraces" y en su versión inicial y más básica, mostraba un pantallazo diciendo que era la policía, incluso personalizando el mensaje al capturar la ubicación geográfica e IP de conexión, aludiendo a la ley de cada país, con el ánimo de hacer más fuerza en el engaño para obtener un éxito asegurado. Tras el pantallazo, el virus desactiva el ordenador.

Estos mensajes harán alusión al FBI si la víctima se encuentra en Estados Unidos, al Cuerpo Nacional de Policía, si se encuentra en España, a la Gendarmería si está en Francia, etc.

El usuario, pensando que es realmente el cuerpo policial quien se pone en contacto por un medio tan "sofisticado", se apresura en pagar una multa para tener su ordenador restaurado e incluso para evitar una posible detención policial.

Todas las víctimas fueron obligadas a pagar sus "multas" a través de un sistema de pago electrónico de prepago que les obligaba a comprar un PIN especial de proveedores como MoneyPak, Paysafecard o Ukash. Ese PIN válido es el objetivo final del defraudador.

Los usuarios se infectan con mayor frecuencia a través de las descargas en sitios web de descarga populares o contendidos "diferentes" , estos sitios web disponen de "programas" insertados en su propio código, en los *banners* publicitarios por ejemplo, que son manipulados por los ciberdelincuentes e infectan los ordenadores de los visitantes.

El pago se requiere en un plazo de setenta y dos horas, plazo en el que si no se ha recibido el pago, se formularía la denuncia, la falsa denuncia. La víctima no tarda en pagar para evitar la vergüenza de ser "descubierto" por su familia consumiendo estos contenidos.

Este PIN de pago será enviado por el Ransomware a un servidor, donde los atacantes lo recuperan y se benefician, dijo el informe de Symantec: "En este momento, los atacantes deben honrar su promesa y enviar un comando al Ransomware diciéndole que se desinstale. Lamentablemente, esto rara vez sucede. En realidad, muchas de las variantes Ransomware ni siquiera contienen el código para desinstalar en sí mismos."

Después, el virus fue mutando, los cibercriminales "más técnicos" mezclaban varios tipos de *malware*. En Estados Unidos, el FBI, detectó una variante denominada **Reveton**[62]**,** que combinaba este virus con un troyano bancario que extraía las credenciales de banca *on-line*, e incorporaba un programa que capturaba todo los que se escribía en el PC, un *keylogger*.

Las últimas variantes del *malware* capturan imágenes de la propia *webcam* de la víctima, mostrándola en el pantallazo de aviso y dando mayor credibilidad todavía al engaño.

[62] **Reveton:** Troyano que modifica la configuración de Internet para conectarse a servidores remotos.

Rogues: los falsos antivirus

Es tiempo de crisis y tenemos que "hilar fino" para que los **"lujos"** de mantener nuestro ordenador seguro no mermen nuestra economía. ¿Por qué pagar treinta euros por un antivirus si hay almas caritativas que no solo nos lo regalan sino que además nos lo envían por *e-mail* o permiten que nos lo descarguemos de las redes P2P?

Si eres uno de los afortunados internautas que han tenido la gran suerte de encontrarse con uno de estos maravillosos antivirus quizás ya no sea necesario que sigas leyendo, porque ya sabes de primera mano lo que son los ***rogues***.

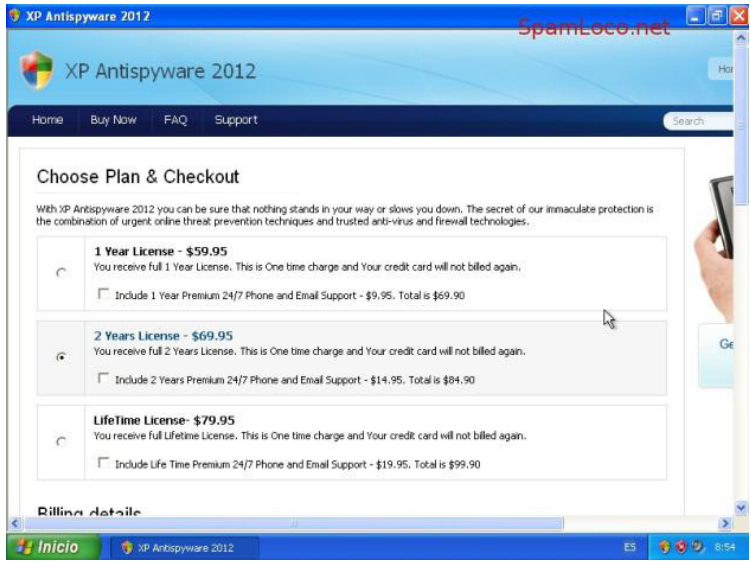
Los *rogues* son un tipo de *malware* que tras la descarga de archivos en las redes P2P para instalar los últimos **códecs**[63] de vídeo, o algún complemento necesario para nuestro navegador o simplemente al navegar por sitios web poco seguros y "recomendables" nos premian con nuevo "inquilino" en nuestro equipo.

La instalación de estos nuevos complementos **genera en nuestro ordenador falsas alertas de virus mediante ventanas emergentes *(pop-ups)*** con las que nuestro propio sistema operativo nos advierte de que se encuentra infectado con el peor de los virus de última generación, pero por suerte en la misma ventana tenemos la solución. Esta no es otra que un *link* de descarga de un súper antivirus potentísimo capaz mitigar la amenaza del virus que nos amenaza.

[63] **Códec** es la abreviatura de codificador-decodificador. Un códec de vídeo es un tipo de códec que permite comprimir y descomprimir vídeo digital.

Una vez instalado el poderoso antivirus nos hace un primer chequeo de nuestro sistema en el que nos confirma la infección del peligroso virus, **en ocasiones incluso nos "aconseja" la desinstalación de nuestro "obsoleto" antivirus.**

Aquí está la estafa, y no es otra que invitarnos a descargar la versión completa del programa de protección **solicitando para ello el pago, por medios "poco seguros", de cierta cantidad de dinero.** Ni que decir tiene que no es un antivirus real y que tanto el análisis como sus resultados son totalmente falsos.



Tenéis que tener en cuenta que, si detectáis que habéis sido víctimas de este tipo de estafa, no basta con desinstalar simplemente el programa, debéis testear vuestro equipo con un antivirus real con el fin de detectar cualquier tipo de *malware* que os haya quedado residente en el PC.

Moraleja: Instalemos solo antivirus y programas de seguridad de empresas conocidas y de confianza descargándolos desde sus páginas oficiales, donde también ofrecen incluso soluciones gratuitas.

Otras vulnerabilidades

¡CUIDADO, QUE NO TE *EXPLOITEN* EL PC!

Al recibir un archivo por cualquier vía y a través de Internet corremos muchos riesgos, el principal es que nuestro equipo se "contamine" con algún virus o que se convierta en la nueva residencia de cualquier tipo de *malware*.

El enviar archivos adjuntos en correos electrónicos mediante *spam*, se ha convertido en una práctica habitual entre los ciberdelincuentes para tumbar nuestras defensas y hacerse con el control de nuestros ordenadores o de nuestra propia seguridad y/o privacidad.

Nuestro ordenador puede verse afectado por el rutinario hecho de abrir un archivo PDF enviado en algún correo, o mediante la ejecución de un archivo Power-

Point que promete el disfrute de unos momentos súper agradables mediante la visualización de maravillosas vistas de playas paradisíacas, hermosos cuerpos o cualquier otro pretexto.

Este tipo de archivos no son maliciosos en sí mismos, sino que son utilizados como "recipiente" que contiene un virus o *malware*, que al ejecutarlo en nuestro ordenador, aprovecha las distintas vulnerabilidades de programas y sistemas operativos no detectadas hasta el momento. Los más utilizados son los que utilizan las vulnerabilidades de Adobe, vulnerabilidades muy populares entre los cibercriminales al ser conscientes de que las aplicaciones como Adobe Reader, Acrobat y Flash Player son utilizadas con frecuencia por los internautas, por lo que aprovechan esta circunstancia para crear los denominados "*exploits* día *zero"* (que explicamos en este mismo artículo), con ellos consiguen ejecutar ese programa oculto en el archivo principal pudiendo afectar nuestra seguridad o privacidad, e incluso convirtiéndonos en el canal de infección de todos nuestros contactos. **¡Fijaos la importancia de mantener nuestros equipos al día!**

Los ciberdelincuentes, para darle mayor grado de éxito a sus acciones, utilizan en sus comunicaciones trampas temáticas de actualidad como desastres que han sucedido recientemente, eventos deportivos como grandes eventos en el mundo del fútbol o la celebración de los Juegos Olímpicos.

Recientemente, y como ejemplo de esto que os cuento, se detectó que circulaba un calendario modificado de las pasadas olimpiadas de Londres en formato PDF, este documento albergaba un *exploit* para explotar vulnerabilidades de Adobe Reader 9 y versiones anteriores.

La traducción de ***exploit*** es: **un programa o código malicioso que "explota" una vulnerabilidad o deficiencia de un sistema operativo, navegador o cualquier otro programa, en beneficio de quien lanzó este tipo de ataque.**

Si bien, el código que explota la vulnerabilidad no es un código malicioso en sí mismo, generalmente se le utiliza para otros fines como permitir el acceso a un sistema o como beneficio de otros *malware* como gusanos y troyanos.

Es decir que actualmente, los *exploits* son utilizados como "componente" de otro *malware* ya que al explotar vulnerabilidades del sistema permite hacer uso de funciones que no estarían permitidas en caso normal.

Este tipo de amenaza pueden tomar muchas formas diferentes (descargas forzadas, instalación de códigos maliciosos ocultos, infecciones silenciosas o automatizadas) pero todas tienen el mismo resultado: el ordenador se infecta sin que sea necesario hacer nada especial como por ejemplo descargar un archivo.

Los *exploits* permiten que los códigos maliciosos se instalen silenciosamente en el sistema, sin el conocimiento del usuario. Esto puede tener como consecuencia el robo de información, el mal funcionamiento del ordenador y otros problemas serios.

Es por ello que siempre es recomendable actualizar las aplicaciones y evitar abrir documentos de origen desconocido.

La perfección no existe y menos en seguridad en la Red, teniendo en cuenta que siempre podemos estar expuestos a un "DÍA CERO" *(ZERO DAY)*, que es como se denomina a **cualquier amenaza desde que el *malware* nace hasta que se incorpora a las bases de datos de los antivirus,** o dicho de otra forma, es como se denomina a las vulnerabilidades que tienen los programas y, que en el momento de ser descubiertas, no tienen parche o solución por parte del fabricante

Este es el espacio de tiempo crítico para nuestra seguridad en la Red pero como siempre podemos mitigar el peligro empleando la lógica para no facilitar la labor de los "malos malotes".

¡CUIDADO CON LOS CÓDIGOS QR!

La cantidad de *malware* dirigido a dispositivos móviles aumentó considerablemente el 2011, principalmente las amenazas se identifican como troyanos en SMS, códigos QR y programas maliciosos que suelen estar embebidos en aplicaciones de teléfonos inteligentes.

Un código **QR** (*Quick Response Barcode* o "código de barras de respuesta rápida") es un sistema para almacenar información en una matriz de puntos o un código de barras bidimensional.

Los códigos QR son fácilmente identificables por su forma cuadrada y por los tres cuadros ubicados en las esquinas superiores e inferior izquierda.

El auge del los códigos QR, sobre todo en el ámbito publicitario, trae consigo la aparición de nuevas opciones de vulnerar nuestra seguridad y sobre todo "atacar" directamente a nuestro bolsillo.

Los códigos QR ofrecen la posibilidad de interactuar con las publicidades que encontramos en comercios, en la calle, con la única condición de disponer de un *smartphone* capaz de leer el QR.

¿Qué pasaría si un QR original esconde otro QR malintencionado creado por un ciberdelincuente?

Una persona que pasea tranquilamente por la calle, no se daría cuenta, apuntaría al código QR, su *software* de lectura QR le diría que quiere acceder a una página de web pero en realidad le daría acceso a la aplicación maliciosa alojada en la Red.

Kaspersky Lab descubrió que una web rusa tenía un código QR malicioso que al ser escaneado, descargaba una aplicación automáticamente que producía una estafa para el usuario sin necesidad de que este tuviera que autorizar ningún pago.

La descarga parecía ser de un programa de chat, pero en realidad, la aplicación enviaba mensajes de texto SMS Premium con un alto coste, estableciendo como beneficiario el propietario del troyano.

Seguramente, con la invasión en el mercado de la telefonía móvil de *smartphones* con acceso a Internet, el uso de los códigos QR se implantará cada vez más entre nosotros, generando un nuevo riesgo a tener en cuenta cuando utilicemos nuestro teléfono móvil.

Tener securizados nuestros terminales evitará más de un problema y nos permitirá protegernos ante este tipo de amenazas.

3. EL *SPAM* O CORREO BASURA

En una comida familiar surgió como temática de conversación los peligros de la Red, los miedos ante lo desconocido en Internet y los problemas que nos podría producir la falta de medidas de protección en la Internet.

El primer punto de conversación se centró en una de las principales vulnerabilidades a las que nos enfrentamos si no tomamos las medidas necesarias para protegernos, y es sobre la ingente cantidad de correos basura que recibimos. Y de eso va a tratar esta entrada como pequeña explicación al problema.

Todos los usuarios de correo electrónico recibimos a diario varios mensajes publicitarios que no solicitamos sobre cosas que no nos interesan.

Llamamos *spam* al correo basura, en definitiva, a los mensajes no solicitados. Normalmente estos correos ofrecen productos y por ello son campañas que se lanzan de forma masiva llegando a molestar a los destinatarios que no han solicitado esos mensajes.

Generalmente estos *e-mails* contienen promociones, fotos, información falsa y archivos enormes que en la mayoría de los casos son virus que afectan a nuestros ordenadores.

El correo basura también puede tener como objetivo la telefonía móvil mediante mensajes de texto, a través del novedoso Whatsapp o cualquier otra forma de mensajería instantánea.

¿Cómo funciona? ¿Cómo se distribuye?

Los *spammers* (personas que lanzan el *spam*, normalmente con ánimo de lucro) tratan de conseguir el mayor número posible de direcciones de correo electrónico válidas, es decir, realmente utilizadas por usuarios. Con este objeto, utilizan distintas técnicas, algunas de ellas altamente sofisticadas:

- Listas de correo: el *spammer* se da de alta en la lista de correo, y anota las direcciones del resto de miembros.
- Compra de bases de datos de usuarios a particulares o empresas: aunque este tipo de actividad es ilegal, en la práctica se realiza, y hay un mercado subyacente.

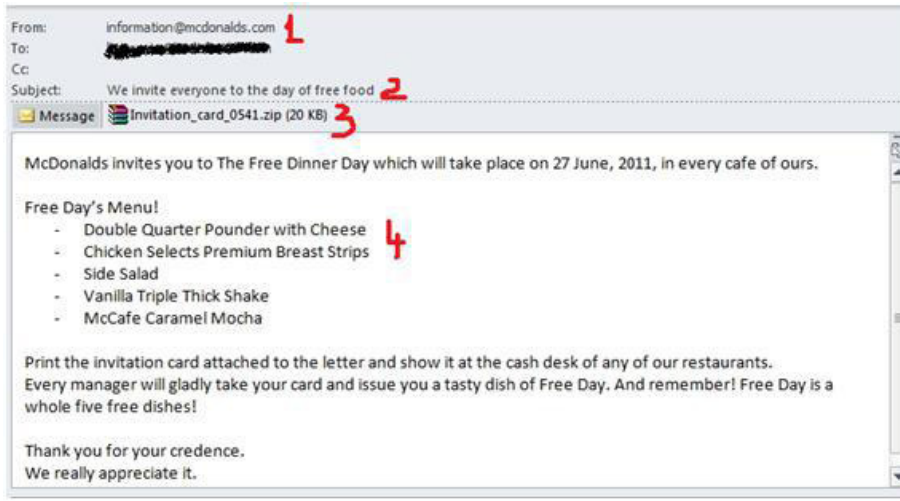
- Uso de robots (programas automáticos), que recorren Internet en busca de direcciones en páginas web, grupos de noticias, *weblogs,* etc.

¿Cómo detectar *spam?*

Algunos ejemplos de *spam* pudieran ser:

- "Gane millones trabajando desde casa."
- "Dieta milagrosa. Pierda 10 kilos en una semana."
- "Chicas XXX ardientes te están esperando."

Pero si tenemos dudas de que pudiera tratarse de un correo *spam*, y abrimos el mensaje, podríamos intentar descubrir si realmente se trata de un correo basura detectando los típicos identificadores de *spam* rápidamente con el siguiente ejemplo:



1. ***From* (remitente):** verifiquemos quién nos envía el mensaje. En ocasiones son compañías inexistentes o la persona que nos envía el mensaje es un desconocido para nosotros. En la mayoría de los casos es el principal identificador de *spam.* El *spam* puede ser tan real que en ocasiones puede imitar a un servicio o usuario real. Por ejemplo, el *spam* puede adoptar una cuenta falsa como administrador@empresa.com o en ocasiones su propio *e-mail.*

2. Observemos el ***subject*** **(asunto).** En ocasiones es engañoso y se usa mayormente para captar nuestra atención.

3. **Archivos.** No abrir ningún archivo o documento que incluya el *spam.* En el ejemplo anterior el archivo adjunto "invitación_card_0541.zip" podría tener algún virus o programa malicioso al instalarlo en nuestro ordenador computadora.

4. **El mensaje del *spam.*** Normalmente está en un lenguaje diferente al nuestro. Si leemos el mensaje cuidadosamente podremos encontrar errores y contradicciones. En el ejemplo anterior lo más probable es que no conozcamos al remitente por lo que resulta sospechoso el recibir una invitación por su parte. En ocasiones, el correo acompaña un enlace que nos lleva a otras páginas fraudulentas que no tienen nada que ver con el mensaje principal, sino para ofrecernos algún tipo de promoción o en ocasiones podrían activar algún programa malicioso.

Recomendaciones para evitar el *spam*

1. **No enviar mensajes en cadena** ya que los mismos generalmente son algún tipo de engaño *(ver artículo sobre los HOAX).*

2. Si aún así se deseara enviar mensajes a muchos destinatarios **hacerlo siempre Con Copia Oculta (CCO)**, ya que esto evita que un destinatario vea (robe) el *e-mail* de los demás destinatarios.

3. **No publicar una dirección privada en sitios webs,** foros, conversaciones *on-line*, etc. ya que solo facilita la obtención de las mismas a los *spammers* (personas que envían *spam*).

4. **Si se desea navegar o registrarse en sitios de baja confianza hágalo con cuentas de *e-mails* destinadas para ese fin.** Algunos servicios de *webmail* disponen de esta funcionalidad: protegemos nuestra dirección de *e-mail* mientras podemos publicar otra cuenta y administrar ambas desde el mismo lugar.

5. Para el mismo fin también es recomendable **utilizar cuentas de correos temporales** y descartables.

6. **Nunca responder este tipo de mensajes ya que con esto solo estamos confirmando nuestra dirección de *e-mail*** y solo lograremos recibir más correo basura.

7. **Es bueno tener más de una cuenta de correo** (al menos dos o tres): una cuenta laboral que solo sea utilizada para este fin, una personal y la otra para contacto público o de distribución masiva.

8. **Cuando recibamos un correo que detectemos como *spam* podemos reportarlo como tal** en nuestro gestor de correo para que en un siguiente envío lo detecte y evitarnos sustos innecesarios.

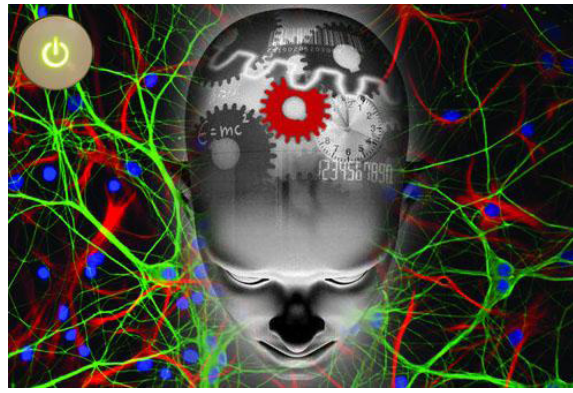
A vosotros, que os reconocéis como participantes de la conversación que da pie a este artículo, y a todos los lectores en general, deciros que efectivamente son muchos los peligros que nos acechan en la Red pero sin ningún lugar a duda, son muchas más las bondades que nos brinda Internet y para disfrutar de ellas simplemente tenemos que emplear la lógica como lo haríamos en la vida "real" para disfrutar de una navegación más segura.

Y como siempre, recordad que nosotros somos nuestra peor vulnerabilidad, pero también nuestro mejor antivirus.

4. INGENIERÍA SOCIAL: EL *HACKING* HUMANO

"Solo hay dos cosas infinitas: el universo y la estupidez humana. Y no estoy tan seguro de la primera…"

Albert Einstein



En este apartado os voy a presentar, lo que en mi opinión es, **el mayor "agujero" de seguridad que podemos encontrarnos en Internet.** Es algo que os vengo diciendo siempre al finalizar mis artículos: **"Nosotros somos nuestra peor vulnerabilidad, pero también somos nuestro mejor antivirus".** En esta ocasión os voy a hablar de **LA INGENIERÍA SOCIAL.**

Si hasta ahora hemos sido "poco técnicos" a lo largo del libro, en este artículo lo vamos a ser menos todavía, puesto que además, como es costumbre, vamos a abordar el tema con un lenguaje lo más sencillo posible para que sea comprensible para todos los lectores.

Como sabéis los contenidos de este libro siempre están encaminados a la seguridad en la Red por parte de cualquier tipo de usuario, pero esencialmente para los más vulnerables. Muchos pensaréis que los más vulnerables son los menores y adolescentes, y ciertamente lo son, porque es sabido que las consecuencias de su vulnerabilidad pueden llegar a ser nefastas y que, como ya vimos en entradas anteriores, los ciberdepredadores utilizan la ingeniería social para acceder a la información de los menores. Pero en este caso no me refiero únicamente a ellos. Vulnerables en Internet podemos llegar a serlo todos, incluso los más preparados técnicamente, porque todos podemos ser víctimas de técnicas de ingeniería social si no prestamos la suficiente atención.

La ingeniería social no es algo nuevo, como casi ninguna de las actividades delictivas llevadas a cabo por ciberdelincuentes. Las estafas mediante las llamadas "cartas nigerianas" ya pretendían beneficiarse de nuestra inocencia llegando a nuestros buzones postales antes de la existencia de Internet, de todos es conocido el llamado "timo de la estampita" que popularizó la actriz Lina Moran en la película *La llamaban La Madrina* en la que demostraba cómo se llevaba a efecto este timo. Pues bien, estas "estrategias" de engaño simplemente utilizan ahora las nuevas tecnologías.

Según **Wikipedia**[64]: **"Ingeniería social** es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos".

Mi traducción es que la ingeniería social es el arte de manipular a la gente para que haga lo que uno quiere, tal como dar contraseñas e información relativa a su privacidad, seguridad, del lugar donde trabaja o de cualquier sistema informático o Red.

¿Qué es la ingeniería social?

El lobo con piel de cordero. Para empezar deciros que en la ingeniería social entra en juego, únicamente, la capacidad humana para engañar a otros individuos, equiparable a un caballo de Troya como citan en **Hackstory**[65] en el artículo de **Mercè Molist**[66] sobre el tema.

Podría decirse que la ingeniería social es un conjunto de acciones y técnicas que influyen en la conducta de las personas y están dirigidas para conseguir información sobre ellas. Es una práctica estrechamente relacionada con la comunicación entre las personas y que algunos llegan a definir como el arte de conseguir de un tercero cualquier dato que pudiera ser utilizado por un atacante.

El objetivo de "el ingeniero social" es ganarse la confianza de la otra persona con el único fin de engañarla y/o manipularla mediante técnicas de persuasión. Su secreto no es preguntar, realmente, sino la forma de hacer la pregunta, en de-

[64] **Wikipedia** es una enciclopedia libre y políglota de la Fundación Wikimedia (una organización sin ánimo de lucro). Sus más de 20 millones de artículos en 282 idiomas y dialectos han sido redactados conjuntamente por voluntarios de todo el mundo y prácticamente cualquier persona con acceso al proyecto puede editarlos.

[65] **Hackstory** es una web, gestionada por la periodista Mercè Molist, y en la que se cuenta la historia del *hacking* presentando al *hacker* como especialista en seguridad informática y no como un ciberdelincuente.

[66] **Mercè Molist Ferrer** es una periodista especializada en Internet, comunidades virtuales y seguridad informática. Colabora en el suplemento sobre tecnología e Internet de *El País* desde sus inicios; escribió también en la ya extinta revista *Web* y en *@rroba.*

finitiva podría definirse como **"yo te digo lo que tú quieres oír y tú me cuentas lo que yo quiero saber".**

Un ejemplo de ingeniería social podría ser (algo que intentaron realmente conmigo y que es tan común últimamente generalmente por competencia desleal entre empresas de telefonía) mediante una llamada telefónica; alguien se hace pasar por nuestra compañía telefónica, nos pregunta si estamos contentos con el servicio recibido y nos dice que confirmemos nuestro domicilio para verificar que están hablando realmente con el titular de la línea. Llegan a decirnos que para comprobar que son quienes realmente dicen no tenemos más que darles el número de nuestro DNI y ellos nos contestarán con la letra del mismo (esta letra se obtiene simplemente con una fórmula que asocia y relaciona el número del DNI o NIF con la letra a través de la suma de los diferentes dígitos que contiene) o sea, algo que todos podríamos hacer con esa fórmula. Pues con este tipo de artimañas pueden llegar, y de hecho lo hacen, a conseguir toda nuestra información, incluso nuestra información bancaria.

El éxito de este tipo de técnicas, que como veis no tienen mucho que ver con la informática, se refuerza con el aprovechamiento de las "vulnerabilidades humanas", y me refiero a la curiosidad, a la inocencia, a la ambición, a la confianza, y sobre todo, al desconocimiento.

Si hablamos de ingeniería social estamos obligados a hablar de uno de los ingenieros sociales más famosos de los últimos tiempos, **Kevin Mitnick** (conocido como **"El Condor".** Sus "hazañas" lo llevaron a ser calificado por algunos como el *hacker* más famoso del mundo o incluso, como el más peligroso y más buscado por el FBI) y quien asegura que la ingeniería social se basa en estos cuatro principios:

1. Todos queremos ayudar.

2. El primer movimiento es siempre de confianza hacia el otro.

3. No nos gusta decir no.

4. A todos nos gusta que nos alaben.

El bien y el mal de la ingeniería social

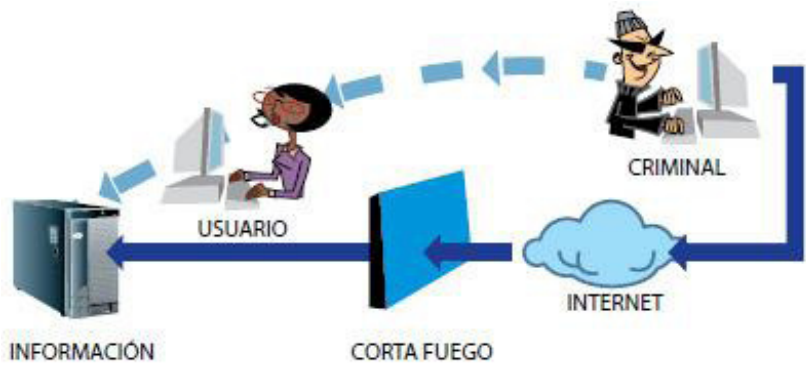
La ingeniería social suele ser utilizada para hacer el mal en la Red y conseguir, con estas técnicas, información sensible de otros usuarios, pero no siempre es así, también puede ser utilizada para el bien, es más, normalmente así lo hacemos, utilizamos ciertos "truquillos" de ingeniería social para hacer cosas buenas.

Un buen ingeniero social no persigue engañar directamente a las fuentes de información que son objeto de tal, sino que simplemente se realiza una tarea de manera encubierta, por lo que esto no implica directamente mentir a una persona, por ejemplo. Es por eso que resulta menos evidente su detección.

Al igual que existe el uso de la ingeniería social para la obtención de información que podría ser usada para perjudicar a aquellas personas que la facilitaron, también existe la cara "B". La ingeniería social puede ayudar a realizar acciones, que, de manera encubierta, beneficien a las personas que facilitan la información para que estas acciones tomen lugar. Valga de ejemplo la manipulación que sufrimos por parte de familiares, cuando en nuestro día de cumpleaños, de manera encubierta nos hacen visitar un sitio determinado para posteriormente, encontrarnos con nuestros amig@s, que nos esperan para la celebración.

¿Qué tiene que ver la ingeniería social con la seguridad en Internet?

Nuestros sistemas informáticos pueden disponer de los antivirus más potentes y tener instalados los mejores cortafuegos, además podemos disponer del mejor sistema de encriptación para nuestra información confidencial y privada, pero todo eso no sirve de nada si no aseguramos la "puerta de entrada" a todo, me refiero a nosotros mismos, al usuario del sistema.



El principio que sustenta la ingeniería social es el que en cualquier sistema **"los usuarios son el eslabón débil"** y en Internet no va a ser diferente.

El principal objetivo de la seguridad informática es asegurar los datos que guardan nuestros ordenadores o sistemas informáticos, ya sean privados o profesionales y que éstos permanezcan alejados de cualquier "intruso" en nuestro sistema.

En cuanto a la seguridad de la información en empresas hay que tener en cuenta que una gran parte de las intrusiones en los sistemas informáticos se realizan utilizando datos que se obtienen de sus usuarios mediante diferentes métodos y con la intervención de personas especialmente entrenadas, los ingenieros sociales.

En la Red, un "ingeniero social" puede hacerse pasar por nuestro banco, por alguien a quien incluso podríamos conocer en realidad, un compañero de trabajo, un cliente, alguien a quien podríamos revelar alguna de nuestras confidencias.

Seguro que muchos habréis recibido correos electrónicos en los que se os comunicaba que vuestro banco había sufrido algún tipo de problema y por ello surgía la necesidad de que accedieses con vuestras credenciales para subsanar y enmendar el fallo, por supuesto os facilitan el acceso mediante un acceso directo a vuestra banca *on-line*, ni que decir tiene que no es la real, es una copia casi exacta del banco real. Incluso en ocasiones recibís ese correo sin ser usuarios de esa entidad bancaria.

En todos los casos se sigue una misma pauta: **la posibilidad de alcanzar algo deseable** (acceso a datos confidenciales, conseguir dinero, evitar la desconexión del teléfono, etc.)

Otros casos reales podrían ser:

- Una página web o programa que nos proporciona el historial de conversaciones de nuestros contactos, o simplemente quién nos ha suprimido como contactos de nuestro cliente de mensajería preferido. Para obtener esta información solo tenemos que acceder a dicha web con nuestro usuario y *password*. *Et voilà!!!*

- Un banco nos dice que hemos recibido una cierta cantidad de dinero y para poder disponer de ese dinero debemos acceder a una página web con nuestras credenciales bancarias. *Et voilà!!!*

- Nos ha tocado la lotería (aunque no hayamos jugado) somos multimillonarios y para hacerlo realidad solo tenemos que pagar, en concepto de tasas, una insignificante cantidad de dinero en comparación con el premio. *Et voilà!!!*

Pues bien, estas acciones aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, en este caso de la inocencia y credulidad del internauta.

Este "arte de engañar" puede ser utilizado por cualquiera, normalmente por creadores de *malware* y ciberdelincuentes que buscan que un usuario revele su contraseña de acceso a un determinado sistema o cualquier otro tipo de información sensible.

¿Cómo podemos evitar ser víctimas de ingeniería social?

Simplemente tenemos que "analizar" la situación, no es necesario ser expertos en nada, solo debemos hacernos algunas preguntas lógicas como si nuestro banco se pondría en contacto con nosotros de esa manera o el motivo de que nos toque un premio de la lotería si no hemos jugado.

En resumidas cuentas, las mejores herramientas para protegerse de los ataques de ingeniería social son:

- **El sentido común y la lógica**
- **La educación**
- **La información**

Identificar los ataques de ingeniería social es primordial para poder disfrutar de Internet de forma más segura, por eso os pongo unos pequeños consejos:

- **Nunca revelar mediante *e-mail* o cualquier otro medio de comunicación nuestros datos personales** (como claves de acceso, números de tarjetas de crédito, cuentas bancarias, etc.).
- **Prestaremos atención a los enlaces que nos lleguen de correos electrónicos que no sean de nuestra confianza y nos soliciten información personal y privada.**

- Como se suele decir nadie regala duros a pesetas, por lo que deberemos **desconfiar de cualquier tipo de comunicación en la que nos ofrezcan la posibilidad de ganar dinero con facilidad.**

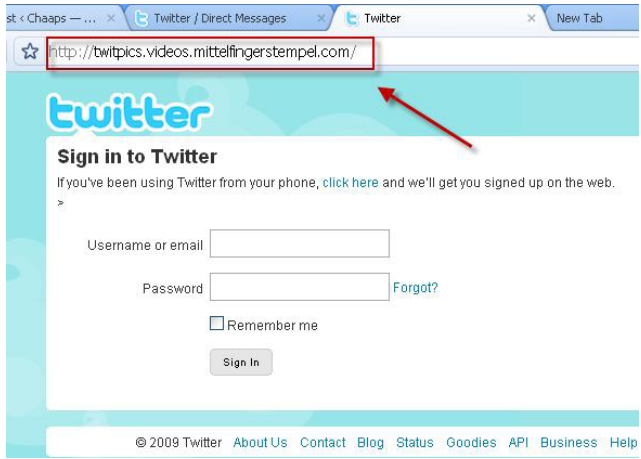
- **Cuando accedamos a nuestro sistema de banca *on-line* deberemos verificar que estamos haciéndolo en la página correcta y no en una página simulada o copiada, normalmente accederemos mediante "http"** (Hypertext Transfer Protocol Secure, que es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en la WWW, generalmente para transacciones bancarias o de pagos o cada vez que se intercambie información sensible en Internet).

5. EL *PHISHING:* ROBOS POR INTERNET

El ***phishing*** o robo de identidad es un tipo de ingeniería social que intenta conseguir, mediante engaños, datos personales del usuario, ya sean datos bancarios, números de tarjeta de crédito, contraseñas, datos de cuenta u otro tipo de información.

Los autores de estos fraudes son unos artistas del engaño, con conocimientos técnicos informáticos elevados, utilizan el envío masivo de mensajes de cualquier tipo y de forma indiscriminada llegando a miles de destinatarios *(spam),* utilizando como cebo mensajes u ofertas atrayentes para pescar a sus víctima, por ello el nombre *phishing* del inglés **'pescar'**. Mediante el engaño, redireccionan a las víctimas a sitios web falsos que emulan páginas webs reales (banca *on-line*, redes sociales, *webmail*, etc.) utilizando mensajes de correo electrónico falsos, SMS e incluso, últimamente, mensajería tipo WhatsApp. Normalmente piden que hay que ingresar nuestros datos bancarios para actualizarlos o que debemos reiniciar nuestras credenciales tras un problema técnico en los servidores, o realizar cualquier transacción en la que se necesita una lógica comprobación del usuario o simplemente que debemos acceder a un nuevo servicio para beneficiarnos de cualquier oferta.

El enlace que nos facilitan emulando la página web verdadera, aunque parezca que apunta al servidor real, redirige hacia otro servidor controlado por el atacante que simula al verdadero, normalmente imitando su diseño y contenido, y los datos que introduzcamos serán enviados al *phisher*, al cibercriminal.



En la imagen se puede comprobar como el *link* no dirige a la verdadera página web de Twitter.

¿Qué buscan?

La finalidad principal del *phishing* es obtener nuestras credenciales bancarias o datos personales, que son utilizados posteriormente para la comisión de distintas fechorías, en las que nos convertimos en víctimas fáciles si no ponemos las medidas de seguridad adecuadas para evitar el engaño.

Los datos personales utilizados los emplean para acceder con nuestra propia identidad:

- En nuestras cuentas de correo, para continuar la cadena de envíos a nuestros contactos o para envíos de correos desde nuestra identidad con fines…
- En nuestros perfiles en redes sociales, para hacerse pasar por nosotros con fines…
- En nuestros servicios de banca *on-line,* la verdad que aquí no sé el fin que persiguen :'(€€€€€€€
- Para abrir nuevas cuentas en nuestro nombre.

- Para obtener documentos oficiales mediante el uso de nuestra identidad.

¿Cómo podemos detectar este tipo de mensajes?

- Los *phishers* (pescadores) pueden simular ser empresas legítimas y utilizan correos electrónicos que también simulan a la empresa "clonada" para solicitar información personal e inducir a los destinatarios a responder a través de sitios web maliciosos.
- Los *phishers* utilizan el engaño para tentar a los destinatarios a responder.
- Los sitios de robo de identidad parecen sitios legítimos, ya que tienden a utilizar las imágenes de *copyright* de los sitios legítimos.
- Las solicitudes de información confidencial por correo electrónico o mensajería instantánea, por lo general, no son legítimas.
- Pueden pedir que realice una llamada telefónica. Las estafas de suplantación de identidad *(phishing)* telefónicas le indican que llame a un número de teléfono en el cual una persona o una unidad de respuesta de audio esperan para conseguir su número de cuenta, su número de identificación personal, su contraseña u otros datos personales valiosos.
- Los mensajes fraudulentos generalmente no están personalizados y es posible que compartan propiedades similares, como detalles en el encabezado y en el pie de página.
- Todo tipo de mensaje de correo electrónico que solicita información bancaria es probablemente una estafa de suplantación de identidad. **La mayoría de los bancos legítimos no requerirán esta información vía correo electrónico.**


BBVA net

Estimado cliente!
Nosotros no hemos podido proceder las operaciones ultimas sobre vuestra cuenta.
Para garantir que vuestra cuenta no esta suspendido, renueve, por favor, vuesta información. Si usted ha renovado su información recientemente, rechazar, desprecie, por favor, porque nosotros procedemos los cambios cuales usted ha hecho.

La Banca en Internet

adelante es no quedarse atrás

- **adelante** es acceder a BBVA ahora y las 24 horas del dia.
- **adelante** es administrar tus cuentas de la manera más sencilla.
- **adelante** es disponer de los productos y servicios exclusivos que mejor se adaptan a ti.
- **adelante** es que nos tengas siempre a un clic de distancia.
- **adelante** es que disfrutes de la mejor banca online.

adelante es BBVA net

Llene la forma following BBVA NET

© BBVA S.A. 2005

Frases en un *e-mail* que indican una actividad de *phishing:*

- "Verifica tu cuenta" mencionando que hay un problema para darle mayor credibilidad.
- "Cancelaremos su cuenta si no actúa en 24 horas" u otros apremios y supuestas razones para actuar.
- "Ha ganado un premio" o "ha ganado la lotería" o "ha sido seleccionado" o similares también son indicativos de *phishing* u otros timos.
- Frases en las que le acusan de un delito (por ejemplo de piratería de música o películas) y le ofrecen una amnistía o cancelar la deuda a cambio de un pago (el conocido "Virus de la Policía").

¿Qué debo hacer si creo haber respondido a una estafa de suplantación de identidad?

Sigue estos pasos para minimizar todos los daños si sospechas que has respondido a una estafa de suplantación de identidad con información personal o financiera o que has ingresado esta información dentro de un sitio web falso.

- Cambia las contraseñas o PIN en todas tus cuentas en línea que podrían estar comprometidas.
- Contacta con tu banco. No sigas el vínculo que aparece en el correo electrónico fraudulento.
- Si sabes de alguna cuenta a la cual se obtuvo acceso o que fuese abierta de manera fraudulenta, ciérrala.
- Revisa tus movimientos bancarios y de tarjeta de crédito con regularidad por mes con el fin de descubrir cargos o solicitudes sin explicación y que no hiciste.

Desgraciadamente, los usuarios suelen caer en este tipo de engaños muy fácilmente por diversas razones y variadas, ayudándose básicamente de una falta de conocimiento por parte de las víctimas del funcionamiento de este tipo de engaños/estafas/robos de identidad.

Por tanto, la mayoría de medidas técnicas que se tomen, ya sea desde el navegador mediante avisos, uso de certificados… no sirven para casi nada.

Es necesario apostar por una educación de los usuarios ante el uso de este tipo de servicios, de forma que éstos sean conscientes de los riesgos que toman a la hora de navegar por Internet y de introducir sus datos tan libremente.

El consejo más importante que se puede dar para evitar el *phishing* es **no pulsar nunca en enlaces sospechosos y menos todavía facilitar nuestros datos personales o credenciales de acceso de forma gratuita, con ello nos evitaremos más de un problema.**

REGLAS DE ORO PARA NO SER "PESCADOS" EN LA RED

Los *phishers* o "pescadores en la red" utilizan el *spam* para lanzar campañas de *phishing*. Tienen un fin claro: aumentar su economía en perjuicio de la nuestra.

Utilicemos la lógica como en la vida real y llevemos a rajatabla estas R**EGLAS DE ORO** para evitar convertirnos en "pececitos":

1. **Desconfiar de los mensajes que parezcan provenir de entidades bancarias** y que nos pidan nuestras claves de acceso a la banca *on-line*. Ante la duda consultemos directamente a nuestro banco.

2. **No abrir mensajes de *spam,*** muchos de ellos están "construidos" con códigos especiales que con la simple apertura ya están infectando nuestro ordenador para otros fines menos "comerciales" o simplemente para confirmar que nuestra cuenta es válida.

3. En caso de abrir un *spam* **nunca hagas *click* en una URL o imagen que figure en el mensaje,** puede llevarte a una web fraudulenta que sin darte cuenta te descargue de forma automatizada un virus o troyano.

4. **Nunca responderemos a un mensaje de *spam*,** son mensajes enviados tras obtener su correo o cuenta de usuario de una lista obtenida por Internet, normalmente de una lista fraudulenta o por simple azar, con nuestra contestación estaremos avisando que la cuenta es real y que pueden empezar una campaña para personalizar una estafa en la que nosotros podríamos ser la víctima.

5. **Mantén deshabilitada la función "auto-responder" de tu gestor de correo.** Una contestación automática es una forma de confirmar a los malos que nuestra cuenta de correo está activa. Utilízala solo en caso de necesidad pero con control (vacaciones, ausencias profesionales, etc.).

6. **Trata tu dirección de correo como a un dato personal y privado,** no aportándolo gratuitamente para cualquier cosa. En caso de necesitar una cuenta para navegación, sé desconfiado y utiliza una cuenta secundaria exclusivamente para la navegación por Internet.

7. **Los documentos adjuntos también pueden traer sorpresa por lo que no debes abrirlos ni reenviarlos,** comprueba todos los correos y archivos que recibas con tu antivirus o antivirus *on-line* (www.virustotal.com).

8. **Si tienes duda de que el remitente puede ser o no un *spamer,* puedes consultarlo y buscar información en Internet** para comprobar que no estar reportado como correo fraudulento; simplemente introduce el correo en www.google.es y lee los resultados.

9. **Si tienes la certeza que es un *spamer* quien te envía el correo bloquéalo** utilizando simplemente los filtros de "correo no deseado" de tu gestor de correo.

10. **Para evitar crear listas de *spam,* cuando envíes un *e-mail* a varias personas, utiliza siempre el campo CCO (Con Copia Oculta)** para escribir las direcciones de los destinatarios, en lugar de escribirlas en el campo CC. De esta forma la lista de direcciones no será visible para los demás.

6. EL *PHARMING*

El *pharming* constituye otra forma de amenaza en la Red, similar al *phishing*. En este caso los *pharmers* (los autores de los fraudes basados en esta técnica del *pharming)* utilizan también sitios web falsos con el objeto de robar información confidencial para poder llevar a cabo sus objetivos finales, realizar estafas en la Red, pero en esta ocasión se hace más difícil el detectarlos ya que la víctima no necesita dar continuidad a un mensaje fraudulento.

Los ciberdelincuentes redirigen a sus víctimas a una página web falsa, al igual que el *phishing*, incluso si el internauta teclea o escribe correctamente la dirección de Internet (URL) de la página que quiere visitar, normalmente de su banco.

Para llevar a cabo este redireccionamiento, de la víctima al sitio fraudulento, los *pharmers* realizan lo que se denomina como envenenamiento de la caché del **DNS**[67], que no es otra cosa que un ataque dirigido al sistema de nombres de Internet. Realmente este "ataque" consiste en la manipulación de los registros DNS de los servidores globales con el objetivo de redireccionar las solicitudes de los usuarios hacia sitios web con contenidos maliciosos.

Sí, esto suena un poco raro, pero vamos a traducirlo…

Cuando nosotros escribimos en nuestro navegador una dirección web, estamos diciendo a nuestro navegador que se dirija a un servidor (ordenador en Internet) donde se encuentra la página que queremos visitar.

Todos los ordenadores en Internet se identifican con una serie de números denominados IP *(Internet Protocol)* y cada página web se encuentra en una "dirección" IP distinta que generalmente no cambia para permitir su fácil localización en Internet.

En analogía a las direcciones postales las IP son las direcciones en Internet, pero en esta ocasión, en la Red, las direcciones se corresponden con un número con la siguiente estructura (aunque ya existen tendencias a modificar el formato para aumentar la cantidad de direcciones a asignar):

111.111.111.111

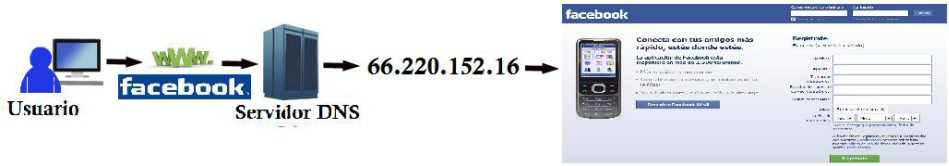
Estas series de números no son fáciles de recordar, por ello cada página web, con su dirección IP se asimilan a un dominio (nombre de la página que queremos visitar), de manera que cuando escribimos el nombre de una página web en nuestro navegador nuestro servidor de Internet lo traduce de forma automatizada hacía la dirección de Internet (IP) de la página.

Un ejemplo:

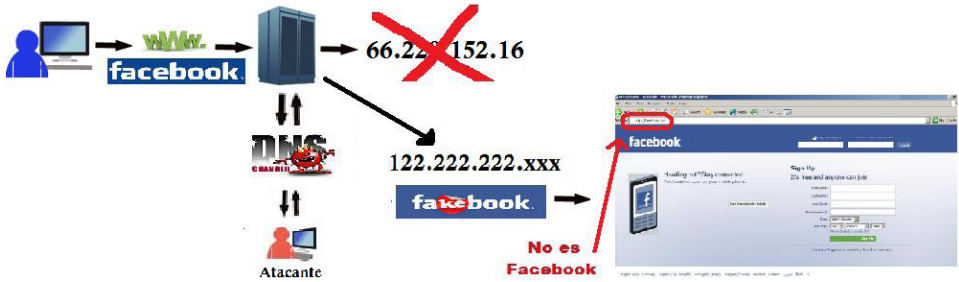
Si queremos visitar la página web del buscador Google tecleamos en la ventana de nuestro navegador la dirección http://www.google.es. Nuestro servidor de Internet traduce esta dirección y nos envía al ordenador donde se encuentra la página que queremos visitar, en este caso a **la dirección IP 74.125.141.94 (podéis probar y escribir en vuestro navegador esta IP, veréis que os lleva a Google).**

[67] **DNS:** Es una base de datos distribuida con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet.

Un ejemplo de cómo accedemos a la red social Facebook:



Visto esto toca explicar lo que es realmente el *pharming* y lo que hacen los *pharmers* para "engañarnos". Vamos a ver un ejemplo en imágenes siguiendo el anterior.



Estos ciberdelincuentes infectan nuestros equipos con *software* malicioso *(malware)* mediante el cual consiguen manipular los nombres de las páginas web que introducimos en nuestro navegador, de forma que cuando introducimos el nombre de la página web a visitar el virus impide que nuestro servidor la traduzca a la dirección IP real, redireccionándonos a la página web fraudulenta, normalmente una copia perfecta de la página web real.

Además, el *pharming* no se lleva a cabo en un momento concreto, como lo hace el *phishing* mediante sus envíos, ya que la modificación de DNS queda en un ordenador, **a la espera** de que el usuario acceda a su servicio bancario. De esta manera, el atacante no debe estar pendiente de un ataque puntual.

El remedio para esta nueva técnica de fraude pasa, de nuevo, por las soluciones de seguridad antivirus. Para llevar a cabo el *pharming* se requiere que alguna aplicación **se instale en el sistema** a atacar (un fichero .exe, una fotografía o una presentación Powerpoint, por ejemplo). La entrada del código en el sistema puede producirse a través de cualquiera de las múltiples vías de entrada de información

que hay en un sistema: el ***e-mail*** (la más frecuente), descargas por Internet, etc. En todas y cada una de estas entradas de información, el antivirus debe detectar el fichero con el código malicioso y eliminarlo.

La lógica, el sentido común y la prevención como mejor solución al *pharming.*

Alerta: Día "D", hora "H". ¡DNS-Changer ataca de nuevo!

En este artículo os voy a presentar un caso real de *pharming*. En esta ocasión los cibercriminales utilizaron un virus llamado "DNS-Changer" que amenazaba con dejar sin Internet a millones de usuarios en el mundo.

Recientemente apareció una noticia que alertó a todos los internautas:

> **"Posiblemente, el próximo 9 de julio, cuando accedas a cualquier página web a través de tu navegador, no obtengas ningún resultado o te encuentres navegando en una web pero en realidad no es la web que te imaginas si no otra "clonada" y con fines…"**

Esto puede tener dos motivos, que se te haya roto el "Internet" o **que un "bichito" llamado DNS-Changer esté haciendo una mala jugada en tu PC.**

¿QUÉ ES DNS-CHANGER Y POR QUÉ ES PELIGROSO?

DNS-Changer es un troyano *(malware)* que modifica la configuración de nuestra conexión a Internet, servicio DNS, de forma que cuando quieres acceder a la Red realiza una redirección a servidores maliciosos sin que te des cuenta.

En cristiano, el servicio DNS es el encargado de traducir un nombre de dominio en una dirección IP. Vamos, que lo que escribimos en el navegador lo traduce a la dirección real de Internet que es un número llamado IP, por lo que si esta traducción

es manipulada, cuando introducimos una página web en nuestro navegador o accedemos a cualquier servicio a través de su nombre de dominio (elblogdeangelucho.wordpress.com por ejemplo), en realidad puede acceder a cualquier página o servicio, con no muy buenas intenciones, gestionado por el ciberdelincuente.

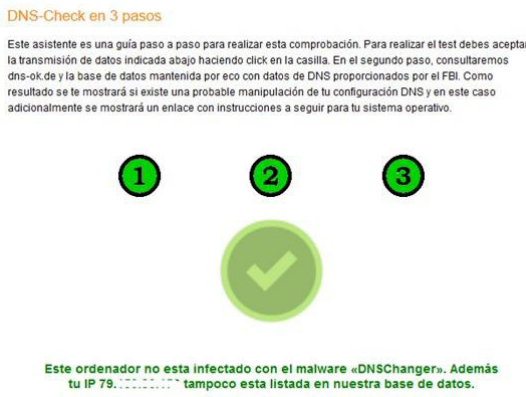
Dicho de otra manera DNS o ***Domain Name System*** es un sistema que permite localizar y direccionar equipos en Internet. **El virus en cuestión secuestra este servicio haciendo que una persona que tenga su ordenador infectado, crea que está visitando una determinada página web cuando en realidad no lo está haciendo.**

Por ejemplo, si nuestro ordenador está infectado y buscamos la página de nuestro equipo de fútbol favorito en un buscador, no saldrá como primera opción. Si pinchamos, iremos a parar a una página idéntica a la que queremos visitar pero que ha sido clonada por los malos.

Actualmente el FBI, tras la detención de los ciberdelincuentes, controla todos los servidores DNS que fueron utilizados por este virus. Dichos servidores van a ser deshabilitados el próximo día 9 de julio de 2012, por lo que a partir de dicha fecha, los equipos (infectados) que continúen utilizando estos servidores DNS no tendrán acceso a Internet. Esto hace que sea importante que estos equipos sean identificados y desinfectados correctamente antes de esta fecha.

¿CÓMO SABER SI TU PC HA SIDO AFECTADO POR DNS-CHANGER?

La forma más rápida de saber si tu PC ha sido afectado por DNS-Changer es analizar tu equipo en la página **DNS-Changer.eu** y seguir los pasos. En esta página colaboran la Oficina de Seguridad del Internauta (OSI) y el Instituto Nacional de Tecnologías de la Comunicación (INTECO) y en ella te dirán si debes reparar la conexión o no.



¿CÓMO DESHACER LOS CAMBIOS EFECTUADOS POR DNS-CHANGER?

¿Ha sido alterada tu conexión? Para volver a la normalidad y evitar que tu PC se quede sin conexión o para recuperarla en caso de que ya la haya perdido, es necesario deshacer los cambios efectuados por el virus.

DNS-Changer no es un virus tradicional. Al infectar un PC no permanece residente en memoria, sino que modifica unos parámetros de la conexión y luego desaparece. Por eso muchos antivirus son ciegos frente a su ataque.

Para restaurar nuestro ordenador debemos realizar las siguientes cuatro tareas:

- Eliminar el virus.
- Deshacer los cambios en la configuración DNS.
- Revisar el archivo *hosts*.

Existen múltiples herramientas que automatizan esta "limpieza" ya que detectan los cambios efectuados por el **virus DNS-Changer** y los deshace, desinfectando de una vez por todas el PC.

Si el DNS-Changer os ha visitado, podéis utilizar cualquiera de estas herramientas. Todas son igualmente eficaces contra el virus:

- Avira DNS-Change-Tool
- KasperskyTDSSKiller
- McAfee AVERT Stinger
- Norton PowerEraser

Desde **INTECO** también nos guían para **"eliminar el bichito"** y restablecer la configuración de PC para poder seguir disfrutando de Internet.

¿CÓMO EVITAR QUE DNS-CHANGER U OTRO VIRUS SIMILAR TE INFECTE?

Si DNS-Changer ha podido alterar la configuración de tu PC, lo más probable es que estuvieras descuidando la seguridad de Windows. En general, **nunca ejecutes archivos desconocidos** y, si usas antivirus, mantén al día su base de datos.

7. ESTAFAS EN LA RED

Tampoco las estafas son una actividad delictiva nueva que aparece con las nuevas tecnologías.

El estafador se ha adaptado a la evolución digital, se ha convertido en "ciberestafador", trasladando las estafas que conocemos en la "vida real" a "la vida virtual". La única diferencia es que ahora las realizan a través de la Red, medio por el que tienen la oportunidad de llegar a más víctimas sin apenas exponer su verdadera identidad. Esta actividad no genera apenas riesgo para el estafador.

En Internet podemos encontrar diferentes estafas, todas acordes a la necesidad de los ciberusuarios de la Red y aprovechando las principales vulnerabilidades del internauta, la confianza, la ambición y la credulidad.

Los grupos en los que se pueden clasificar las estafas en la Red podrían clasificarse en:

- **Fraudes en subastas o ventas *on-line.*** El falso anonimato de la Red hace proliferar un ingente número de vendedores desaprensivos que se aprovechan de los clientes a los que se adjudica la subasta. Una vez que el cliente realiza el pago, éste recibe un producto que no se corresponde con el que esperaba recibir o bien se recibe un producto sin valor alguno. O simplemente el envío no se realiza nunca.

- **Redes piramidales o trabajos desde casa.** Normalmente ofreciendo generosas ofertas de empleo a través de *spam,* que permiten incluso trabajar desde casa. Ofrecen una cantidad de dinero fácil mediante un negocio aparentemente efectivo y sin riesgos. Simplemente hay que aportar una cantidad de dinero para la compra de algún producto, insignificante suma en comparación con las ganancias y con recuperación inmediata tras la venta de los productos. Este tipo de trabajo promete la multiplicación de los

beneficios si se reclutan otros "vendedores". Por ello su estructura piramidal al constituirse una cadena en la que los únicos beneficiarios reales son quienes la iniciaron.

- **Falsas inversiones.** Promesa de ganancias tras una pequeña inversión, con la salvedad que el dinero llega directamente al estafador al no existir realmente la "empresa" donde invertir. En ocasiones suelen ser acciones verdaderas de una empresa que se han revalorizado a la baja. El estafador aprovecha el desconocimiento de la caída de los valores en bolsa para llevar a efecto su engaño.
- **Premios de loterías, venta de productos milagrosos, falsos alquileres vacacionales, falsas herencias, inversiones en nuestra empresa.**
- **Cualquier tipo de estafa que pueda tener cabida en la imaginación del estafador aprovechando la credulidad del internauta poco precavido.**

Estafas nigerianas. El *scam*

"EL CIBERTIMO DE LA *SCAMPITA*"

¿Recordáis la película *La llamaban La Madrina* con Lina Morgan que hacía el timo de la estampita con José Sazatornil como gancho? Pues **los "cibermalos" han adaptado el clásico timo a las nuevas tecnologías.**

Internet está al alcance de todos, para lo bueno y para lo malo, en este caso para lo malo, pues ciertas personas, o mejor dicho ciertos grupos organizados de ciberdelincuentes, se dedican a remitir *e-mails*, a miles de personas, mediante los que cuentan una historia **(léase milonga)** para hacer caer en el engaño a sus receptores. Muchos de los destinatarios no se tragan el "anzuelo" pero otros sí, os

sorprenderíais de ver cuántos y **de lo que serán capaces de hacer por conseguir su "premio".**

Pues sí, efectivamente me estoy **refiriendo a las llamadas estafas nigerianas, timo nigeriano o también conocido como timo 419 (*scam* 419)** (por el número de artículo del código penal de Nigeria que viola).

Con este **"negocio"** el estafador obtiene una cantidad de dinero de la víctima, todo en concepto de adelanto a cuenta de una supuesta fortuna que le ha prometido y que tiene varias formas de "presentarse en público"; generalmente como una gran cantidad de dinero que necesitan sacar de un país tercermundista y necesitan nuestra ayuda para hacerlo, en una supuesta herencia millonaria, de un suculento premio millonario de una lotería, de un porcentaje de una gran cantidad de dinero proveniente de una cuenta bancaria abandonada por un trágico fallecimiento, de un contrato de obra pública o simplemente de una gigantesca fortuna que alguien desea donar generosamente antes de morir y justo ha pensado en nosotros para donarnos esa cantidad.

A priori, yo catalogaría esta actividad como un "delito de guante blanco", porque además se lo "curran", se montan toda una trama digna del mejor guión cinematográfico de una película española de los años setenta.

Todo da comienzo con un correo no deseado, con un *spam.* **No es una estafa nueva,** solo emplea las nuevas tecnologías para difundirse. Seguro que los más viejos del lugar han llegado a recibir en alguna ocasión una de las antiguas cartas **(sí, sí, esos sobres de papel que, al abrirlos, nos sorprendían con una maravillosa carta que nos arreglaría la vida),** sé que es difícil entenderlo pero antiguamente los seres humanos se comunicaban por correo postal.

Os pongo un ejemplo de *e-mail* (ladrillazo a la vista), veréis que cometen muchas faltas y además se expresan fatal en castellano:

"Hola mi Querido:

Estoy realmente muy interesado en ti ,mi nombre es (Yeni) 25 años chica de Sudán, soy de una familia de tres, la primera hija de mis padres, mi padre era un hombre de negocios antes de su muerte, en la presente crisis en mi país, pero actualmente i soy residente en Senegal, a causa de la guerra rebelde en mi país, los rebeldes atacaron nuestra casa una mañana temprano y mataron a mis padres y mis dos hermanos pequeños en una fría blood. God salvar mi vida porque yo estaba viviendo en la escuela, por lo que i logrado hacer mi camino a un país vecino Senegal con la ayuda de unos soldados con otros refugiados de mi país, por lo que actualmente soy residente en la (Ndioum campamento de refugiados aquí en Dakar, Senegal, donde estoy en busca de asilo político en virtud de las Naciones Unidas Alta Comisión)
Estoy en un gran dolor aquí en el campamento, al igual que soy alguien en la cárcel, no tengo mi libre circulación, se trata de mis tres meses en este campo con
sufrimientos y dolores,i realmente necesita el hombre un ser querido, que me ayude a cabo de la situación,

Deseo contacto con usted personalmente para compartir mi amor y mi experiencia con ustedes, mis queridos, hay una cosa que han particullar me ha estado molestando durante algún par de días, y no he podido encontrar una solución al mismo, que es un de mis experiencias, sólo me ven como una parte de ti, y me siento libre, creo que un día en una buena relación es como un año en mi sitio, si el amor se entiendan,

Mi difunto padre de una bendita memoria depositó la suma de EE.UU. $ 6,7 millones en un banco de Senegal con mi nombre como los familiares, que fue la razón por la que mi manera de árboles en otras Senegal a retirar dinero a mi cuidado, pero i lamentablemente fue declarado como refugiado desde entonces por lo que estaba en el interior del campamento. que me puse en contacto con el banco hace unos días no comprobar cómo puedo retirar el dinero a mi atención y salir de este campamento a fin de que yo pueda continuar mi educación, pero insistió en que el banco,i debe proporcionar un socio forighn a pararse en mi nombre para transferir el dinero en cuenta a las personas por el hecho de que todavía estoy en el campamento de refugiados, y tengo todos los documentos y todas las cosas que mis

padres consighning operación con el banco, que le ayudará a transferir el dinero a su cuenta tan fácilmente, necesito un ser querido y la confianza que merece el hombre que me ayude a transferir el dinero en su cuenta y que me ayude salir de este campamento de refugiados desde el fondo a su país para una inversión del fondo y continuar con mi educación, por favor mi querido ahora soy un huérfano, no tengo cuerpo que puede estar para mí en esta transacción, y el tipo de dolores estoy atravesando en este campo es insoportable para mí, necesito su ayuda, de cualquier manera usted sabe que usted me puede ayudar en esta situación, yo te amo con todo mi corazón, y nunca en mi vida olvide su esfuerzo a mi preciosa vida, si usted me puede ayudar a transferir este dinero en su cuenta personal para mí unirme a ustedes en su país que siempre se agradece, soy fiel y muy humilde que nunca pesar de saber de mí, i que desea compensar adecuadamente con 25 % por ciento del total de dinero después de la operación tan pronto como llegué a su país,

gracias

este es el número para obtener mi teléfono, (+221xxxxxxxxxxx), que es el campamento de refugiados de número de teléfono, controla revrend por el padre que está a cargo del campamento, sólo decirle que usted desea hablar con (miss ama funsho) que él me invitaba a su oficina para su llamada, en asseptance para que me ayude a transferir el dinero, sólo mensaje de vuelta con esta mi dirección de correo electrónico i de manera que le dará el banco de contacto en el Senegal
Me gustaría que usted transmita a todos sus datos personales,

el nombre de su país -------
su nombre completo y su edad --
su dirección completa --------
su número de teléfono ---------
su oficina ---------
y su número de fax ---------
de modo que voy a enviar a la entidad bancaria para la libre introducción,

gracias y un hermoso día."

¿Difícil no caer en la tentación de aceptar el trato verdad? Pues creed si os digo que estos "negociantes" hacen su agosto permanente y brindan con los mejores *champagnes* para celebrar su éxito.

La operación está organizada con gran profesionalidad en países como Nigeria, Benin, Ghana, Togo, aportando contactos de oficinas, números de fax, correos electrónicos, teléfonos fijos y móviles e incluso, a veces, sitios fraudulentos en Internet.

IVFS'

IVORIAN VIRGIN FINANCE & SECURITY

BOULEVARD ISAKA BODA, COCODY,
06 BP 1345 ABIDJAN 06 - COTE D'IVOIRE

CERTIFICAT DE DEPOT

RC : 2458478

REF : IVFS/KKB/158/02

Nom du déposiaire: Name of depositor	MR. HILLARY LEONARD
Code de sécurité Security Code	IVFS / 2002 / DHX/ 676
Code de transaction Transaction Code	233 / CCPA / 101 / 33488
Numéro du certificat de dépôt Certificate of deposit number	IVFS / ZPA / 415 / ABJ
Objet : Item:	Deux (2) valises (effet familiale) / Two (2) boxes (family valuables)
Numéro de référence : Reference number	233 / CCPA / 101 / 33039
Date de dépot : Issued on	12 JUNE 2002 / 12TH JUIN 2002
Raison du dépôt : Purpose of deposit	SECURITE DES BIENS / SAFE KEEPING
L'héritier: Beneficiary	MISS. HILLARY NANA HELEN.
Mot de passe: Password	MASQUE / NOT SHOWN
Adresse de l'héritier Beneficiary address	RUE DES MARTYRS SANTSE 524 ADOBA RES RWANDA
Pays d'origine: Country of origin	RWANDAISE

Certificat délivré par la compagnie IVORIAN VIRGIN FINANCE & SECURITY.
With full proof of ownership and declaration by IVORIAN VIRGIN FINANCE & SECURITY.

REV. SAWADOGO
Directeur

MR. HILLARY LEONARD
Déposiaire
Depositor

A quien acepte la oferta, los timadores le enviarán algunos documentos (casi siempre archivos gráficos adjuntados a mensajes de correo electrónico) con sellos y firmas de aspecto oficial. A medida que prosiga el intercambio, pronto se le pedirá que envíe dinero o que viaje al extranjero para entregarlo personalmente para hacer frente a supuestos honorarios, gastos, sobornos, impuestos o comisiones. Se van sucediendo excusas de todo tipo, pero siempre se mantiene viva la promesa del traspaso de una cantidad millonaria. A menudo se ejerce presión psicológica, por ejemplo alegando que la parte nigeriana, para poder pagar algunos gastos

y sobornos, tendría que vender todas sus pertenencias y pedir un préstamo. A veces se invita a la víctima a viajar a determinados países africanos, entre ellos Nigeria y Sudáfrica. Esto es especialmente peligroso, porque en ocasiones el inversor puede acabar secuestrado por el estafador o incluso muerto. En cualquier caso, la transferencia nunca llega, pues los millones jamás han existido.

Últimamente gran cantidad de estafadores provenientes del África Occidental se han establecido en diversas ciudades europeas (especialmente Ámsterdam, Londres y Madrid, entre otras). A menudo se dice a las víctimas que deben viajar allí para cobrar sus millones, para lo cual deben primero pagar una elevada suma, que parece sin embargo insignificante si se la compara con la fortuna que los incautos esperan recibir.

La víctima recibe un mensaje del tipo "soy una persona muy rica que reside en Nigeria y necesito trasladar una suma importante al extranjero con discreción, ¿sería posible utilizar su cuenta bancaria?". La suma suele rondar las decenas de millones de dólares y al inversionista se le promete un determinado porcentaje, como el 10% o el 20%.

Lógicamente cuando nos damos cuenta de haber sido estafados ya es demasiado tarde…

Compra/Venta por Internet

¡QUE NO TE LA DEN CON QUESO!

Comprar o vender por Internet, siguiendo unas normas básicas de seguridad resulta **"casi"** completamente seguro. El **problema es cuando la "ganga" nos ciega e impide que podamos emplear la lógica como haríamos en la "vida real".**

Aprovechando el "falso anonimato" de Internet algunos "personajes", haciéndose pasar por compradores o vendedores, pretenden llenarse los bolsillos a costa de la ingenuidad de los demás, poniendo anuncios trampa en los distintos portales de compra-venta de segunda mano.

Como medidas para no caer en sus engaños, tanto si queremos comprar o vender, tenemos que tener en cuenta ciertas pautas de seguridad y lógica:

1. Siempre debes elegir **portales de compra-venta de confianza** tanto para comprar como para vender, porque disponen de un servicio de control de posibles falsos anuncios (¡pero cuidado, la perfección no existe!).

2. Si buscas algún artículo que te interesa, procura que el **vendedor se encuentre en un lugar próximo o que puedas desplazarte para comprobar el producto** e incluso probarlo.

3. **No te dejes engañar fácilmente por los anuncios con precios extraordinariamente bajos,** recuerda que nadie regala duros a pesetas (como ejemplo los vehículos de alta gama puestos a la venta a menos de la mitad de su precio real).

4. **Desconfía si el vendedor se encuentra en el extranjero o si el anuncio está mal redactado en un pésimo español** (siguiendo con el ejemplo del punto anterior, la venta de un vehículo que se encuentra en Reino Unido y lo venden tan barato por la incomodidad de tener el volante en el lado contrario).

5. **Desconfía si la otra parte te solicita tus datos bancarios o de tarjeta de crédito,** y máxime si te pide los códigos de seguridad, fecha de caducidad, etc.

6. **Intenta recabar todos los datos posibles del comprador/vendedor,** solicitándole sus contactos personales para comprobarlos.

7. Con los datos que hayas obtenido **realiza búsquedas en Internet para ver si esa persona o empresa están reportados como estafadores** (Google es una buena herramienta).

8. **Entabla contacto con los compradores/vendedores por teléfono,** no solo y exclusivamente por medio de correo electrónico o fax, eso les puede hacer "invisibles" en un momento dado.

9. **No pagues el producto de forma anticipada,** tienes formas de realizar pagos más seguros, contra reembolso tras la comprobación del artículo, por medios de pago electrónicos y seguros con garantía de devolución, etc.

10. Si has llegado a la conclusión de que te interesa comprar o vender el producto a una persona determinada, **procura que el trato final sea en persona** o recuerda las medidas de seguridad que has leído anteriormente.

Falsas ofertas de empleo

¿QUIERES SER MI MULA? ¡PAGO BIEN!

La maldita crisis nos afecta a todos, pero a alguno, me refiero a los cibercriminales, esta mala racha económica puede salirle rentable simplemente agudizando el ingenio por un lado y por otro teniendo un poco de suerte.

En este caso el factor suerte no es otro que el "topar" con un "navegante" sin información, alguien que desconozca la forma de actuar de estos "personajes" que se valen de cualquier artimaña para llenarse los bolsillos de forma sencilla aprovechándose del desconocimiento de los usuarios de la Red y **en este caso beneficiándose de la situación de angustia que pueda estar pasando su víctima, por la situación económica, o bien simplemente por las ganas de ganarse un dinero fácil y rápido.**

Con lo que os voy a explicar a continuación más que nuestro bolsillo corremos otros peligros, corremos el grave riesgo de pasar de ser una víctima estafada a ser un colaborador de una actividad delictiva y por consiguiente con consecuencias penales para nosotros.

CAPTACIÓN

Muchos de vosotros habréis recibido algún correo como el que nos mostraba el diario *ABC* recientemente en el que ofrecía un empleo bien remunerado y sin apenas movernos de nuestra casa.

Oferta del trabajo

Un trabajo bien retribuido!

Te ofrecemos una posibilidad de ganar dinero fácilmente. Puedes simultanear este trabajo con él que tienes ya. que encontrar 2-3 horas libres al día 1 - 2 veces a la semana.

Te explicamos como funciona:

1. Realizamos el ingreso de 3000 EUR en tu cuenta.
2. Una vez llegado retiras el dinero.
3. **Ya has ganado 20 % del ingreso - te queda 600 EUR!**
4. Luego nos entregas el resto 2400 EUR.

Los montos transferidos y su frecuencia pueden ser diferentes, todo depende únicamente de tus preferencias y posibili actividad está absolutamente legal y no viola ninguna ley de UE o de España.

Si te interesa la propuesta y quieres probar, mándanos un mail a la dirección: es@nix-finance.com. Te contactaremo pronto posible para contestar tus preguntas.

¡Ten prisa! La cantidad de vacancias está limitada!

Le pedimos perdón si este mensaje le ha molestado. En caso que este e-mail le ha llegado por error y si desea dar de baja su dirección electrónica de nuestra bas

O tal vez un correo con las siguientes características:

"Propuesta del trabajo

¡Un trabajo bien remunerado!

¡Te proponemos una oportunidad de ganar dinero sin esfuerzo! No hay que dejar tu trabajo actual, se puede simultanear. Solo hay que disponer de 2-3 horas libres al día 1-2 veces por semana.

El procedimiento será el siguiente:

- *Te enviamos una transferencia de 3000 € en tu cuenta.*
- *Retiras el ingreso en efectivo una vez llegado.*
- *¡En este momento ganas 20% del ingreso – te queda 600 €!*
- *Enseguida nos entregas el resto del ingreso – 2400 €.*

¡Las cantidades de ingreso y su frecuencia dependen solamente de tus preferencias y posibilidades! Para hacerte parte del negocio tienes que vivir en España y tener una cuenta abierta en una entidad bancaria en España. Nuestra actividad es totalmente legal y no viola las normas de UE ni del país.

Si te parece interesante nuestra oferta y deseas colaborar, ruego enviarnos un correo electrónico a esta dirección:xxx@xxxxxxx.com. Te contestaremos en breve y aclararemos todas dudas y preguntas posibles.

¡Ten prisa! Las vacantes son limitadas!

Mil disculpas si este mensaje te ha molestado. En caso que este e-mail te ha llegado por error y si quieres dar de baja tu correo electrónico de nuestra base de datos – rogamos mandarnos un e-mail sin texto a nuestra dirección siguiente: xxxx@xxxxxx.com . Muchas gracias."

He leído en alguna entrada a blogs o noticias que este tipos de correos, por supuesto *spam (ver artículo sobre el* spam*)*, no tiene otra misión que la de realizar un *phishing (ver artículo sobre* phishing*)*. Pero este tipo de afirmaciones quedan bastante lejos de la realidad, con este tipo de correos no pretenden capturar nuestros datos personales para utilizarlos con otros fines, si no que pretenden utilizarnos a nosotros mismos. **Pretenden que, sin que nos demos cuenta, colaboremos con ellos como "canal" para blanquear dinero, ocultando con ello el verdadero origen del dinero.**

¡YA SOY UNA MULA!

Efectivamente, es más grave de lo que *a priori* parece. Si accedemos a lo solicitado en los correos nos estamos convirtiendo en colaboradores necesarios en la comisión de un delito de blanqueo de capitales. Esta figura es denominada "mula" o "mulero" (como también se denomina a quien transporta la droga).

Según se puede leer en ***El Blog de S21sec,*** la aparición de la palabra "mula" en el entorno del fraude en Internet no es algo nuevo y data ya de varios años atrás. Como viene siendo frecuente, es una traducción del término anglosajón *"money mule"*, y se puede definir como una persona que transfiere dinero o mercancías que han sido obtenidas de forma ilegal en un país (generalmente a través de Internet), a otro país, donde suele residir el autor del fraude.

Normalmente estas transferencias dinerarias, tan "beneficiosas" económicamente para nosotros, se realizan a otros países, generalmente a través de compañías como Western Union y SIEMPRE como beneficiarios personas inexistentes, que por algún tipo de "fenómeno paranormal" son capaces de retirar las cantidades transferidas desde cualquier punto del planeta sin ser detectados ni controlados.

Claro queda que tras estos correos se esconden redes criminales, mafias que se dedican a captar este tipo de "mulas", cibercriminales que con esta acción pretenden "mover" grandes cantidades de dinero para ser blanqueado, sin que sus nuevos "colaboradores" tengan conocimiento del delito que están cometiendo y que, por el contrario, participan encantados a cambio de una cantidad de dinero fácil.

CONSECUENCIAS

Recordad lo que os dicho al principio del artículo, si nos convertimos en una "mula" nos estamos convirtiendo automáticamente en colaboradores necesarios para la comisión de un hecho delictivo penado con la ley.

Uno de los principios básicos de nuestro Estado de derecho es el que sostiene que la ignorancia de la ley no exime de su cumplimiento y la culpabilidad exige imputabilidad. O dicho de otra manera, **en caso de aceptar este tipo de propuestas de "negocio" NO PODREMOS ALEGAR JAMÁS EL DESCONOCIMIENTO DE LA LEY Y PODRÍAN CONDENARNOS, INCLUSO CON PENAS DE PRISIÓN, POR UN DELITO DE BLANQUEO DE CAPITALES.**

Espero haber sido lo suficientemente claro para que no caigáis en este tipo de engaños, para ello simplemente recordad que tenéis que emplear siempre la lógica, como hemos hablado en otras entradas, la "vida" en Internet no difiere de la vida real y haciendo caso del refranero español nadie, y repito, nadie, regala duros a pesetas, como se solía decir.

MORALEJA: Para evitar ser usado como "mula" o intermediario, no aceptéis trabajos no solicitados de manejo de dinero o transferencias entre cuentas bancarias, ya que podríais entrar a formar parte, sin vuestro conocimiento, de una red delictiva.

Citas en Internet

CUANDO EL AMOR TE DEFRAUDA

Con la llegada de la Web 2.0 añadida a los servicios de mensajería gratuita por Internet (chats y mensajería instantánea), el aumento de las personas que utilizan los servicios de citas en Internet con la esperanza de encontrar a un compañer@ ocasional o un amor verdadero se ha multiplicado.

Lamentablemente a veces no solo corremos el riesgo de sufrir un "desamor", también podríamos llegar a tener roto algo más que el corazón, por ejemplo el bolsillo.

Los cibercriminales están utilizando estos servicios para llevar a cabo varios tipos estafas. Ell@s, aunque principalmente son mujeres, buscan a personas emocionalmente vulnerables, una vez que establecen una conexión, intentan robarles su dinero mediante el engaño, jugando con la sensibilidad de la víctima y su buen corazón.

CÓMO FUNCIONA LA ESTAFA

Estos ciberdelincuentes, quienes también utilizan las redes sociales y salas de chat en Internet para encontrar a sus víctimas, suelen decir que se encuentran en países lejanos a España, normalmente países subdesarrollados o que están atravesando graves problemas políticos y económicos, por lo que el vivir en ellos se hace muy difícil.

También se dan casos en los que las víctimas suelen ser mujeres de alrededor de cuarenta años, que están divorciadas, viudas y/o discapacitadas.

Para realizar sus estafas, los delincuentes comúnmente:

- Envían un mensaje o una foto y te dicen que están interesados en conocerte. También pueden crear un perfil con intereses similares a los tuyos en el sitio web del servicio de citas.
- Generan una conexión personal y se comunican contigo por chat durante semanas o hasta meses.

Una vez que se ganan tu confianza, intentan sacarte dinero jugando con tu buena fe y sobre todo con tu sensibilidad diciendo que no tienen medios económicos y que necesitan afrontar un gasto imposible por una enfermedad de un hijo o un familiar muy próximo. También utilizan como engaño que quieren salir del país para mejorar su calidad de vida y que les gustaría venir a España, y por supuesto conocerte, incluso a veces incitan a que vayas a visitarles a su país y cuando llegas te das cuenta que la única verdad es que el país existe realmente pero nada más.

Los problemas de crisis que se están viviendo actualmente en España están propiciando que este tipo de estafas sitúen a los estafadores directamente en nuestro país. El *modus operandi* es muy similar salvo a la hora del envío de dinero. En estos

casos prefieren recibir esas “aportaciones” a través de plataformas de envío de dinero (Western Union, MoneyGram, por citar alguna). Ya sabéis, tema de confidencialidad para que la familia no se entere ;-)

CÓMO PROTEGERSE

Para evitar caer en estas trampas lo ideal sería desvirtualizar las comunicaciones y llevarlas al campo real, si bien existen servicios de citas en Internet de buena reputación y que son reconocidos a nivel nacional. Si el “enamorado” en Internet tiene las siguientes conductas, es probable que se trate de una estafa:

- Insiste que te comuniques con él o ella a través de un correo electrónico personal o por un servicio de chat, en vez de comunicarse a través del sitio web del servicio de citas.
- Declara su amor al poco tiempo de conocerte.
- Te envía una foto que parece que fue tomada de una revista.
- Promete visitarte y cuando llega el momento de viajar cancela su vuelo en el último momento por una situación grave e insólita.
- Pide dinero para cosas como viajes, emergencias médicas, el pago de cuentas de hotel o de hospital, el trámite de documentos oficiales como visas o porque ha perdido dinero en una mala operación financiera.

Sí, lo sé, el amor es maravilloso y además ciego y sordo. Por suerte hay mucha gente que se puede identificar y portar esta camiseta...

Asociación de consumidores necesita tu ayuda

Este artículo es una traducción/interpretación de una noticia aparecida en el diario de noticias belga *RTL*.

Al parecer la mayoría de las víctimas conocidas son ciudadanos belgas, pero como dice el sabio refranero español "cuando las barbas de tu vecino veas cortar…".

Y como casi siempre... todo comienza con un *e-mail (spam).*

Se recibe un correo electrónico de una supuesta asociación de consumidores que nos explica que está realizando una investigación, y que para llevar a efecto esta "investigación" solicita nuestra ayuda para que participemos de forma activa en "la buena acción", y siempre en beneficio y protección de todos los consumidores.

Por supuesto nuestro importante papel en la investigación no será en vano para nosotros y será remunerado. **La "asociación" nos promete una compensación económica a cambio de nuestra participación,** pero esta parte la dejaremos mejor para el final de este artículo.

El proceso es simple: en el correo enviado se explica que la asociación está comprobando la calidad del servicio en Western Union (compañía que ofrece servicios financieros y de comunicación, muy utilizados para transacciones de dinero) afirmando haber recibido varias denuncias de consumidores.

Tras aceptar su participación en la investigación, la asociación le envía un cheque (por supuesto falso) con una cantidad de varios miles de euros, que usted deberá transferir directamente a través de Western Union a nombre de un "colaborador" en otro país, normalmente un país de Europa del Este.

Por supuesto, ahora viene la "gratificación" y el gancho para que la víctima participe, de la suma total nos quedamos con trescientos euros como pago por nuestra colaboración.

Una vez que el dinero es transferido, nos convertimos directamente en víctimas de una estafa de la que todavía no somos conocedores de la magnitud del problema.

Por algún tipo de fenómeno paranormal, muy utilizado por mafias del Este especialistas en este tipo de "transacciones", el dinero es retirado, de forma inmediata, desde cualquier parte del mundo utilizando identidades falsas.

Ahora viene lo peor y es que cuando Western Union comprueba que el cheque es falso, el dinero ya ha sido retirado. Y ¿sabéis a quién reclaman la totalidad del cheque? Si habéis pensado, como dice el dicho popular, que "al maestro armero", os confundís. Efectivamente **habréis sido víctimas de una estafa por la totalidad del cheque que os enviaron, puesto que la compañía de transferencias os lo reclamará a vosotros.**

Como empezábamos el artículo, no se tiene conocimiento de que este tipo de estafas hayan "aterrizado" en nuestro país (ni en otro que no sea Bélgica), pero **siguiendo el lema de este libro *Información + Educación = una Red más Segura,* esperamos que si se les ocurre aparecer por "casa" estemos prevenidos y no caigamos en su engaño.**

Porque como ya sabéis…

En Internet como en la vida real hay que actuar siempre con lógica y como decimos en España nadie regala duros a pesetas.

8. OTRAS AMENAZAS

A diferencia de otras amenazas, como el *phishing* o el *scam* existen amenazas que no tienen como fin, *a priori*, el lucrarse de los usuarios de la Red.

Aunque no persigan fines económicos o no revistan una amenaza extremadamente dañina, es aconsejable no bajar jamás la guardia en Internet y no subestimar ni la más leve intención de "engaño".

Han existido casos en los que, ante el temor de que se pudiera hacer realidad el mensaje de un correo electrónico recibido, el usuario ha formateado o borrado su disco duro perdiendo toda la información que en él se guardaba.

Por ello nunca debemos de menospreciar la más mínima amenaza en nuestro sistema puesto que podría constituir una "puerta" de entrada para otros peligros que pueden llegar a ser "devastadores" para la seguridad de nuestros equipos, pudiendo llegar a alterar nuestra propia seguridad o privacidad.

Mensajes engañosos: los *hoax*

¿QUÉ ES UN *HOAX*?

A día de hoy es común la utilización del ya viejo y conocido correo electrónico, pero además, con la llegada de la Web 2.0 y de los nuevos formatos de mensajería

y redes sociales, la comunicación entre usuarios de Internet se hace mucho más directa y sobre todo inmediata.

Acceder de forma inmediata y diaria a nuestros buzones de mensajería se ve ya una práctica común tanto en nuestra actividad profesional como en el ámbito personal. Pero si analizamos al detalle este hecho se podría comprobar que la mayoría de los mensajes que recibimos podríamos catalogarlos como de "información engañosa".

Este tipo de mensajes engañosos son conocidos con el nombre de *hoax*. Los *hoax* nos informan de una posible alarma de un virus peligroso o que podríamos ser víctimas de un engaño si no realizamos una acción determinada, nos advierten de un grave problema de salud de alguna persona sin recursos o nos alertan sobre graves consecuencias si no distribuimos un mensaje a todos nuestros contactos.

Un ejemplo reciente son los mensajes recibidos a través de **WhatsApp** a nivel mundial, comunicando que el servicio de mensajería sería de pago a partir de una fecha determinada, aconsejándonos que si reenviamos el mensaje disfrutaríamos de la gratuidad permanente del servicio. Ante esta ola de mensajes, **el propio servicio de mensajería anunció en su blog que la realidad de estos mensajes no era más que un *hoax.***

Este tipo de cadenas ya habían circulado con anterioridad y también en otras aplicaciones como el Blackberry Messenger. Incluso años atrás, pasaba con Hotmail o el MSN.

Y si estos mensajes son falsos ¿cuál es la verdadera intención de quien inicia la cadena de mensajes?

Por lo general, este tipo de alarmas, suele ser totalmente falsa. El propósito final de estos mensajes podría tener dos direcciones:

1. Saturar los servidores de las empresas de mensajería o correo.
2. Obtener cuentas de correo electrónico o mensajería para preparar posteriores campañas de *spam* con fines fraudulentos, estafas, *phishing,* etc.

¿CÓMO PODEMOS IDENTIFICAR QUE UN MENSAJE ES REALMENTE UN *HOAX*?

Normalmente los *hoax* se "delatan" a sí mismos si analizamos su contenido:

1. Piden que reenviemos a toda nuestra lista de contactos el mensaje aconsejando no romper la cadena.

2. No proporcionan ningún *link* donde informarse realmente de lo que informan y si lo aportan es un *link* creado especialmente para el efecto, formando parte del engaño.

3. A veces solicitan, en el caso de los correos electrónicos, remitir algo a cambio de una compensación económica (que nunca llegará). Es una forma de conocer desde donde se ha remitido el correo.

4. Al recibir una alarma sobre un virus, debemos consultar si la existencia del virus es falsa o verdadera en páginas específicas sobre este tipo de alertas:

- **Instituto Nacional de Tecnologías de la Comunicación (INTECO)**
- **Oficina de Seguridad del Internauta (OSI)**

¿QUÉ HACER ANTE UN *HOAX* PARA EVITAR PROPAGARLO?

Cuando tengamos la certeza que hemos sido destinatarios de un *hoax* debemos tomar ciertas medidas de precaución para evitar continuar con el engaño y no seguir propagándolo **rompiendo la cadena:**

1. No reenviando el mensaje.

2. En caso de tratarse de un correo electrónico y querer informar a nuestros contactos: NUNCA REENVIARLO. Simplemente copiar el contenido del *hoax* y pegarlo en un nuevo *e-mail.*

3. Las direcciones de tus contactos incluirlas siempre en la casilla CCO (Con Copia Oculta).

4. Romper la cadena eliminando el mensaje.

IV
MENORES EN LA RED

Con la llegada de las nuevas tecnologías ha cambiado mucho el cuento, los padres ya no tenemos que estar en la ventana pendientes de ver con quién está jugando nuestro hijo, o si le surge el más mínimo problema. Nuestros hijos han dejado de ser tan "callejeros" como lo éramos nosotros y ahora se "entretienen" con sus ordenadores, consolas y *smartphones* en la tranquilidad de sus habitaciones para la **"falsa" tranquilidad de los padres.**

Ahora, en la era de la comunicación, nuestros hijos son especialistas en la socialización, **tienen cientos de "amigos" con quienes habla y comparte confidencias** en redes sociales, en medio de una partida de sus juegos *on-line* preferidos o a través de los programas de mensajería instantánea instalados en sus teléfonos móviles de última generación.

Son especialistas en el uso y disfrute de las nuevas tecnologías, tengamos en cuenta que han nacido a la par, son realmente **"nativos digitales", verdaderos expertos en "maquinitas y aparatos varios", gozan del control absoluto de las nuevas tecnologías y de sus herramientas, ¡ellos han inventado "el Internet"!**

Por el contrario, nosotros, los "inmigrantes digitales", no nos enteramos "de la misa la mitad", no tenemos ni idea de *tuentis*, *facebús* o *jabús*. Esa es la idea que tienen nuestros hijos de nuestro conocimiento de las nuevas tecnologías y esa es precisamente la idea que tenemos que quitarles de la cabeza. Para ello tenemos que empezar por "educarnos" nosotros mismos.

¿Tenemos razón para preocuparnos? Sí. ¿Tenemos razón para desesperarnos? No. *A modo de ejemplo:* en el tema de Internet podemos parecer turistas y nuestros hijos autóctonos de la Red. Por ello debemos familiarizarnos con todo esto tan nuevo para nosotros, no hace falta convertirnos en expertos en la materia para proteger a nuestros hijos.

Como de costumbre, no quiero ser ni parecer alarmista ni detractor de Internet. Al contrario, como internauta que soy, desde los principios de Internet, abogo por los numerosos beneficios de la Red en todos los aspectos, tanto culturales y educativos como sociales y comunicativos, pero que como se suele decir en el sabio refranero español "por un garbanzo negro se estropea el cocido".

¡Pues no estoy de acuerdo!, simplemente quitemos ese "garbanzo negro" de Internet para que nuestros hijos puedan disfrutar de sus bondades y nosotros de la tranquilidad de saber que nuestros hijos están seguros en la Red. Para ello no necesitamos hacer ningún máster como expertos informáticos para poder protegerles, simplemente debemos acabar con la llamada "brecha digital" entre padres e hijos y ser conocedores de los peligros a los que se pueden enfrentar en el mundo virtual como conocemos los peligros que les acechan en el mundo real.

Los padres no siempre somos conscientes de **los peligros que entraña la Red** aunque tenemos, en ocasiones, una cierta percepción de inseguridad. Se ha repetido, y en varias ocasiones, el peligro de la "falsa soledad" en Internet de nuestros menores, el peligro de que nuestros hijos puedan ser víctimas de un ciberdepredador que les acose mediante las técnicas del conocido *grooming*. O simplemente que ellos mismos sean víctimas dentro de su propio círculo o incluso los

causantes del problema en los casos de *ciberbullying* o *sexting*, los tres peligros "ING" de los menores en la Red.

Conscientes de estos tres peligros "principales", que explicaremos en este capítulo, tenemos que **abordar otros peligros de los que no tenemos consciencia pero no por ello se convierten en menos graves.**

Me refiero a las experiencias verdaderamente negativas, como por ejemplo durante la navegación. Con no más de tres *clicks* de ratón un menor puede llegar al visionado de imágenes fuertemente pornográficas o violentas. Solo el 45% de los padres conoce las experiencias negativas que sus hijos han sufrido en uno u otro momento en la Red. El problema es que **más del 60% de los menores afirma haber tenido experiencias desagradables y negativas.**

Muchos padres ni siquiera saben que, aunque sus hijos dediquen poco tiempo a navegar por Internet, luego dejan el ordenador encendido descargando contenidos, mientras que los padres permanecen totalmente ajenos al contenido que se descargan. Recordemos los "extintos" videoclubs, en ellos encontrábamos distintas secciones y temáticas, en Internet pasa igual, podemos disfrutar de los mejores contenidos de animación infantil pero también de las temáticas más duras y atroces de las que jamás podríamos imaginar.

Cambiar las reglas del juego

Los peligros en Internet aumentan conforme crece la exposición de los menores a la Red sin una adecuada supervisión por parte de los adultos. Por otro lado, esa falta de supervisión puede además provocar que los niños hagan usos inadecuados o poco responsables de la Red. El verano es un momento ideal para cambiar las reglas del juego.

Para los especialistas, **la clave del éxito está en el diálogo.** Los menores deben saber que pueden confiar en los padres en todo momento y que van a tener su apoyo. Muchos menores no les cuentan a sus padres los problemas que tienen en Internet por temor a irritarles.

El ordenador debe estar situado en una sala común como el salón, o una habitación de uso familiar, aunque eso no va a garantizar que el menor acceda a Internet a través de los ordenadores de los amigos, o los de un cibercafé o biblioteca.

Por otro lado, los padres muchas veces olvidan que el teléfono móvil es una vía de acceso a Internet cada vez más habitual y que los riesgos que se corren con el teléfono móvil son similares a los de un ordenador conectado a la Red. Por eso es conveniente revisar habitualmente la factura telefónica y la actividad de la cuenta de los menores y además establecer un lugar común, por ejemplo una mesita auxiliar en el salón, donde se recarguen juntos los teléfonos de padres e hijos. Que en ningún caso se los lleven a solas a la habitación por las noches.

No se trata de prohibir Internet. Esta medida solo trasladaría el problema a otros ordenadores. Es mejor explicar a los hijos por qué no deben acceder a determinadas páginas y qué peligros les acechan si desarrollan determinadas conductas que ellos creen inocuas, por ejemplo, proporcionar información personal en las redes sociales. Hay que dejarles claro de forma razonada que si ponen muchas fotos de la casa, escriben su dirección y dicen que se van de vacaciones, hay muchas posibilidades de que al volver no queden ni las bisagras de las puertas.

Por suerte, en esta lucha contra los peligros que amenazan a los menores en Internet, **los adultos tienen a la tecnología de su parte.** Todos los ordenadores domésticos deberían tener instalado un antivirus y un cortafuegos, porque solo así se evita que el ordenador sea pasto de redes de ordenadores zombis que usarán la máquina para cometer todo tipo de delitos.

Se les puede explicar a los menores que no conviene que visiten ciertas páginas, pero además el acceso a esas páginas se puede bloquear desde el control de contenidos de navegador o desde un programa de control parental.

De igual manera, es posible establecer un horario de uso. Los programas de control parental permiten fijar la franja horaria en la que puede navegar el niño. **Para ello cada hijo deberá tener una cuenta de acceso de usuario con privilegios limitados, ¡JAMÁS COMO ADMINISTRADOR!**

Protegerlos de los contenidos que pueden ser nocivos e incluso peligros para ellos no es sencillo.

Gran parte de los archivos que circulan en las redes de intercambio P2P están contaminados, incluyen programas espía, troyanos, virus, contenido sexual o pornográfico y, en muchos casos, el contenido real no tiene nada que ver con el título.

En el siguiente "tramo" del capítulo dedicado a los menores en la Red vamos a explicar, mediante las distintas entradas publicadas en *El Blog de Angelucho* **los peligros que acechan a nuestros menores, pero también explicaremos la forma de evitarlos, y con ello podremos hacer que nuestros hijos utilicen Internet de forma segura para ellos y para tranquilidad nuestra.**

1. LOS CIBERDEPREDADORES

Radiografía de un ciberdepredador

En esta entrada voy a emplear el término **ciberdepredador** para denominar a la persona adulta que padece una parafília **(desvío de índole sexual)** en la que el objeto sexual elegido para la excitación y relación sexual es un menor y que como forma de acercamiento y acceso a los niños utiliza Internet. Aunque los conceptos genéricos pueden hacerse extensivos a la vida fuera de las nuevas tecnologías.

Los ciberdepredadores actúan de distintas formas con el único interés de conseguir acceder a niñ@s para alimentar sus "instintos sexuales". Estos instintos pueden verse satisfechos con el solo visionado de imágenes en las que aparecen los menores, pero en los peores de los casos su finalidad es la de abusar de ellos, producir su propio material pedófilo e incluso integrarlos en sus propias redes de prostitución infantil.

El fin de la entrada es el intentar conocer su *modus operandi* en Internet, haciéndoles una "radiografía", considerando fundamental conocer sus "movimientos" para poder practicar defensas efectivas a favor de la seguridad de los menores en la Red. Las distintas formas de actuar de los ciberdepredadores deben de conocerlas tanto los padres, como los educadores, como los propios niños para poder evitarlos.

¿QUIÉNES SON?

Existen distintos perfiles para clasificar a los ciberdepredadores, existiendo una "versión" diferente que depende incluso de cada país desde donde se emite el análisis.

Según mi particular opinión, un ciberdepredador puede estar englobado a su vez dentro de **tres grupos diferenciados,** dentro de una escala de menor a mayor de acuerdo al grado de acceso que tenga con el menor.

1*. BOYLOVERS* (preferencia niños) y *GIRLLOVERS* (preferencia niñas):

- *A priori* no "trafican" con material de imagen o vídeo considerado como pornografía infantil, pero sí consumen todo tipo de imágenes en la que los menores aparecen en poses más o menos eróticas.
- Cuando pasan al siguiente "grado" de la pedofilia lo hacen y lo comunican en privado, no de forma pública.

2. PEDÓFILOS:

- Adultos que sienten singular predilección sexual y afectiva hacia los niños, no llegando nunca al acto sexual, reaccionando por curiosidad para alimentar sus fantasías sexuales con menores.
- El pedófilo es consumidor habitual de material pornográfico con menores como protagonistas practicando sexo explícito entre sí o con adultos, o en poses eróticas (pornografía infantil) para potenciar su excitación, utilizando para ello redes P2P públicas o privadas, listas de correo y cualquier otro medio para el intercambio del material pedófilo.

- Cambia y descarga (trafica) contenidos pedófilos y, además de visualizar, en ocasiones también graba los contenidos con los que "comercia".
- Se escudan dentro de comunidades *boylovers.*
- Pasa mucho tiempo en chats, foros y webs de temática pedófila pero también se mueve por otros y redes sociales donde encontrar sus víctimas.

3. PEDERASTAS:

- Adultos que, al igual que los pedófilos, sienten predilección sexual por los menores de edad, con la salvedad que además "dan el paso" de mantener relaciones sexuales con los niños.
- La finalidad del pederasta es encontrar menores en Internet para contactar en persona. Normalmente es prudente hasta comprobar que realmente ha contactado con un menor, a quien le dice y hace ver precisamente lo que el niño quiere escuchar.
- Emplean técnicas de **ingeniería social** e incluso de *hacking* para tener acceso a los menores, no dudando en acosarlos y amenazarlos *(grooming)* para conseguir sus propósitos.

Además de estos tres grupos, podríamos incluir otro subgrupo y encuadrarlo en cualquiera de ellos, o incluso independiente en algunos casos, me refiero al:

PRODUCTOR DE PORNOGRAFÍA INFANTIL:

- Puede mantener o no relaciones con los menores.
- Emplea las mismas técnicas para acceder a los menores que los pedófilos o pederastas.
- Busca menores para explotarlos sexualmente con el fin de difundir los vídeos e imágenes con fines económicos o como mero intercambio de "material" por otro poco conocido.

- Abre y gestiona webs de pago en distintos países paraísos inaccesibles a las legislaciones y comisiones rogatorias internacionales.
- En ocasiones organiza reuniones adultos/niños como mero negocio.

Siguiendo con mi opinión personal, yo definiría a estos grupos como evolutivos, es decir un *boylover* puede convertirse en pedófilo y éste en un pederasta, pero también pueden quedarse anclados dentro del primer o segundo grupo sin dar el "salto" por determinados factores.

Tanto para un pedófilo como para un pederasta el niño es un simple objeto sexual no escatimando en realizar actividades de extrema perversidad para conseguir sus fines, no dudando tampoco en ejercer violencia física, emocional, chantaje, etc. para tener acceso a ellos de una u otra manera.

¿CÓMO ACTÚAN?

La llegada a nuestros hogares de Internet, la Web 2.0 y el fuerte aumento de la utilización, por parte de adultos y menores, de *smartphones* y sobre todo de redes sociales como forma de comunicación, ha potenciado, ayudándose del "falso anonimato" de la Red, que personas con **tendencias sexuales PROHIBIDAS E ILÍCITAS** busquen sus satisfacciones en Internet.

Los pederastas han cambiado los parques por los chats, la mensajería instantánea y las redes sociales donde practican la actividad conocida como *grooming* o ciberacoso infantil, ésta viene a definir la nueva táctica con la que pedófilos tratan de contactar a sus potenciales víctimas acosándolos virtualmente para conseguir sus pretensiones empleando todo tipo de **estrategias para ganarse la confianza del menor.**

Para ver más claramente cómo actúan los ciberdepredadores vamos a utilizar un símil. Este cibercriminal actúa y piensa como lo que es, "un cazador". Si alguno de vosotros es cazador sabrá que para disfrutar de una buena jornada de caza deberá conocer a la perfección los distintos hábitats en los que se mueven vuestras piezas, camuflarse e incluso utilizar reclamos para atraerlas, ¿verdad? Pues un ciberdepredador hace lo mismo en Internet para acceder a los menores.

No solo van a frecuentar juegos *on-line* para menores, salas de chats de niños, foros de series de moda, páginas web del cantante favorito de los críos o redes sociales sin ningún tipo de control parental donde saben que se dan reunión sus víctimas, sino que además se hacen pasar por uno de ellos, utilizan dotes especiales de convencimiento, de **ingeniería social** *(Ver artículo Ingeniería social: El hacking humano, Capítulo III. Amenazas en la Red, punto 4)*, para acceder a toda la información que necesitan de los niños. Información que les es facilitada de una forma pasmosa, teniendo en cuenta que no la tengan ya expuesta de forma pública en sus perfiles.

Una vez que han elegido a su víctima y ha logrado "engatusarla" con todo tipo de artimañas, comienza un contacto de forma más privada, por medio de mensajería instantánea, mensajes privados o mensajería móvil (WhastApp). Comienza el acercamiento "sexual" solicitando fotografías sugerentes, al principio es como un juego, como algo normal entre "chic@s de nuestra edad", pero el contenido sexual de las conversaciones va *in crescendo*, en el momento que tienen su "presa cogida" y el ciberacosador dispone de todo el control de la situación comienza el infierno para el menor, que en el peor de los casos no dirá nada a sus padres, tutores o amigos por miedo a represalias, llegando a acceder a todo lo que se le pida con tal de que sus padres no se enteren de la existencia de su "ciberamigo".

Además de las maniobras de convencimiento descritas, pueden utilizar otro tipo de acciones para conseguir el control total sobre el menor. **Utilizan técnicas *hackers,* y que me perdonen los *hackers* puesto que con su trabajo, normalmente en la sombra, ayudan a sacar de sus madrigueras en la Red a estas alimañas, desmantelando verdaderas organizaciones pedófilas.** Estos ingenieros sociales troyanizan el ordenador del menor (introducen un virus), teniendo acceso a la cámara web, audio y por supuesto a los archivos del propio ordenador, obteniendo todo tipo de información que es utilizada contra el menor para acosarlo y convencerle para que acceda a sus pretensiones sexuales.

Lamentablemente este acoso no termina en el plano virtual, ya de por sí muy duro para el niño. En muchas ocasiones, en demasiadas ocasiones diría yo, este acoso finaliza con el contacto real con el menor.

¿CÓMO EVITAR QUE NUESTROS HIJOS CAIGAN EN SUS TRAMPAS?

Es cierto que nosotros, como internautas, no podemos hacer nada para que los ciberdepredadores no proliferen en Internet. Tampoco podemos hacer nada para luchar contra esta lacra social, salvo denunciar a las autoridades cuando encontramos algún sitio web con temática pedófila o si nos topamos con alguno de estos individuos en la Red.

Lo que sí podemos hacer es educar a nuestros hijos como lo hacían nuestros mayores cuando no existía Internet con sus sabios consejos: "No hables con desconocidos", "no aceptes caramelos de personas que no conozcas", "no te subas al coche de un extraño", "no abras la puerta a nadie mientras te encuentres solo en casa".

Apliquemos estas "normas" de la vida real a la "vida virtual", eduquemos a nuestros menores para que ellos mismos protejan su propia seguridad y privacidad en la Red, t**engamos activado un buen CONTROL PARENTAL de forma activa,** que nada tiene que ver con realizar una actividad de espionaje activo hacia los menores, hablemos con ellos de los peligros que pueden encontrar en Internet y qué deben hacer si caen en alguno de ellos, que por supuesto es contar con sus padres o tutores.

También podemos apoyarnos utilizando algún tipo de *software* o filtros de control parental.

Se dice que la vida en Internet es virtual pero, lamentablemente, sus peligros son muy reales.

Informemos y eduquemos a nuestros hijos para que puedan disfrutar de las bondades de Internet de forma segura.

Pedófilos en la Red: símbolos que los delatan

Internet es la herramienta de comunicación más importante de las que disponemos hoy en día, pero también es una de las menos controladas. Es por esta razón que seguir el rastro de pedófilos y pederastas, de consumidores de pornografía infantil, e incluso de miembros de foros donde comparten estas parafilias, se hace muy difícil.

Escondidos tras el anonimato de las pantallas de sus ordenadores, los pedófilos generan comunidades clandestinas, con sus reglas y con sus propios símbolos que les hacen reconocerse entre ellos mismos.

El FBI elaboró un informe en enero 2008 sobre la pedofilia. En él se indican una serie de símbolos utilizados por pedófilos para ser identificados.

La simbología de lo que la comunidad pedófila denomina como “el movimiento de los amantes de los niños” incluye un corazón, un triángulo y una mariposa. En todos los casos, el contorno mayor alude al adulto y la figura menor que contiene hace referencia al menor.

El triángulo (llamado BLogo) simboliza la atracción hacia los varones menores.

El corazón (o GLogo) identifica la preferencia por las niñas.

Los símbolos están siempre compuestos por la unión de dos similares, uno dentro del otro. El de forma mayor identifica al adulto, la de menor al niño.

La mariposa, formada a su vez por dos corazones grandes y dos pequeños (rosas y celestes) representa a quienes gustan de ambos.

La diferencia de tamaños entre ellos muestra una preferencia por niños mayores o menores en cuanto a la edad. Los hombres son triángulos, las mujeres son corazones.

Estos símbolos también pueden encontrarse en elementos como monedas, medallas, joyas, anillos, colgantes, etc., entre otros objetos.

Otras tendencias, en cuanto a las formas de identificación entre las comunidades pedófilas, apuntan hacía una caricatura adorable llamado **Pedobear:** un oso de pelaje café, sonrisa permanente y siempre dispuesto a jugar con las niñas.

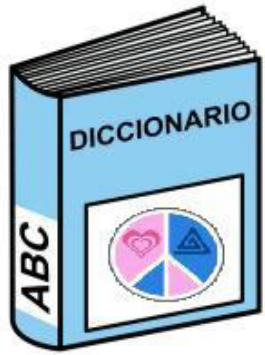
En páginas informativas de la Red se dice que la caricatura fue ideada en sitios de humor negro, en 1996, como un oso con inclinaciones sexuales hacia las niñas, pero últimamente dejó ser de una "broma" para ser utilizada por pedófilos como un símbolo de identificación y de ataque en Internet.

Pedobear es un "*meme*" (idea que se propaga a través de la Red) que se volvió popular a través del tablón de imágenes 4chan. Como su nombre sugiere (siendo "pedo" un diminutivo de "pedófilo"), es un osito pedófilo empleado para crear macros humorísticos sobre temas tabú como los pedófilos, la pornografía infantil o el *lolicon*.

Pedobear aparece mayoritariamente en redes sociales, salas de conversación y foros frecuentados por niños y niñas, a quienes la imagen les lleva hasta sitios donde adultos las invitan a salir o les muestran fotografías de sexo explícito.

Si conocemos sus secretos, podremos evitar los peligros que acechan a nuestros menores.

Pedófilos en la Red: conozcamos su vocabulario



En el artículo anterior, *Pedófilos en la Red: símbolos que los delatan,* hablábamos sobre la simbología mediante la cual podemos reconocer a los pedófilos en la Red.

Continuando con la idea de que la información es la mejor forma de defenderse de estos ciberdepredadores, a continuación os relaciono una recopilación de acrónimos utilizados en el mundo pedófilo para intentar pasar desapercibidos en sus conversaciones.

- **AF:** amigo adulto amigo (de un niño).
- **AL:** amante adulto.
- **AOA:** edad de atracción.
- **AOC:** edad de consentimiento (edad a la que uno puede legalmente tener relaciones sexuales, difiere según los países).
- **Novio BF:** utilizado principalmente acerca de las relaciones homosexuales.
- **BC:** *BoyChat* (chat de niños).
- ***BoyChatter:*** niño que chatea.
- **BI (bi):** bisexuales (atraídos por ambos sexos).
- **BL:** *boylover* (una persona amante de los niños).
- **BLL:** amante *boylover* (un *boylover* en una relación romántica con otro *boylover*).
- **BLN:** BoyLover.net (foro de la comunidad *boylover* desarticulado en una operación internacional contra la pornografía infantil en la que también participó el Grupo de Delitos Telemáticos de la Guardia Civil).
- **BLR:** *boylover.*

- **BM:** momento especial.
- **CG:** web o punto de reunión y de comunicación entre *boylovers* y *girllovers.*
- **CL:** *childlover* (una persona que ama a los niños de ambos sexos o miembro de un movimiento de unidad entre *boylovers* y *girllovers*).
- **CM:** (despectivo) abusador de menores.
- **CP:** pornografía infantil (también **KP**).
- **CSA:** abuso sexual infantil.
- **GL:** *girllover* (amante de las niñas).
- **GTG:** reunión real entre varios *boylovers.*
- **PK:** de porno infantil, también **CP.**
- **LB:** niño querido.
- **LBL:** amante de los niños pre-púberes (menores de ocho años). (Comparar con **TBL**).
- **PRF:** informar de un problema (en *BoyChat*).
- ***Sadvocate:*** persona que piensa que él sabe mejor que nadie acerca de los niños (despectivo).
- **SGL:** amor del mismo sexo.
- ***Siggy*** o ***sigpic:*** imagen opcional asociada con un apodo o *nick* en un foro o chat.
- **SO:** delincuentes sexuales.
- **SYF:** niño amigo especial; con este acrónimo los pedófilos definen a sus niños preferidos.
- **TA(BRE):** culo apretado; **AME:** culo apretado (un término de Pokémon para sus detractores).
- **TBL:** *teenboy amante* (que ama a los adolescentes). (Comparar **LBL**).
- **TV:** travesti.
- **YF:** joven amigo.
- **YIF:** joven amigo imaginario.

2. LOS PELIGROS

El peligro de la falsa soledad

Estoy seguro de que los que nacísteis el siglo pasado, antes de la instauración de la "era Internet" habéis escuchado de vuestros mayores los siguientes consejos: "No hables con desconocidos", "no aceptes caramelos de personas que no conozcas", "no te subas al coche de un extraño", "no abras la puerta a nadie mientras te encuentres solo en casa".

Eran otros tiempos en los que los padres nos educaban sobre los peligros a los que estabamos expuestos si entablábamos relaciones con "desconocidos".

Hoy sin embargo, con Internet la cosa ha cambiado, abrimos la "puerta" de nuestra casa a cualquiera, inconscientes de los peligros a los que nos exponemos o simplemente porque no queremos verlos, y lo peor de todo, con nuestra "desidia", exponemos a los peligros de la Red a nuestros menores.

¿Cuántas veces habréis "obligado" a vuestros hijos a que se fuesen a jugar a la habitación y de esa forma poder estar relajados en vuestro sofá disfrutando de esa película o de ese partido de fútbol? Claro, es que en la habitación es donde menos molestan y donde más seguros están, no pueden correr ningún peligro, y ¡además tienen "el Internet grabado" en su ordenador o *smartphone* y se lo pasan genial navegando!

Como se suele decir que una imagen vale más que mil palabras os recomiendo ver un vídeo de la **Asociación Protégeles** que hace una buena síntesis de lo que os

pretendo transmitir. *Link* Youtube: http://www.youtube.com/watch?feature=player_embedded&v=y83YUvutccA

Como veis, al abrir la puerta de nuestras casas con las nuevas tecnologías, exponemos de forma inconsciente a los menores a innumerables peligros que acechan en Internet y no solo como blanco fácil de posibles pederastas o pedófilos convirtiéndolos en objetivos de sus prácticas relacionadas con la prostitución y corrupción de menores **(pornografía infantil, *grooming,* etc.),** sino que además pueden ser víctimas de vejaciones o amenazas, contra su propia imagen y contra su integridad moral que pueden provenir de su propio entorno de amigos o compañeros de colegio y sufriendo con ello una fuerte intimidación psicológica con graves consecuencias ***(ciberbullyng)***, o simplemente, **con no más de tres *clicks* de ratón** desde una página web cuya temática sean los dibujos animados de moda o su cantante favorito, pueden acceder a contendidos para adultos **(sexuales, violentos, etc.)** o relativo a temáticas **proanorexia** o **probulimia** en las que presentan estas actividades como los estilos de vida de moda.

Cada vez más, dentro de los círculos en los que se mueven los menores, se extiende más la comunicación entre compañeros y amigos utilizando las nuevas tecnologías, en redes sociales, salas de chats, mensajería instantánea o móvil, ¿pero sabemos quién se esconde realmente detrás de un *nick* aparentemente de otro menor desconocido? **Un ciberdepredador piensa como un cazador,** no va a buscar a sus víctimas en chats de pedofilia porque sabe que allí no encontrará menores. Se va a dirigir a los lugares de los que sabe que son sus puntos de reunión,

chats de series televisivas o de animación infantil, de artistas con gran calado entre los menores y adolescentes o en chats de juegos *on-line* de moda.

Una vez "engatusados" los menores, puesto que han leído de su nuevo amigo exactamente lo que ellos esperan encontrar **(son verdaderos especialistas en emplear técnicas de convencimiento e ingeniería social para llevar a buen puerto su engaño)**, son tentados a tener contactos más personales y privados invitándoles a contactar por otros medios más directos e íntimos como Messenger o WhatsApp. **EL PRINCIPIO DEL FIN.**

La mayoría de las veces somos nosotros mismos o, en este caso, nuestros hijos, quienes facilitamos la labor a los "malos" para saber todo de nosotros y tener un acceso más sencillo a nuestras propias vidas. Les ponemos las cosas demasiado fáciles aportándoles TODO, dejamos de un lado nuestra seguridad y privacidad haciendo públicos nuestros gustos, aficiones, nuestras imágenes, datos personales, cuándo nos vamos de vacaciones y cuándo volvemos, si iremos a la fiesta de moda, etc.

Imaginaos que vais por la calle y un desconocido os aborda y os pregunta por vuestro nombre, dirección, aficiones, vuestra sexualidad, vuestros gustos, etc. ¿Se lo diríais?, pues ahora analizad vuestros perfiles o los de vuestros hijos en redes sociales y sobre todo el control de privacidad que tenéis/tienen para restringir el acceso a desconocidos. O simplemente analizar las listas de "amig@s" y valorar si lo son tanto como para tener tanta información personal sobre vosotros.

Seamos igualmente conscientes, y así debemos hacérselo ver a nuestros hijos, de que al igual que podemos/pueden ser víctimas en la Red, **el falso anonimato de Internet** puede convertirnos también en autores materiales de estos peligros hacia otras personas, y por consiguiente poder tener serios problemas legales. La ley no entiende de "virtualidades".

Tanto padres como hij@s debemos tomar conciencia de los peligros que existen y tomar las medidas necesarias para prevenirlos. Aprendamos y difundamos a nuestros hij@s las grandes bondades y posibilidades que ofrece Internet, y al igual que hacían con nosotros, inculquemos unas normas y recomendaciones para que su experiencia virtual en la Red no se convierta en un peligro generando nefastos problemas en su vida real.

Si habéis aguantado el "ladrillazo" hasta aquí estaréis conmigo en que todo se resume como siempre, en dos palabras: **CONTROL PARENTAL**

Los tres peligros

En esta entrada voy a hacer un pequeño resumen de una charla que di recientemente colaborando con la Fundación Alia2 sobre los peligros de los menores en la Red, en ella tratamos los tres peligros principales a los que se enfrentan nuestros menores en la Red, denominados por algunos como **"los tres ING" por la terminación del término que los identifica.**

Cuando hablamos de los peligros en la Red, en la que son víctimas los más pequeños, rápido nos viene a la cabeza la figura del ciberdepredador comentada, analizada y radiografiada en este libro.

Es cierto que los peligros que corren los menores ante *boylovers*, pedófilos o pederastas revisten un grave peligro, muchas veces irreparable para el menor y por ello **tenemos que estar siempre "ojo avizor"** ante esta calaña, conociendo sus movimientos en la Red para evitar que consigan sus objetivos.

CIBERACOSO SEXUAL HACIA MENORES *(GROOMING)*

Esta acción podría catalogarse como **el primer ING, *el groomING.*** Esta actividad encaminada a acosar sexualmente al menor **es siempre cometida por un adulto hacia un menor** que, ayudándose de las nuevas tecnologías, y una vez ganada la confianza y creada una conexión emocional con el niño, encamina toda su actividad a iniciar con el menor una relación sexual, primero virtual y posteriormente física,

no dudando en coaccionar y amenazar al menor con el único fin de conseguir su objetivo.

La peligrosa pedofilia no es el riesgo más frecuente para los niños en Internet.

Tal vez exista una falsa creencia que nos ciegue para no ver otros peligros a los que se enfrentan los menores. Peligros con mucha mayor incidencia negativa durante el paso por Internet de niños y adolescentes: **el *sextING* y el *ciberbullyING* (los dos ING restantes).**

Mayor incidencia negativa no solo porque es mayor el número de casos, sino porque en muchos de ellos tanto el autor como la víctima suelen ser menores o adolescentes.

¿QUÉ ES EL *SEXTING*?

Segundo ING, el *sexting* (contracción de *sex* y *texting*) comenzó haciendo referencia al envío de mensajes de naturaleza sexual y con la evolución de los teléfonos móviles, ha derivado en el envío de fotografías o vídeos de contenido sexual.

Consiste en enviarse fotografías o vídeos erótico/sexuales de uno mismo o reenviar los recibidos, a través de las nuevas tecnologías pero normalmente usando los teléfonos móviles.

A priori, esta actividad normal en el mundo de los adolescentes, no reviste ningún peligro. Suelen ser imágenes tomadas, por norma general, en el seno de una relación afectiva. Pero cuando esa relación se rompe…

Lamentablemente estas imágenes terminan en Internet, de forma descontrolada, debido al despecho que se tiene con la antigua pareja y es aquí cuando empieza el problema. Esas imágenes que circulan libremente por la Red pueden caer en manos de cualquiera y esto es un verdadero peligro ante el cual la mayoría de los menores son inconscientes, el enviar fotografías explícitas que pueden ser armas utilizadas por ciberdepredadores, con el peligro añadido de que una fotografía puede aportar más datos que los que solo se ven.

Una fotografía puede contener, en la información oculta (metadatos) los datos exactos de donde se tomó la misma, un *smartphone* es capaz de guardar esa información en las fotografías que se hacen con este tipo de terminales.

La publicación de los contenidos, por terceras personas y de forma descontrolada, puede ocasionarle a los menores graves problemas emocionales y psicológicos.

¿QUÉ ES EL *CIBERBULLYING*?

Para terminar voy a explicaros el tercer ING. El ***ciberbullying.***

Según el Instituto Nacional de Tecnologías de la Comunicación **(INTECO)** define que el *ciberbullying* supone la difusión de información lesiva o difamatoria en formato electrónico a través de medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales o la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de vídeos y fotografías en plataformas electrónicas de difusión de contenidos.

El anonimato, la no percepción directa e inmediata del daño causado y la adopción de roles imaginarios en la Red convierten al *ciberbullying* en un grave problema.

Es una práctica muy extendida en el ámbito escolar, que en ocasiones se sale de los conceptos y se hace extensivo a los adultos que están en este círculo del menor, haciéndose, lamentablemente, demasiado rutinario el acoso a los profesores.

Como veis, hay algo más que pedofilia en la Red que puede mermar la armoniosa actividad de los niños y adolescentes en la Red, las tres ING las cuales pueden terminar, lamentablemente, con graves consecuencias para los críos y en muchas de las ocasiones de forma irreparable.

Hemos visto a los menores como víctimas y tenemos que cuidarlos, informando y educando para evitar que caigan en redes de ciberdepredadores o que sean el objetivo de las "peligrosas gracietas" de sus "exnovietes" o compañeros de actividades escolares. **Todo esto lo podemos conseguir con un debido CONTROL PARENTAL.**

Pero como ya habréis deducido, el peligro de las tres ING, no solo se queda en el menor como víctima, sino que, en muchos de los casos el menor o adolescente es también él responsable de estas acciones “delictivas”.

Las fuentes del peligro

En líneas generales, los principales riesgos a los que se enfrentan los menores en la Red ya los hemos tratado en este libro, son los que presentamos como los tres ING *(grooming*, *sexting* y *ciberbullying)*.

Presentamos en las distintas entradas cómo detectarlos, cómo evitarlos y cómo luchar contra estos riesgos.

Veíamos que el *grooming* era producto de la actividad de los ciberdepredadores para conseguir hacer realizadas sus más perversas fantasías sexuales, en las que siempre aparecen como protagonistas los más desprotegidos, los niños.

Hablábamos de los peligros del *sexting*, actividad que iniciada por los menores podría conllevar a escenarios de extremo peligro, enlazándose con *grooming* o ciberacoso.

También quedaron claras las graves consecuencias del *ciberbullying*, tanto psicológicas para la víctima, como penales para el autor. Apuntábamos que el *ciberbullying* era considerado como tal cuando tanto el autor como la víctima eran menores, puesto que si no fuese así adoptaría el nombre de ciberacoso, aunque sinceramente me da igual que me da lo mismo, como se suele decir, las consecuencias son las mismas salvo por la gravedad que las “figuras” protagonistas recaen en menores en el primero de los casos.

Estos tres ING, han sido presentados como peligros hacia los niños, pero ni que decir tiene que los tres pueden darse también entre adultos. En ese caso le pondríamos otros nombrecitos, como sextorsión, ciberacoso, y vete tú a saber cuántos nombres más, y si son términos de origen anglosajón mejor, por aquello que "visten más", pero no me quiero alejar de el motivo de este artículo, **¡PROTEGER A LOS NIÑOS EN LA RED!**

Una vez conscientes y conocedores de los principales peligros que acechan a nuestros hijos en la Red, creo que sería conveniente que conociésemos el origen de todo esto, dónde comienza todo y por qué.

Si sirve de algo mi humilde opinión al respecto, creo que el origen de los peligros a los que se enfrentan nuestros pequeños se podrían englobar en tres grupos diferenciados:

1. **Por los contenidos que pueden llegar a consumir los menores.**
2. **Por la interacción de los menores en la Red con otros internautas.**
3. **Por la falta de conciencia a la hora de proteger su propia seguridad y privacidad.**

Contenido inadecuado en Internet para menores

Es evidente que Internet es una herramienta educativa de bondades incalculables, que facilita a todo tipo de usuario una gran cantidad de información y contenidos, especialmente importantes en el proceso de aprendizaje de los niños.

Discernir en cuanto al tipo de contenidos que pueden consumir los niños creo que no debería ser un problema para ningún padre o educador, puesto que, como adultos, deberíamos ser conscientes de los contenidos que pueden ser perjudiciales e incluso peligrosos para ellos.

Creo que el principal problema al que nos enfrentamos es que los menores no son conscientes en muchas ocasiones de los riesgos que conlleva el consumo de contenido adulto, en este caso en Internet. En Internet no existe la "censura" por lo que **contenidos relativos a la pornografía, violencia, temas de anorexia, contenidos xenófobos, drogas, sectas, etc. están al alcance de todos en Internet, y también de los niños.**

Contenidos que pueden ir más lejos que el mero "consumo" de material inadecuado para un niño, puesto que incluso pueden poner en peligro sus vidas (páginas de anorexia y bulimia), así como las llamadas páginas de muerte, que incitan al suicidio, o los juegos *on-line* de extrema violencia, son claros y peligrosos ejemplos.

Muchas veces esto es consecuencia del total desentendimiento hacia los niños, de la ausencia de la figura adulta que supervise y proteja la actividad del menor en la Red, de la ausencia total del llamado **CONTROL PARENTAL.**

Pensaréis que llegar a estos contenidos es muy complicado para un menor, pero estáis muy equivocados. Con apenas tres *clicks* de ratón un niño que comienza su navegación en una página de sus dibujos animados preferidos, puede llegar a este tipo de contenidos peligrosos e inapropiados.

Podéis hacer la prueba vosotros mismos, seguro que ya habréis comprobado en alguna ocasión que muchas páginas web se sirven de anuncios *on-line* o *banners* con el pretexto de hacer publicidad, cuando lo que en realidad están haciendo es conducir al internauta a alguna página pornográfica o de juegos *on-line*.

En este aspecto es muy importante el controlar para proteger de los contenidos que pueda llegar a visitar el menor en Internet.

Pero como casi siempre vamos a intentar proporcionaros solución a este problema, es algo que seguro no habéis oído hablar nunca y además difícil de pronunciar, me refiero al CONTROL PARENTAL.

Interacción de los menores con otros internautas

Otra fuente de peligrosidad a la que se enfrentan los niños es su propia "actuación" en la Red. Desde la llegada de la Web 2.0 han proliferado numerosas salas de chat, juegos *on-line*, redes sociales y mundos virtuales especialmente dirigidos a los menores.

Si leísteis el artículo "Radiografía de un ciberdepredador", recordaréis que presentábamos a estos "monstruos" como verdaderos cazadores y poníamos algún símil con los cazadores o pescadores que buscaban sus presas en su "hábitat natural". Recordaréis también que decíamos que estos depravados buscaban a sus víctimas en salas de chat, páginas web, juegos y redes sociales frecuentadas por menores.

Además del grave riesgo de los crímenes sexuales que acechan en la Red, queda claro que **l**os menores y adolescentes en la actualidad están más fuertemente motivados a comunicarse *on-line* que cara a cara, cuantos más amigos tengan en sus perfiles de redes sociales más "guays" son en su círculo "real". **En la mayoría de los casos el concepto de amistad está totalmente desvirtuado, considerando amistad a cualquier persona que solicite ser agregado en su perfil, y dada la facilidad de comunicación en la Red, esta persona comienza a ser desde ese momento su principal "confesor".**

También es lógico el contacto entre menores que se conocen en un círculo real (colegio, residencia, actividades lúdicas, etc.), esto potencia el conocer virtualmente al amigo del amigo del amigo, es decir, ¡a nadie! Incluso esta forma de "ciberamistad" conlleva y potencia la tiranía que todos llevamos dentro en algunas ocasiones, y aprovechando o bien el falso anonimato que nos da la Red o bien la falsa impunidad que nos proporciona, pueden llegar a ser tanto víctimas o autores de actividades con graves consecuencias para ambos (hablábamos anteriormente del *ciberbullying* y *sexting*).

Por ello es muy recomendable la educación, inculcar al menor que debe comportarse como lo haría en la vida real y que ante cualquier problema que le pudiera surgir tiene a sus padres y profesores para ayudarle y para subsanar el problema sin la necesidad de llegar a "males mayores".

Pero como casi siempre vamos a intentar proporcionaros solución a este problema, es algo que seguro no habéis oído hablar nunca y además difícil de pronunciar, me refiero al CONTROL PARENTAL.

Falta de conciencia en cuanto a seguridad y privacidad en la Red

En los apartados anteriores ya hemos visto que muchas veces por ingenuidad y otras por la falta de conciencia ante la importancia de proteger su propia privacidad, **los menores facilitan alegremente su más preciado tesoro en Internet, su privacidad en perjuicio de su propia seguridad** y la de su entorno, facilitando información que solo debería ser conocida por los círculos más próximos poniéndose, en ocasiones, en grave peligro a sí mismo e incluso a su propia familia.

Los conocidos como ciberdepredadores, empleando técnicas psicológicas de ingeniería social y utilizando falsas identidades, se acercan al menor ganándose su confianza poco a poco, una labor muy trabajada y meticulosa que tiene como único fin el mantener conversaciones privadas con el niño para conseguir sus propósitos, a veces virtuales pero en muchas ocasiones logran citarse con los pequeños para llevar a cabo sus peores propósitos. Por otro lado, tarea fácil para el ciberdepredor, dado que se aprovechan de la ingenuidad de los críos para conseguir de ellos información personal tanto de ellos como de sus familias, para que *a posteriori* sea más sencillo contactarlos y localizarlos.

Hablábamos de la facilidad de comunicación de los menores y adolescentes por Internet con otros internautas, superando el interés de la comunicación *on-line* a la comunicación personal.

Para un menor o adolescente, lamentablemente, en muchas ocasiones su éxito social se basa en la gran cantidad de amigos que tiene en la Red; personas que en su vida real no tendrían ninguna cabida, pero en la Red "todo vale" posiblemente para compensar el vacío de "habilidades sociales", por lo que se ven incentivados a proporcionar más información sobre sí mismos a sus amigos virtuales ante el convencimiento de que cuanta más privacidad comparten más amigos tienen y más amigos son.

Es muy recomendable hablar con los pequeños de los peligros que pueden entrañar ciertos comportamientos en Internet, advertirles de las "falsas" amistades de Internet, advertirles de que si desconocidos intentan conversar con ellos en Internet deben eludirles y contárselo a sus padres o profesores, que si por cualquier motivo llegasen a participar en esas conversaciones, con desconocidos o con esos "falsos amigos", nunca deben dar información personal y de localización (como dirección, teléfono, nombre del colegio o lugares que frecuentan).

Por supuesto, ni que decir tiene que, bajo ningún concepto deben enviar fotografías suyas o de sus familiares, vestidos o desnudos, y aconsejarles que siempre se debe utilizar un pseudónimo o *nick* que no le identifique por su nombre, edad, residencia, etc.

En otras ocasiones los adolescentes pretenden mostrar un perfil más adulto en Internet de lo que realmente son, o bien para eludir la imprescindible mayoría de edad exigida en ciertos medios, en redes sociales como Tuenti y Facebook es necesario tener al menos catorce años para crear un perfil y que no es de fácil comprobación. O bien ante la búsqueda de los desconocidos ante ciertos contenidos adultos y que solo siendo "más mayores" pueden acceder.

Pero como casi siempre vamos a intentar proporcionaros solución a este problema, es algo que seguro no habéis oído hablar nunca y además difícil de pronunciar, me refiero al CONTROL PARENTAL.

No, no me he confundido, el párrafo anterior está repetido tres veces a lo largo de este artículo, es cierto, como siempre digo, que Internet tiene muchos peligros, pero también nos ofrece, a todos, muchas bondades, y a los más pequeños también como enorme fuente de educación e información.

No os olvidéis de la importancia del CONTROL PARENTAL siempre que un niño se acerque a un ordenador.

4. CONTROL PARENTAL

Cuando los viejos del lugar empezamos a disfrutar de Internet solo éramos conscientes de lo que la Red nos ofrecía, pero no de los peligros que tras nuestros módems se escondían.

Hace quince años, inconscientes de nosotros, dejábamos solos ante el peligro a nuestros hijos, solos en sus habitaciones donde nada les podía ocurrir, estaban totalmente "controlados" y además entretenidos disfrutando de los contendidos de Internet para menores. Nada les podría suceder y mientras tanto, nosotros disfrutábamos de la tranquilidad en el salón viendo nuestra película favorita sin ser molestados.

En las entradas de este libro, en las que explicamos los peligros a los que se enfrentan los menores en Internet *(Menores en la Red),* terminamos siempre con un consejo, de forma directa o indirecta siempre terminamos diciendo dos palabras**: CONTROL PARENTAL.**

El control parental, en la mayoría de los casos, es confundido con una actividad digna del famoso "Agente 007" en misión espiar a nuestros hijos.

Pero esa idea se aleja completamente de la realidad.

¿Qué es el control parental?

Recordaréis vuestras primeras salidas al parque, siempre acompañados de vuestros mayores, controlando que no tuvierais ningún problema y supervisando todo lo que hacíais, y sobre todo verificando que vuestros compañeros de juego fuesen apropiados.

Ya habréis leído, si seguís este libro, las míticas frases que nos decían nuestros mayores cuando empezaban a darnos "alas" y no nos mantenían tan "controlados": "No hables con desconocidos", "no aceptes caramelos de personas que no conozcas", "no te subas al coche de un extraño", "no abras la puerta a nadie mientras te encuentres solo en casa".

En estos dos párrafos hemos descrito qué es el famoso CONTROL PARENTAL. Como veis nada que ver con el espionaje, simplemente es una supervisión de la actividad de los menores hasta que son capaces de "volar" solos y siempre tras un período de aprendizaje controlado.

¿Es posible el control parental en Internet?

Es posible sin duda, simplemente tenemos que continuar la labor que hacían nuestros padres empleando métodos educativos y de información hacia nuestros hijos en su paso por la Red, combinándolos con las nuevas tecnologías.

Supervisando, educando e informando, **NO ESPIANDO** sus movimientos en la Red, esto podría ser perjudicial dado que el menor podría rechazar incluso la participación de sus padres en este tipo de actividades.

En resumen, podemos utilizar dos tipos de control:

- **Control activo:** educando, informando y estando pendientes directamente de las actividades de nuestros hijos.
- **Control pasivo:** ayudándonos de "herramientas" específicas que controlen que nuestros hijos no accedan de forma involuntaria a contendidos impropios para ellos en la Red.

La Fundación Alia2 (entidad sin ánimo de lucro que trabaja para proteger los derechos de los menores en Internet, fomentando un uso seguro y responsable de la Red) publicó un interesantísimo artículo "Límites en el uso de Internet: ¿Deben los padres controlar, vigilar o prohibir?" lo podéis leer íntegramente su página web: http://www.alia2.org

¿Qué conseguimos con un control parental en Internet?

En este apartado podríamos escribir muchísimo, por eso me voy a limitar a citar lo que he leído en http://control-parental.es.tl/

> "Cualquier colectivo peligroso en el que a ningún padre le gustaría ver metido a su hijo está en Internet.
>
> Grupos antisistema, webs sobre anorexia, cómo cultivar drogas, armas, extremistas de izquierda o derecha, sectas religiosas, juegos de azar, apuestas deportivas, subastas *on-line,* descarga de música y cine. Todos están ahí. Y los niños, y más a determinadas edades, no saben qué es lo que está bien y mal. Qué es verdad y qué mentira. Y cuánto vale el dinero. Aquí no hay dos rombos para advertir. Prohibir no es la solución. El día de mañana va a necesitar utilizarlo. Y además, sus compañeros se están comunicando a través del Messenger y otros programas similares. Si se les prohíbe, se les está aislando.
>
> No es nuestra intención crear alarma. La alarma ya está creada. En mayor o menor medida todos hemos oído hablar de problemas relacionados con Internet. Pretendemos informar y aconsejar posibles soluciones a los variados problemas que han ido surgiendo como consecuencia de un mal uso del ordenador."

¿De qué herramientas disponemos para tener un buen control parental?

Hoy en día ya es impensable el tener un ordenador sin la protección de un antivirus. Sabemos que un antivirus, como hemos visto en este libro, no es suficiente para mantenernos libres de virus, tenemos que utilizar también el sentido común. Pues igualmente deberíamos concienciarnos, si tenemos hijos pequeños, que deberíamos siempre de disponer de herramientas específicas de control parental.

Son muchas las herramientas de las que disponemos para poder ejercer un control parental más o menos eficiente, tanto de pago como gratuitas.

El Instituto Nacional de Tecnologías de la Comunicación (INTECO) ofrece en su página web un buen listado de útiles gratuitos.

http://cert.inteco.es/software/Proteccion/utiles_gratuitos

En la misma línea se encuentra la **Oficina de Seguridad del Internauta (OSI)** en su objetivo de fomentar la cultura de la seguridad en Internet entre los más pequeños. http://menores.osi.es/

Además de programas específicos, también podemos configurar nuestro navegador para bloquear sitios web o filtrar contenido perjudiciales para los niños:

- **Firefox:** http://support.mozilla.org/es/kb/Control%20parental
- **Explorer:** http://windows.microsoft.com/es-es/windows-vista/Set-up-Parental-Controls
- **Google:** http://www.google.com/familysafety/

Consejos para un uso más seguro de la Red por menores

Para evitar que los niños caigan en páginas no aptas para menores, existen varios medios, pero el más importante son los propios padres o tutores bajo el **imprescindible** control parental. Sería conveniente que enseñéis a los niños, a partir de los trece años, a navegar dándoles ciertas confianzas, **JAMÁS** descuidarnos y confiarnos, pero sí comenzar a que sepan convivir con unas normas básicas para utilización de la Red según ***cibermanagers***[68]***:***

[68] ***Cibermanagers*** es un novedoso proyecto basado en una metodología que aporta y conjuga las potencialidades de dos estrategias: el aprendizaje y servicio solidario y la educación entre iguales. http://www.cibermanagers.com.

- **Ten cuidado con las fotografías que subes y nunca manejes ninguna comprometedora.**
- **Tapa la *webcam* y no te fíes de quien está al otro lado.**
- **Pide ayuda a una persona adulta en caso de problemas.**
- **Usa contraseñas seguras, protégelas y cámbialas de vez en cuando.**
- **Ten precaución con las personas nuevas que contactas en la Red. Ten especial cuidado con los contactos que agregas.**

En edades más tempranas no debemos dejar nunca al menor ante el "el peligro de la falsa soledad" en la Red. Cualquier página, por muy infantil que nos parezca puede contener algún tipo de contenido no apto para ellos, o incluso algún *link* publicitario o enlace a contenidos inapropiados para ellos.

5. MENORES RESPONSABLES PENALMENTE

Cuando el menor es el responsable de ciertas actividades delictivas cometidas a través de Internet, lo es en la mayoría de los casos por **la creencia del falso anonimato que nos otorga la Red,** pero en la mayoría de las ocasiones lo es ante el convencimiento de que **"¡Como soy menor no me pueden hacer nada!".**

Muy lejos de la realidad en ambos casos. Aunque en cuanto al anonimato en la Red es cierto que se pueden "camuflar" las conexiones a Internet, pero estas acciones no resultan tan efectivas como se pretende, y menos en estos casos en los que se limitan a cambiar su pseudónimo, perfil o correo electrónico.

Con este apartado vamos a volver a retomar los peligros que acechan a nuestros menores en Internet y lo haremos presentando un nuevo peligro, o mejor dicho, una nueva "falsa conciencia" resultante de la combinación de las anteriores. Y no es un peligro nuevo por lo novedoso, sino precisamente por la falta de conocimiento.

Me refiero al extendido sentimiento de que: **"En Internet puedo hacer lo que quiera, nadie me va a reconocer"** y ello sumado a otro erróneo concepto de impunidad: "**Como soy menor no me pueden hacer nada".**

Los adultos, padres, educadores, tutores, etc., debemos abrir los ojos, debemos ser conscientes de estos conceptos erróneos, si recordáis en otro artículo hablábamos de la necesidad de conocer **la fuente de los peligros** para evitarlos. Para abrirnos los ojos solo tenemos que conocer **la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.**

No voy a entrar en conceptos jurídicos porque para ello tenemos un buen referente en la Red, me refiero a mi buen **"ciberamigo"** y **"ciberjurista" Juan Antonio F. A., @alegrameeeldia** en Twitter y que nos acerca el mundo del derecho a los internautas con su blog:

http://enocasionesveoreos.blogspot.com.es

Si bien creo necesario transcribir el primero de los puntos del primer artículo de esta Ley:

"*Artículo 1. Declaración general.*

Esta Ley se aplicará para exigir la **responsabilidad de las personas mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos o faltas en el Código Penal** o las leyes penales especiales."

Creo que con este primer punto del artículo y que abre la Ley, queda suficientemente claro lo que quiero trasladaros para que seamos todos conscientes y podamos **"informar y educar"** a nuestros menores para que utilicen la Red de forma responsable.

Esta ley viene a decir que los menores mayores de catorce años y menores de deciocho son **RESPONSABLES PENALMENTE** de sus actos, quedando exentos de

esta responsabilidad los menores de esas edades, pues en ese caso no se le exigirá responsabilidad penal, sino que se le aplicará lo dispuesto en las normas sobre protección de menores previstas en el **Código Civil.**

Pero en ambos casos, **cuando el responsable de una falta o delito sea un menor de dieciocho años responderán solidariamente junto a él, sus padres o tutores por los daños y perjuicios causados.**

Menor autor

Como queda de manifiesto en la ley que regula la responsabilidad penal del menor, los menores pueden ser responsables de cualquier tipo de delitos que comentan de acuerdo al Código Penal español. Por tanto, sus irresponsabilidades, también conllevarán responsabilidad cuando se cometan a través de la Red, al igual que cualquier adulto.

Os preguntaréis qué actividades pueden realizar los menores en Internet que pudieran conllevar a estas responsabilidades. Es sencillo, todos hemos oído hablar de los daños provocados en los sistemas informáticos (borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos, programas informáticos o documentos electrónicos ajenos), por supuesto hemos oído hablar de injurias, amenazas, ciberacoso *(ciberbullying),* robo de identidad (usurpación de estado civil) o incluso de acoso sexual, y todo ello por Internet. Pues de todos estos delitos o faltas **pueden ser responsables los menores, unas veces por desconocimiento de la responsabilidad, otras por inconsciencia del falso anonimato en la Red y SIEMPRE por una falta de educación.**

De todos es conocido el problema de *ciberbullying,* recientemente noticia por el lamentable y dramático caso de Amanda Todd, la joven de quince años que no pudo soportar más el *bullying* que sufría y decidió quitarse la vida tras los prolongados tormentos a que fue sometida, primero por un despiadado acosador sexual

y luego por compañeras y compañeros, amigas y amigos suyos, hasta hacerla sentir acorralada ante el precipicio de la muerte.

El peligroso *sexting,* como también vimos en "Los peligros y sus responsabilidades", no es una actividad delictiva en sí por el mero hecho de enviar a otras personas imágenes "comprometidas" o sexualmente explícitas. El *sexting* comienza simplemente por una irresponsabilidad de la víctima, en este caso de un menor que envía una imagen a otro menor. Lo que sí es considerado un delito es el descubrimiento y revelación de secretos. Eso es lo que se le imputaría a ese menor receptor en el momento que difunda la foto que ha recibido, o conseguido por otras vías, indistintamente del medio de difusión que utilice, a través de mensajes de teléfono móvil, redes sociales, correo electrónico, etc.

En un reciente estudio impulsado por un grupo de investigadores de la Facultad de Psicología de Granada desde el 2001, se destaca un llamativo aspecto y es que: "Aproximadamente el 50% de los agresores de abusos sexuales son menores de edad, y dentro de eso hay un grupo de niños, preadolescentes o niños". Lamentablemente demasiado común. En ocasiones, posiblemente, porque el menor comienza a descubrir su sexualidad e inicia su particular "investigación", escudado bajo la "falsa soledad" de su habitación y el falso anonimato que la Red le proporciona al no utilizar su nombre real o falseando su perfil en redes sociales.

También es de todos conocido el excesivo número de casos en los que profesores son víctimas "gratuitas" de agresiones físicas que luego son "colgadas" en la Red, o psicológicas mediante campañas de *bullying* trasladadas a Internet y las nuevas tecnologías. Los vídeos de móvil, las redes sociales o portales como Youtube son las nuevas herramientas de algunos alumnos para arremeter contra sus maestros.

Por todo ello tenemos, y debemos, informar y educar a nuestros hijos para que utilicen Internet de forma responsable, hay que enseñar a los menores que lo que se hace en Internet tiene las mismas consecuencias que lo que se hace en la vida real, concienciarles de que **todas estas "actividades delictivas" no resultan "tan baratas" como se imaginan.**

Pero para ello tenemos, y debemos, concienciarnos e informarnos nosotros mismos primero.

Consecuencias

Las medidas susceptibles de ser impuestas a los menores quedan establecidas en el artículo 7 de la Ley de Responsabilidad Penal del Menor.

Pero en líneas generales las medidas que pueden imponer los jueces de menores, pueden ser cualquiera de las siguientes:

- Internamiento en régimen cerrado.
- Internamiento en régimen semiabierto.
- Internamiento en régimen abierto.
- Internamiento terapéutico.
- Tratamiento ambulatorio.
- Asistencia a un centro de día.
- Permanencia de fin de semana.
- Libertad vigilada.
- Obligación de someterse a programas de tipo formativo.
- Prohibición de acudir a determinados lugares.
- Prohibición de ausentarse del lugar de residencia sin autorización judicial.
- Obligación de residir en un lugar determinado.
- Obligación de comparecer personalmente ante el Juzgado de Menores o profesional que se designe.
- Cualesquiera otras obligaciones que el juez, de oficio o a instancia del Ministerio Fiscal, estime convenientes para la reinserción social del sentenciado.

- Convivencia con otra persona, familia o grupo educativo.
- Prestaciones en beneficio de la comunidad.
- Realización de tareas socio-educativas.
- Amonestación.

Algún ejemplo:

laopinion.es » **Sucesos**

Granadilla

Un menor, detenido por amenazar por Internet a sus compañeros

Ha sido detenido como supuesto autor de las amenazas a más de veinte de sus compañeros de instituto

elcorreo.com

Edición: Bizkaia | Ir a Edición Araba/Álava | Personalizar

Portada Local Deportes Economía Más Actualidad Gente y TV Ocio Participa Blogs Servicios Hemeroteca IR

Política Mundo Sociedad Cultura Vidasolidaria Salud Tecnología e internet Final de la violencia de ETA elcorreo .tv

Estás en: Bizkaia - El Correo.com > Noticias Más Actualidad > Noticias Sociedad > **Detenido un menor por hacer chantaje sexual por Internet**

ACOSO EN LA RED

Detenido un menor por hacer chantaje sexual por Internet

Se hacía pasar por una chica en Tuenti, conseguía fotos de otros adolescentes desnudos, y luego les extorsionaba para tener relaciones sexuales

18.06.12 - 02:33 - EL CORREO | MADRID.

DELITOS INFORMÁTICOS .COM

Inicio | Consultas jurídicas | Adecuación a la LSSI | Protección de datos | Contratos

Detenido un menor que acosaba a otros a través de Internet

22. mayo 2012 | Por Editor | Categoria: Acoso, Noticias

Y muchas otras noticias que podemos encontrar en los medios de comunicación en las que tanto las víctimas como los autores son menores, los siguientes casos se han extraído de *El blog de e-Legales.*

- Dos adolescentes roban la identidad a un internauta para extorsionarle en una red social.
- 5.000 euros de multa por burlarse de una desconocida en una red social.
- Un menor madrileño acusado de dos delitos por realizar *grooming* a una compañera del instituto.
- Acusados de extorsión dos menores por atraer adultos con anuncios falsos de prostitución en Internet.
- Condenado por burlarse de un compañero en Tuenti.
- Imputados seis jóvenes por un delito al honor tras colgar un montaje de una joven en Tuenti.

¿Suficiente?…

V
ARTÍCULOS

En este capítulo del libro quedarán plasmados los artículos publicados en *El Blog de Angelucho* y que no se ha visto conveniente su inclusión en cualquiera de los capítulos precedentes, pero que se hacen necesarios para la continuidad de la filosofía del libro *Informar y Educar X1Red+Segura.*

En alguno de ellos se puede apreciar el cúmulo de distintas de las amenazas explicadas y desarrolladas en el libro y que son frecuentemente utilizadas por los ciberdelincuentes para su beneficio y siempre en perjuicio del usuario menos informado de la Red.

1. SEAMOS NUESTRO PROPIO CSI

Analizando correos fraudulentos

En esta entrada vamos a ir un poquito más allá, quiero haceros llegar y concienciaros como siempre de una alerta real que existe en Internet, pero además quiero intentar transmitiros la forma de poder detectar este tipo de “problemas” por vosotros

mismos. Entramos en materia un poquito más técnica, pero como siempre voy a intentar "traduciros" todo para que sea de la forma más comprensible posible para todos, vamos a meternos un poquito en el papel de los **CSI de Internet,** pero de forma sencilla. Que me perdonen los **GRANDES** ***(ellos se reconocerán).***

Una amiga, María, me comenta que ha recibido un correo electrónico un poco "extraño", y que os cuento a continuación.

La situación es la siguiente: María recibe un correo electrónico de una amiga, de las de toda la vida, pero que desde hace algún tiempo solo mantiene contacto por este medio y por redes sociales dado que cada una de ella se encuentra en un país distinto, María en España y su amiga en Costa Rica.

Estos son los datos de este primer correo (omito los datos reales, ya sabéis, temas de privacidad):

"Date: Mon, 25 Jun 2012 06:18:37 -0700

From: ########@yahoo.com

To: ######@hotmail.com

Hope you get this on time,sorry I didn't inform you about my trip in Spain for a Program, I'm presently in Spain and am having some difficulties here because i misplaced my wallet on my way to the hotel where my money and other valuable things were kept. presently i have limited access to internet,I will like you to assist me with a loan of 2,950 Euros to sort-out my hotel bills and to get myself back home

i have spoken to the embassy here but they are not responding to the matter effectively,I will appreciate whatever you can afford to assist me with,I'll Refund the money back to you as soon as i return,let me know if you can be of any help.I don't have a phone where i can be reached

Please let me know immediately

Best Regards

########

Para los que entendéis perfectamente inglés, salvo por la preocupación de los problemas de la persona que os envía el correo, nada más, ¿verdad?, el correo viene a decir que esta persona se ha desplazado a España, y tras haber tenido problemas se encuentra sin medios económicos e incluso su Embajada, al no ser española, le da la espalda. Necesita la cantidad de 2.950 euros para saldar su deuda con el hotel y poder volver a su país.

Estas dos personas SIEMPRE se comunican en castellano, eso hace dudar a María y asustada por la posible grave situación de emergencia de su amiga decide contestarla urgentemente para hacerle las preguntas lógicas, ¿eres tú?, ¿estás en Madrid y tienes algún problema?

La contestación no tarda, nuevamente en pésimo inglés como veis a continuación:

"Date: Mon, 25 Jun 2012 14:04:30 -0700

From: ########@yahoo.com

Subject: Re: Eres tu? To: ######@hotmail.com

Thanks for your kindness and response towards my predicament,your mail brought me a huge relief,I have made inquiry on how you can transfer the money to me and I was told that Western Union Money Transfer is the easiest and fastest way to transfer money to Spain.here is my details below

Receiver's: Names : ###### #### (nombre real de la amiga de María)

Receiver's Address: St Francisco Vitoria ###

Zaragoza, 50008

Spain

Once again ,i am very grateful for your concern,write me immediately, so i know when the money has been wired,kindly help me scan a copy of the receipt given to you or help me write out the necessary details on the receipt

Please I will be waiting to hear from you soon

Thanks
#########"

Esta vez, la supuesta amiga de María le expresa lo aliviada que se siente al tener noticias de María y le dice que le envíe el dinero a través de Western Union a una dirección en Zaragoza, siendo ella misma la única beneficiaria de la transferencia.

Bien, hasta aquí la historia contada por María, y es a partir de aquí donde empezamos a ver la verdadera "cara" de estos correos.

A priori, el texto en sí de los correos no nos dice demasiado salvo que la persona que escribe lo hace de forma pésima en inglés, y que por lógica no es la amiga de María, puesto que siempre se comunican en castellano.

El correo de origen, el de la amiga de María, es el correo real de esta persona, con lo cual caben dos posibilidades:

1. ***Hackeo*** **de la cuenta de la amiga de María y que alguien haya accedido a la cuenta para enviar este tipo de correos a personas que aparezcan en la propia agenda de contactos de la verdadera titular.**

2. **Que el correo haya sido enviado utilizando un "servicio anonimizador" de correos, con lo cual en el *"from"* (correo origen) podemos poner lo que nos de la real gana, haciéndonos pasar por cualquier correo real.**

María confirma por otro medio que no ha sido su amiga quien le ha remitido el correo y que le han *hackeado* la cuenta de correo.

Lo primero que tenemos que averiguar es desde donde le han enviado el correo a María, para verificar que efectivamente no ha sido su amiga quien lo remitió. El texto escrito en el *e-mail* no nos lo va a decir, **tenemos que** "investigar en las tripas del correo", cojamos nuestra lupa de investigadores y a la faena…

¿CÓMO PODEMOS SABER DESDE DONDE NOS LLEGA UN CORREO?

Digamos que cuando nos envían un correo electrónico nosotros solo vemos lo que hay dentro del sobre, **comparándolo con el ANTIGÜO correo postal,** ¿lo recordáis?, ese que se escribía en un papelito y luego se metía en un sobre donde se ponían los datos del destinatario, para que llegase la carta, pero también nuestros datos, los del remitente, por si la carta no encontraba su destinatario y nos la tenían que devolver.

En este sobre se estampaban, además del sello de correos, matasellos de por donde pasaba nuestra carta desde el origen al destino.

En Internet las conexiones se identifican mediante las llamadas conexiones IP, que se asemejan a las direcciones postales con el nombre, número y ciudad donde residimos, o donde reside la persona a quien enviamos el correo. Estas IP nos las asigna cada proveedor de servicios de Internet–ISP (la compañía que nos provee de Internet), y **son únicas a nuestra conexión, es decir, no pueden existir el mismo día y a la misma hora dos conexiones con la misma dirección IP.**

Los datos relativos a las IP de los usuarios de Internet son datos de carácter personal y por lo tanto están sometidos a la normativa europea y nacional de protección de datos, protegidos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal LOPD, con lo que no vamos a poder saber, salvo que tengamos un "amparo" legal (orden judicial), a quién pertenece una IP en concreto un día y a una hora determinada, pero lo que sí podemos

saber es la geolocalización de la IP puesto que éstas son asignadas por "tramos" a cada país, y dentro de cada país a su vez a cada proveedor de servicio, pudiendo incluso a geolocalizar la ciudad de la conexión, pero no al titular de la línea.

Pues bien, sabiendo que en Internet también existen las "direcciones postales" (IP) nos encontramos con la grata sorpresa de que en un correo electrónico también existe ese "sobre" que se utiliza en las cartas postales, lo que pasa es que nosotros no lo vemos normalmente, pero podemos configurar nuestro gestor de correo electrónico para verlo.

El "sobre" de un correo electrónico se llama CABECERA TÉCNICA y se puede ver si a nuestros gestor de correo le decimos que, dentro de los detalles de las propiedades del mismo, **nos muestre los encabezados de Internet de nuestros correos,** o dicho de otra forma el origen de los correos que recibimos.

Bueno, pues ya sabemos que tenemos opciones para a ver el origen de los correos que recibimos y además que podemos traducir las direcciones de Internet a localizaciones geográficas reales, así que volviendo al caso de María **vamos a ver estos "detalles técnicos"** de los correos en cuestión.

Os pongo a continuación la cabecera técnica de uno de los correos que recibió María, he diferenciado sus partes en colores para traduciros y explicaros su significado:

```
"Mon, 25 Jun 2012 14:04:30 -0700
Received: from [98.139.215.142] by nm4.bullet.mail.bfl.yahoo.com with NNFMP; 25 Jun 2012
21:04:30 -0000
Received: from [98.139.212.196] by tm13.bullet.mail.bfl.yahoo.com with NNFMP; 25 Jun
2012 21:04:30 -0000
Received: from [127.0.0.1] by omp1005.mail.bfl.yahoo.com with NNFMP; 25 Jun 2012
21:04:30 -0000
X-Yahoo-Newman-Property: ymail-3
X-Yahoo-Newman-Id: 581851.4276.bm@omp1005.mail.bfl.yahoo.com
Received: (qmail 74815 invoked by uid 60001); 25 Jun 2012 21:04:30 -0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=sl024;
t=1340658270; bh=VXsU8yyrDU9LkUHE8jzEWOsdwp57caTvkCDsM6a7t7E=; h=X-YMail-OSG:Received:X-
RocketYMMF:X-Mailer:Message-ID:Date:From:Reply-To:Subject:To:In-Reply-To:MIME-
Version:Content-Type:
b=24zkxh5im8OQ5xS8h9WxWnKKCDlXFewbnjQsLoi1D5Qa0J0W62spZ4vwOvQwgbtfX7sd4REcogImxO0pzS+7ST
vl3FogHOYaRlzY3aJvysVZEdy42ts+nN0KCaJJsP2zfWk6+v/3AyUIdAIA/cd2xNJY4ilfGyVzfaTFJuAAxc=
Domainkey-Signature: a=rsa-sha1; q=dns; c=nofws;
  s=sl024; d=yahoo.com;
  h=X-YMail-OSG:Received:X-RocketYMMF:X-Mailer:Message-ID:Date:From:Reply-
To:Subject:To:In-Reply-To:MIME-Version:Content-Type:

b=bXY7eBu2gK916bmY1WmzjNgKfVEOIKtXaJF2+3avsXTI/xaLX5UWadASWUOJVcIwXfsm4Kf2QhzzzE1BIIzgj0
t6ZpxGpDSPDbT6Y1srjyNwi20bK5UUPFNyL6eB/mEyeQKIysNGkopf6Jv5WF120Uy44byF4icmbv2pEOKxtatAs=;
X-YMail-OSG: laHsfs8VM1l5DSWIlTL4hEVG6GvbXo29NtpfY4gmLz7hUOV
 sVEmdqWrVmL9.HrwbJyPxl410qj_UhaLmVQM4wEI6IG_91MOi2r2jEaealj6
 XksgnwSj3WnwEawxGsK_PIH_N1ERaQzk8mskyG7eNSscEXNDT61jNpUj0561
 T5TSR6nvI_AJcmH1T0S37aCE0.zC2XEWEQ1O9EPTrcRsm.ccoWmM180SAwOk
 QQy.h_A0LYpN0rjaeLxyyzjgEASb0qwg8VNYyeE.bN1VqQnP.FPkXEJs9Mql
 FgDxwTlceVjwRUKEm0aw.1OjGCCEgUgtYO0L30sPAx4f3PWRIXoYhfCpLwAy
 m0dc5Mwggyjk1XzexSKFoujIE1SNhQs7x9Q6hu9kQ.DCzpuiqlpNI.1Uk7WV
 mnsyRQFDd5WhLNaGpOqtOLFWwhOz_PA01RlEo84cEQabUmLwxuWzpJCyCF
 3nuQv0zEQ
Received: from [41.139.115.252] by web140904.mail.bfl.yahoo.com via HTTP; Mon, 25 Jun
2012 14:04:30 PDT
X-RocketYMMF: #######
X-Mailer: YahooMailClassic/15.0.8 YahooMailWebService/0.8.118.349524
Message-ID: <1340658270.70694.YahooMailClassic@web140904.mail.bfl.yahoo.com>
Date: Mon, 25 Jun 2012 14:04:30 -0700 (PDT)
From: ####### <#######@yahoo.com>
Reply-To: #######@yahoo.com
Subject: Re: Para tu?
To: =?iso-8859-1?Q?Mar=#########?= <#######@hotmail.com>
In-Reply-To: <BLU163-W2196C4DE1343B9C3418676B5E10@phx.gbl>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="-618166160-284677140-1340658270=:70694"
Return-Path: #######@yahoo.com
X-OriginalArrivalTime: 25 Jun 2012 21:04:30.0548 (UTC) FILETIME=[1D0E6140:01CD5316]

---618166160-284677140-1340658270=:70694
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: quoted-printable

Thanks for your kindness and response towards my predicament your mail=0Abs=
ought me a huge relief.I have made inquiry on how you can transfer=A0=0Athe=
 option=A0 to me and I was told that Western Union Money Transfer is=0Athe e=
asiest and fastest way to transfer money to Spain.here is my=0Adetails belo=
w.

Receiver's Names ######
Receiver's Address:=A0 St Francisco Vitoria ##
=A0Zaragoza, 50008=A0=20
Spain

Once=0Again,i am very grateful for your concern,write me immediately, so =
i=0Aknow when the money has been wired.kindly help me scan a copy of the=0A=
receipt given to you or help me write out the necessary details on the=0Are=
ceipt.

Please I will be waiting to hear from you soon.

Thanks
##########"
```

1

2

3

¿Ya la habéis leído entera? ¡Cuántos símbolos, números y letras raros y sin sentido! ¿Parece *Matrix* verdad?, no os preocupéis, vamos a traducirla.

La última parte, **marcada con el número 3**, es lo que nosotros realmente leemos, pero además contiene algún que otro dato técnico o codificación.

Marcado con el número 2 tenemos la identificación del mensaje, un identificador que da el que provee de servicio de correo electrónico, en este caso Yahoo. com.

Marcado con el número 1 tenemos los pasos que ha ido dando el correo desde que salió del ordenador de la persona que lo envió hasta el ordenador de María. Marca los servidores por donde ha ido pasando.

Dentro de la parte marcada con el número 1 unos apartados llamados ***RECEIVED*** que son las direcciones IP (recordad lo que hemos dicho de ellas, son las comparaciones a direcciones postales pero en Internet). El primer *received* y el último (siempre empezando por abajo) apuntan al servidor del emisor y del destinatario del mensaje.

Pues siguiendo esto que acabamos de decir, vemos que el primer *receveid* que nos encontramos, leyendo desde abajo, es ***Received: from*** **[41.139.115.252].**

O sea, que desde la dirección IP 41.139.115.252 está enviando la amiga de María su correo electrónico.

Tranquilos, ya hemos hecho lo más difícil, ahora solo nos queda saber a qué zona **geográfica corresponde esa IP, y para ello vamos a utilizar algún servidor WHOIS** que no es otra cosa que una base de datos pública en la que tienen almacenadas todas las IP, con lo cual nos van a decir tanto el país desde donde se envió el correo electrónico, como a qué compañía proveedora de servicios pertenece la IP desde la que se envió. Algunos incluso nos la van a geolocalizar, siendo fiable en cuanto al país pero no al 100% en la zona, porque marcan el servidor que provee servicios que puede estar en una ciudad distinta que desde donde realmente se envió el correo. Os pongo el ejemplo que nos ocupa.

Si introducimos la IP que hemos resuelto en la página http://www.adslayuda.com para saber toda la información pública relativa a esa IP nos da el siguiente resultado:

Item	IP	Ciudad	Región	País	IPS	Dominio
41.139.115.252	41.139.115.252	-	-	NIGERIA	MOBITEL NIGERIA LIMITED	-

Bueno, pues ya terminamos nuestra "investigación", vemos que la "amiga" de María le ha enviado el correo desde Nigeria con una conexión a Internet de la compañía MOBITEL NIGERIA LIMITED y desde una ciudad muy cerquita de la capital nigeriana Lagos.

Algo raro, ¿verdad?, pues sí, efectivamente si pensabais que pudiera tratarse de algún tipo de estafa habéis acertado. Es una modalidad más de las llamadas estafas nigerianas que combinan con técnicas *phishing* o de ingeniería social para

el robo de contraseñas y aprovechan los datos robados para contactar con los contactos de las primeras víctimas e incluirlos en el club de los estafados.

Este tipo de estafa no es nueva, lleva funcionando más de cinco años, pero todavía hay "peces" que caen en las redes de estos cibercriminales. NO SE LO PONGÁIS FÁCIL.

2. ¡¡TELEGRAMA URGENTE!!

"Tienes un virus"

En una ocasión recibí el correo electrónico que os pongo en la captura con el asunto de "Telegrama", además en la categoría puede apreciarse que indican **"URGENTE".** ¿Cómo puede ser posible?

¡Qué curioso!, ¿cómo puedo recibir un telegrama por correo electrónico si yo no he dado mi cuenta de correo al servicio postal de correos? Y en caso de que se lo hubiera facilitado, ¿qué sentido tiene enviarme un telegrama por *e-mail*?

Antes de nada busco en el "oráculo" (Google) la cuenta de correo desde donde me envían mi telegrama, el resultado no es otro que lo que me esperaba, se trata de un **correo basura,** vete tú a saber con qué intención.

Pues bien, analizando en las "tripas" del correo electrónico, veo que **el mismo ha sido remitido desde una conexión a Internet (dirección IP) ubicada en Noruega.** Bueno, puede ser normal, allí posiblemente los locales sean más asequibles y como estamos en crisis Correos querrá ahorrarse unos eurillos en el alquiler de su oficina.

Vamos a ver, me corroe la curiosidad, yo quiero saber que me dicen en mi "telegrama" y pulso en: "Haga *click* aquí para abrir su Telegrama", y me aparece:

¡Vaya, parece ser que no va a ser tan sencillo leer mi correo!, ahora resulta que me **tengo que descargar un archivo "datos.exe",** y ese archivo viene desde la dirección IP 209.137.145.143. ¡¡Pero bueno, una IP de los mismos USA!! ¿Tan importante soy? ¿Tanta crisis hay que correos tiene que solicitar ayuda a los americanos para que sufraguen las conexiones de envíos de telegramas?

Bueno, qué le vamos a hacer, voy a ver realmente desde donde me descarga el archivo, no sea que la IP que pongan esté confundida, seguramente problemas de idioma ;-) …

Entre los noruegos y los americanos me están liando, ahora resulta que el *link* de descarga (borrado parte del *link* para evitar descargas involuntarias) apunta a una IP brasileña:

http://201.77.208.83/wcf/helpdesk/Report/UA487IA.asp?script/templates/GCM.....87984546

Me da a mí que esto no va a ser un telegrama, ¿no querrán jugarme una mala pasada?

Me he descargado el archivo, pero voy a ver qué es realmente antes de ejecutarlo. **Recuerdo haber visto una página en la que se podía comprobar si los archivos que me descargo tienen algún virus e incluso comprobar los propios *links* de descarga, esa página se llama https://www.virustotal.com.**

¡Caray con el archivito!, resulta que es reconocido por diecinueve antivirus de cuarenta y dos como un virus peligroso, que es una "nueva variante de SPY Banker.XXX" y que además se recibe en *e-mail* simulando ser un telegrama.

Este virus tiene como misión anular nuestro antivirus, infectar los archivos ejecutables del sistema operativo, crea una unidad compartida C, captura correos electrónicos, roba contraseñas del equipo, modifica el "arranque" de nuestro ordenador para poder ejecutarse cada vez que lo encendamos. Vamos ¡UNA JOYITA!

Menos mal que no he llegado a ejecutarlo, pero si lo hubiera hecho también me dicen en **www.satinfo.es** como **puedo "limpiarme" utilizando ELISTARA 25.41.**

http://www.zonavirus.com/descargas/elistara.asp

3. JUEGOS OLÍMPICOS

¡Cuidado con las estafas 2012!

La situación requiere un esfuerzo olímpico, he estado "corriendo" por los cinco continentes y "navegando" por los siete mares para recopilar información sobre las **ESTAFAS OLÍMPICAS.**

Los *spammers* siguen utilizando los grandes eventos para seguir generando *spam* e infectar ordenadores. Si hace unos meses ocurría con la **Eurocopa 2012,** ahora sucede con los **Juegos Olímpicos "London 2012"** y, concretamente, con la venta de entradas para asistir a los eventos deportivos, sorteos para disfrutar el evento en persona, loterías especiales de las olimpiadas, alquileres inmobiliarios e incluso puestos de trabajo.

Queda menos de un mes para que empiecen las olimpiadas y los ciberdelincuentes han visto una oportunidad en estos eventos deportivos para **crear *spam*** y hacerlo circular a través de los *e-mails* y redes sociales, con el único fin de llenarse los bolsillos.

Durante estos meses previos a la celebración de las olimpiadas, se ha notado un aumento notable en el **bombardeo publicitario.** Los ciberdelincuentes envían correos con excelentes ofertas para adquirir entradas o participar en sorteos para disfrutar del evento en Londres. Los internautas, confiados, clican sobre dichos

e-mails y *links* para **obtener el "premio"** o para enviar datos personales y como consecuencia los PC se infectan o empiezan a enviar *spam* con esos datos.

La celebración de los juegos olímpicos se ha convertido en la ocasión perfecta para que los *spammers* sigan infectando los PC de los usuarios con la creación y el envío de *spam*, sumado a que las vacaciones de verano están a la vuelta de la esquina y los internautas tienen más tiempo para navegar por la Red. El resultado puede ser catastrófico para más de uno.

Según Martin Thorborg, cofundador de **SPAMfighter:** "Los cibercriminales ahora dirigen sus esfuerzos en generar este tipo de bombardeo publicitario **aprovechándose de estos eventos.** Los usuarios, a pesar de conocer las amenazas no suelen poner remedio. Debido a ello, desde SPAMfighter recomendamos tener instalado un filtro *antispam*, tener protegido tanto el PC como otro tipo de dispositivos con programas antivirus y *antispyware,* y evidentemente hacer uso del sentido común cuando recibimos correos".

Probablemente halláis escuchado algo sobre el virus de la antorcha olímpica que se envía a través de *e-mail* a modo de ***HOAX,*** diciendo que no debemos abrir un archivo adjunto de Microsoft Office Power Point 97-2003 o 2007 afirmando que es un virus muy peligroso que abre una antorcha que quema el contenido del disco duro.

A los estafadores de profesión, se les podría alabar su espíritu emprendedor, su creatividad, determinación y diligencia. Pues parecen ser capaces de aprovechar toda ocasión para engañar a la gente más rápido de lo que nosotros nos podemos imaginar. Los Juegos Olímpicos de Londres 2012 no están lamentablemente exentos de tales fraudes maliciosos. A continuación algunos ejemplos de estafas, relacionadas con los Juegos Olímpicos de Londres 2012:

Las estafas nigerianas se suben al carro olímpico

Están circulando correos falsos que **simulan ser enviados por el Comité Olímpico** para recopilar información de las personas e intentar estafarlas. El anzuelo

es un viejo conocido en el mundo de las estafas nigerianas, un suculento **premio relacionado con una lotería.**

En los mensajes se informa a los usuarios que han **ganado la lotería de los Juegos Olímpicos 2012** y para obtener el premio (ochocientas mil libras esterlinas) deben completar un formulario con sus datos. Para darle más seriedad al asunto, el correo t**ambién incluye un documento PDF con el logo de las olimpiadas** e información de contacto, por supuesto el COI se pone en contacto con nosotros desde un correo de Hotmail ;-)

A lottery for the Future 2012 Olympics

Address 61-70 Southampton Row UK
Phone: + 44 703 174 5960
Fax: + 44 844 500 6552
Email: sir.george_ellis.olympic@hotmail.co.uk

Congratulations!

Your E-mail address is one of the 9 lucky selected winning Email Address that won in the London 2012 Olympic Campaign Promotion; you have won the sum of (£800, 000.GBP) Pounds (Eight Hundred Thousand Great British Pounds Sterling), i wish to congratulate you on this Nomination.

Below are your identification numbers, kindly fill the below information's for official Records.

REFERENCE NUMBER: UK/2012 /OLY/CAMP
BATCH NUMBER: UK/2012/153/CAMP/
SECURITY CODE: 2011/2012/8828

1. Your Full name: .....
2. Your Country: .....
3. Contact Address: .....
4. Telephone Number: .....
5. Fax Number: .....
6. Marital Status: .....
7. Occupation: .....
8. Sex: .....
9. Age: .....

You are required to forward the requested details of your winning to the above office contact details, to enable us facilitate the processing of your claim.

NOTE: THE IOC (INTERNATIONAL OLYMPIC COMMITTEE) SUPPORT BARCLAYS TEAM, TO CREATE AWARENESS FOR THE UPCOMING 2012 OLYMPIC GAMES, WHICH IS SPONSORING THIS PROGRAM.

Regards.
Elizabeth Adams.
Promotion Manager

LONDON 2012 OLYMPICS PROMOTION

Una vez que la información es completada y enviada, los estafadores se comunican con las víctimas para chantajearlas y solicitarles un pago por adelantado, generalmente por Western Union, que sería necesario para cubrir los costos en la entrega del premio.

Por supuesto, todo esto es mentira y una vez que el pago se realiza las víctimas no vuelven a tener noticias.

Estafas con ofertas de falsos alojamientos

Los estafadores toman ventaja de la alta demanda de alojamiento durante la temporada alta y publican alojamientos inexistentes u ofrecen sus servicios como agentes de reserva de hoteles. Algunos se hacen pasar por dueños de propiedades y suministran fotos de las mismas lo que hace su oferta más creíble. En la mayoría de los casos, las fotos utilizadas son robadas de otras páginas de reserva de hoteles o simplemente descargadas al azar de Internet. Algunos estafadores expertos crean sitios web falsos, por lo que se aconseja siempre verificar la credibilidad del anunciante mediante el análisis de todos los datos que aparecen en el anuncio (nombres, direcciones de correo electrónico, números de teléfono, dirección del sitio, las fotos y el texto utilizado en el anuncio). Y, por favor, nunca reserves por impulso. Toma suficiente tiempo para una planificación adecuada de tu viaje o evento para protegerte de estos posibles engaños.

Lo típico de este tipo de estafadores es que siempre exigen pagos por adelantado, lo que denominan “bono” o “garantía de la reserva”. Solicitan asimismo documentos de identificación personal que pueden utilizar como clave para cometer fraudes de identidad. Es entendible que se necesite una garantía para la reserva, pero recomendamos no hacerlo con medios de pago como Western Union o una transferencia internacional a cuentas de origen extraño. Pues si lo haces de este modo no podrás recuperar nunca tu dinero, igualmente te recomendamos no dar mucha información acerca de tus datos personales.

Venta de falsas entradas

La única forma de adquirir entradas para los Juegos Olímpicos de Londres 2012 es comprándolas en el **sitio oficial.** Si alguien está intentando revender sus entradas debido a alguna razón a un precio más barato, lo más probable es que esté intentando hacer un fraude. No confíes tan fácilmente en los anuncios demasiado atractivos y en los sitios web sin haber verificado la veracidad de la información.

Falsas ofertas de empleo

En las que te ofrecen un trabajo súper bien remunerado dentro del ámbito turístico, en un hotel o restaurante.

Tras varios contactos, te agasajaran la "oreja": "¡Has sido seleccionado entre cien candidatos!" "¡Eres el mejor preparado!". Por supuesto tienes que enviar junto con tu documentación para la formalización del contrato un dinero en "conceptos varios" que te será reembolsado junto con tu primer salario.

Tienen razón en una cosa, seguramente si envías la documentación y el dinero, es que eres el mejor preparad@, ¡pero para estafarte!, puesto que lamentablemente nunca llegará ese tan ansiado primer sueldo "inglés".

Recuerda que en Internet tienes que utilizar la lógica, como decían nuestro mayores "nadie regala duros a pesetas".

VI
CIBERCONSEJOS

En este sexto capítulo de *X1Red+Segura: Informando y Educando v1.0* se plasman los artículos cortos a modo de alertas que han ido apareciendo en el blog que da pie a este libro.

Estos "mini" artículos tienen dos misiones, la primera alertar sobre amenazas potenciales en la Red y la segunda, la más importante, cómo evitarlas.

En definitiva, con esta serie de ciberconsejos se pretende concienciar al usuario para que pueda optimizar con seguridad su navegación por la Red.

Las amenazas en la Red no cesan en su evolución, por ello este capítulo. Al igual que los anteriores relativos a amenazas en la Red, siempre quedarán abiertos a futuras actualizaciones.

Internet debe de ser un punto de encuentro familiar

En casa tengamos el ordenador a la vista de toda la familia (en el salón o en una sala de estar común), no en un rincón escondido ni en el dormitorio de los niños.

El uso de Internet debe de ser una actividad abierta y familiar, navegando juntos cuando estén los peques, saber con quién se comunican y controlar el tiempo que dedican a estar conectados.

Debemos educarles y enseñarles las bondades de la Red pero también los peligros a los que se pueden enfrentar.

No olvidemos que muchas veces son los niños quienes pueden enseñar mucho a los padres.

Recordad que en Internet siempre hay que utilizar la lógica y que nosotros mismos somos nuestro mejor antivirus.

Cómo tener una contraseña segura

La importancia de tener una contraseña segura es de vital importancia para evitar "problemas" tanto con nuestra privacidad como con nuestra seguridad.

La elección de una contraseña segura no tiene por qué estar reñida con la facilidad de recordarla, siempre y cuando se mantenga dentro de unas normas básicas seguridad.

Una contraseña se considera que tiene una seguridad aceptable cuando tiene al menos ocho caracteres, es alfanumérica y además utiliza algún símbolo.

Existen programas que generan por nosotros nuestras contraseñas, recordándolas por nosotros. Otra una forma sencilla de crear una contraseña más o menos segura es creando una "sigla" desde una frase fácil de recordar para nosotros al tener significado directo para nosotros. Por ejemplo: "**M**i **h**ijo **n**ació **e**l **12** de **dic**iembre de **2004**". Con esa frase como guía, puede usar **Mhne12/Dic,4** como contraseña.

Emplear distintas contraseñas para cada servicio que utilicéis en Internet.

¿Privacidad pública?

Ya estamos llegando al veranito, las vacaciones, el buen tiempo, las salidas de fines de semana. Pero claro, nosotros tenemos que contarlo y, sobre todo, "compartir" nuestra buena suerte con **TODO EL MUNDO.**

Con este afán de informar y de compartir, **con nuestros 1.750 "AMIGOS"** en las redes sociales, no nos damos cuenta de que estamos allanando el terreno a los malos.

Para ser "sociales" tenemos que perder el anonimato y regalar nuestra privacidad a toda la comunidad internauta.

> "Este fin de semana no estaremos en casa, nos vamos toda la familia a una casa rural paradisíaca y no volveremos hasta el domingo por la noche".
>
> "Me voy de vacaciones 15 días a las Islas Afortunadas, mi avión sale a las 10 de la mañana del domingo y me olvido del mundanal ruido de la ciudad hasta mi regreso a final de mes."

¡Qué suerte tenéis! y ¡qué fácil se lo ponéis!, pero para hacer las cosas 100% podríais completar la información e indicarles dónde dejáis una copia de la llave de casa (normalmente bajo el felpudo) o dónde escondéis en vuestro domicilio las pertenencias más valiosas.

¿Vale la pena pagar con nuestra privacidad por tener más "éxito virtual"?

EN INTERNET NO APORTEIS INFORMACIÓN PERSONAL QUE PUEDA PERJUDICAROS NI DESVIRTUÉIS EL VERDADERO SIGNIFICADO DE LA PALABRA AMISTAD.

¡Hola soy tu banco! ¿Me dejas robarte?

"¡Hola soy tu banco!, necesito que accedas con tu usuario y *password* de conexión a la banca *on-line,* es necesario para actualizar tus datos de conexión en la nueva plataforma de seguridad del banco."

Este tipo de robos y estafas son actuaciones muy simples por parte de los ciberciminales, se podría decir que casi invisibles para la víctima.

Normalmente se produce tras una campaña de *phishing* en la que capturan nuestros datos relativos a banca *on-line* haciéndose pasar por nuestro banco, que mediante cualquier burda excusa te solicitan ingresar en tu cuenta mediante un *link* que se propone en el correo.

Lógicamente este *link* es una copia de la página original de nuestro banco, en el momento que accedemos, posiblemente nos dará un error o nos lleve a la página real del banco, pero el mal ya está hecho, ya han capturado nuestras credenciales.

Hay que seguir normas básicas para evitar este tipo de peligros:

- Realizar compras en Internet utilizando siempre, y únicamente, sitios de confianza certificados y señalados como tales, en el navegador deberemos ver siempre: **https://**

- Evito la captura de mis datos bancarios y de tarjeta de crédito protegiendo mi ordenador con un antivirus actualizado, con ello evitaré, en la medida de lo posible, cualquier programa malicioso.
- Ante la duda, ante la recepción de cualquier *e-mail* o mensaje sospechoso, y antes de realizar cualquier movimiento bancario en la Red, consultar al banco directamente.
- Ante este tipo de correos no responder nunca, además nuestro banco JAMÁS se va a poner en contacto por correo para estos menesteres.

Recordad, en Internet tenéis que utilizar la lógica en vuestra navegación.

Consejos para un alquiler vacacional seguro

Ya estamos en veranito, al final, y gracias a nuestros esfuerzos vamos a poder disfrutar unos días de esas ansiadas vacaciones en la playita.

Solo queda una cosa, encontrar el chollo BBB (bueno, bonito y barato) y además tenemos que procurar ahorrarnos unos eurillos en estos tiempos tan achuchados que vivimos.

La crisis también ha obligado a muchos propietarios a poner sus viviendas vacacionales en alquiler para poder afrontar las hipotecas.

Los cibercriminales aprovechan estas "coyunturas" para procurar hacer su agosto particular, y nunca mejor dicho.

Tienen varios procedimientos, uno de ellos, utilizado en otras estafas de compra/venta, es copiar íntegramente anuncios reales que encuentran en la Red, modifican el precio del alquiler estableciendo precios irrisorios en relación con los

precios reales del mercado, por supuesto otro cambio es el de forma de contacto, ¿adiviináis cuál es el nuevo?

Como excusa del alquiler, en muchas ocasiones, es porque se encuentran residiendo en el extranjero y este año no van a poder disfrutar de su "paraíso en España". Ojo, en este caso también se puede dar que el destino sea al extranjero.

La forma de pago suele ser por adelantado, al menos el 50%, y el resto una vez en el paradisíaco apartamento, normalmente a través de plataformas como Money Gram o Western Union, que suelen ser las más utilizados por los estafadores que las cuentas bancarias.

¿Os imagináis vuestra cara una vez que hacéis el viaje hasta la costa y os encontráis con que en el apartamento que habéis alquilado ya hay gente habitándolo, y por supuesto no tienen conocimiento de los datos de la persona que os lo ha alquilado? y ¿si el destino en vez de el Levante español sea cualquiera de nuestras islas u otro destino fuera de España? ¿Os imagináis la papeleta?

A veces utilizan métodos más sofisticados, diseñan y ponen en "circulación" páginas web emulando ser agencias de viajes o de alquiler. Los precios igual de increíblemente baratos.

En ambos solo tienen que lanzar el anzuelo y esperar su "pez".

Prestad atención a vuestros "tratos y contratos" en la Red, actuad siempre con lógica.

Para evitar que esto pueda dar al traste con las vacaciones, lo mejor es seguir una serie precauciones para no caer en una posible estafa:

1. Desconfía de los anuncios en los que el precio de alquiler es desmesuradamente bajo. Los pisos baratos son los que más llaman la atención de los usuarios.

2. Consulta el número de personas que han alquilado previamente ese alojamiento. El que haya un buen número de arrendatarios es una buena señal de seguridad, así como también, leer las opiniones de éstos sobre el alojamiento.

3. En caso de que el anunciante sea una agencia, solicita sus datos completos (dirección, teléfono, sitio web...). Y en caso de que el anunciante sea una

persona física que asegura gestionar el alquiler, pídele los datos del propietario y contacta con él.

4. Desconfía de los anunciantes que no pueden hablar por teléfono con cualquier excusa y que solo proporcionan su dirección de correo electrónico.

5. Investiga a través de buscadores los datos que te ha facilitado el anunciante. Hay otros en los que la gente cuenta sus casos cuando han sido estafados.

6. No es aconsejable pagar por adelantado. Muchos anunciantes exigen dicho pago como medio de garantía.

7. Desconfía de los anunciantes que exigen el pago rápido y antes de realizar una transferencia bancaria, asegúrate de que el anunciante ofrece las garantías suficientes. Será más seguro que el anunciante acepte el pago con tarjeta de crédito.

8. Si contactas por teléfono procura guardar todos los mensajes recibidos y enviados, así como el número de teléfono.

9. Solicita al anunciante una fotocopia del DNI y un breve compromiso de contrato en el que aparezcan las fechas de la estancia, el precio y la posible fianza.

10. Sospecha de los correos electrónicos que solicitan datos o claves de acceso.

Si queréis pasar unas buenas vacaciones prestad atención a los "chollos" que encontráis por la Red, algunos son reales, pero lamentablemente nadie regala duros a pesetas.

Recordad que vosotros mismos sois vuestra propia y mayor vulnerabilidad pero también vuestro mejor antivirus, emplead la lógica en Internet.

Protejamos a wifi

Dejar abierta nuestra red wifi o con una protección débil puede traernos graves consecuencias, es como si dejases la puerta de casa abierta de par en par. Para evitar males mayores es aconsejable cambiar los valores por defecto de nuestro *router* wifi:

- Cambiar la contraseña de administrador del *router* para evitar accesos no deseados. Tener en cuenta que las contraseñas normalmente son por defecto y siempre las mismas.
- Cambiar el nombre de SSID para no dar pistas a quien pretenda acceder a nuestro *router*. El nombre de nuestra wifi por defecto puede indicar que compañía nos da el servicio y por consiguiente da pistas del los fallos conocidos del *router* que facilitan a sus usuarios así como las contraseñas que utilizan por defecto.
- Cambiar el tipo de encriptación por WPA2 por ser la más segura.
- Cambiar también la clave de acceso a la Red que viene por defecto, debiendo utilizar una contraseña robusta combinando mayúsculas, minúsculas, números y símbolos, creando cadenas de más de siete caracteres y sin ningún sentido aparente.

Utiliza la lógica y recuerda que tú eres tu peor vulnerabilidad pero también tu mejor antivirus.

Comprobar si un archivo o *link* contiene virus

¿Tienes dudas o sospechas de que un archivo que te han enviado o que has descargado pueda tener algún tipo de *malware*?, puedes comprobar si están reportados como peligrosos en el siguiente *link:*

https://www.virustotal.com/

Utiliza la lógica y recuerda que tú eres tu peor vulnerabilidad pero también tu mejor antivirus.

¿Cómo comprobar si un *link* es realmente seguro?

Según el informe Symantec Intelligence de octubre de 2011, los *spammers* utilizan *scripts* de código abierto para abreviar direcciones URL y dirigir a los usuarios a *sites* maliciosos.

La percepción de que las direcciones URL abreviadas son seguras está muy extendida, así, se convierten en el blanco perfecto de los *spammers*.

Ante un mensaje o un correo electrónico en el que leemos: "Hola Pepe (Pepe es tu nombre), ¿sales tú en esta foto? http://esta.es/p3l1gr0" o simplemente en un *link* similar te ofertan algún producto o te notifican un premio, te quedan solo dos posibilidades: preguntar a quien te envió el mensaje el contendido real de lo que te envía, o, lo más probable, que hagas *click* sin tomar ningún tipo de medida y totalmente **a ciegas para terminar donde los "malos" quieren tenerte, en sus garras.**

Una vez redirigido al terreno de los *spammers* tu privacidad e incluso tu bolsillo pueden ser blanco de sus objetivos criminales, convirtiéndote en víctima de *phishing* obteniendo todas tus credenciales de acceso a banca *on-line*, redes sociales, correo electrónico, etc.

http://safeweb.norton.com/ es un buen enlace para comprobar si los *links* acortados nos llevan donde realmente nos dicen o si cualquier URL está catalogada como potencialmente peligrosa.

Si eres “ciberempresario” blinda tu puerta

Si tienes una página web desde la que ofreces y vendes tus productos, o simplemente gestionas datos personales de los usuarios o clientes de tu página, deberías prestar la máxima atención y securizar tu “cibertienda” o página web.

Una mala securización de tu página podría terminar con un grave problema para ti y para tus clientes, que tienen el derecho de tener sus datos personales protegidos y tú la obligación de protegerlos.

Está al orden del día el “robo” de datos personales y confidenciales de las bases de datos de *sites* de grandes compañías y organizaciones. Estos datos confidenciales de usuarios son utilizados para la **realización de algún tipo de fraude.**

El **robo de información** sensible y confidencial y su posterior divulgación puede acarrear demandas con graves “consecuencias” económicas de acuerdo a lo estipulado en la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) (Ley Orgánica 15/1999, de 13 de diciembre).

Existe la falsa creencia de que solo las empresas que desarrollan actividades relacionadas con las nuevas tecnologías, Internet, etc. están obligadas a cumplir las obligaciones que impone la Ley de Protección de Datos. Pero esta ley es de obligado cumplimiento para **TODAS** las personas físicas o jurídicas que posean datos de carácter personal de personas físicas.

> “Por dato de carácter personal se entiende cualquier información referida a **personas físicas** (no jurídicas) identificadas o identificables: nombre y apellidos, dirección, teléfono, DNI, número de la seguridad social, fotografías, firmas, correos electrónicos, datos bancarios, edad y fecha de nacimiento, sexo, nacionalidad, etc.

El responsable del fichero y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado."

MORALEJA: Pon un experto en seguridad informática en tu "ciberempresa".

Desinfección del Ransomware o "Virus de la Policía"

Parece ser que el **Ransomware (Virus de la Policía, de la SGAE, de la Gendarmería Nacional Francesa y de no sé cuantas cosas más) se está poniendo "duro".** Este *malware* debe de haberle salido muy rentable a sus creadores y no paran de crear nuevas mutaciones para seguir llenándose los bolsillos a costa de los internautas poco precavidos e informados.

Durante el mes de mayo de 2012 han aparecido dos nuevas y peligrosas variantes del comúnmente conocido Ransomware **"Virus de la Policía"** con sus variantes: **"SGAE y Rannoh locked".** Si bien guardan ciertas similitudes en su *modus operandi* con variantes anteriores, éstas incorporan también algunas diferencias que están logrando infectar a cientos de nuevas víctimas.

Por suerte los chicos de @InfoSpyware, ¡GRANDES en la materia!, no descansan en protegernos con sus informaciones y sobre todo aportando soluciones a nuestros "males" en la Red.

@InfoSpyware ha creado PoliFix que detecta y elimina el Virus de la Policía (también llamado Ukash virus) en todas sus variantes conocidas.

Para usar PoliFix, siga los siguientes pasos:

1. Acceder a Guía de desinfección en página del autor **(InfoSyware):**

2. Descarga PoliFix en una memoria USB desde otro PC.

3. Inicia el PC infectado en modo a prueba de errores.

4. Conecta el *pendrive* en el ordenador.

5. Ejecuta PoliFix desde el *pendrive* y espera.

Recuerda que tú eres tu principal vulnerabilidad pero también tu mejor antivirus.

Abuel@s en la Red

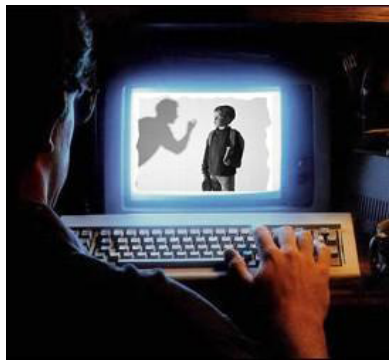
La Oficina de Seguridad del Internauta dedica un día a los "cibermayores" y celebra el **Día del abuel@ internauta** con la finalidad de acercar las nuevas tecnologías a los mayores.

Me parece una magnífica idea muy necesaria y a la que me quiero sumar añadiendo al libro estas palabras de agradecimiento a la OSI y de ánimo a los que se animen a adentrarse en el "nuevo mundo" de Internet sumándose al disfrute de las bondades que nos ofrece la Red.

Simplemente quiero deciros que en Internet debéis seguir utilizando, como lleváis haciendo tanto tiempo en la vida, la lógica. Simplemente recordad cómo os educaron vuestros mayores, y cómo habéis educado a vuestros hijos, y aplicarlo a la vida virtual. No se diferencia, nada más que ahora utilizamos ordenadores. Solo debemos adaptar y aplicar la misma educación a las nuevas tecnologías.

La mejor forma de estar seguros en Internet es conociendo sus peligros para evitarlos. No es necesario ser ingeniero para navegar de forma segura por Internet, simplemente estar al día de las amenazas a los que nos podemos enfrentar para poder disfrutar de las bondades que nos ofrece la Red y para eso la OSI os lo pone fácil con sus consejos.

Pedofilia en la Red



La pedofilia y la corrupción de menores a través de Internet se han convertido en las principales ciberamenzas, aunque no las únicas, para nuestros menores. Ayudándose de las nuevas tecnología esta "calaña" ha encontrado la forma de satisfacer sus instintos más depravados y oscuros, violando la intimidad de nuestros hijos que navegan alegremente por la Red ante la despreocupación de los padres en la tranquilidad de que los niños se encuentran protegidos en la **"falsa soledad"** de sus habitaciones.

Existe una errónea creencia que relaciona los peligros de la Red directamente ligados al uso de un ordenador, pero debemos concienciarnos de que un ordenador hoy en día no es un monitor y una CPU o un ordenador portátil. Hoy en día cualquier videoconsola, y no necesariamente de última generación, o un *smartphone* es un medio de conexión a Internet y por consiguiente una desconocida fuente de peligros para nuestros menores.

Recientemente ha saltado a la noticia la detención de un ciberdepredador, **reincidente,** viejo conocido de las Fuerzas y Cuerpos de Seguridad del Estado y que alardeaba sin complejos de ser el mayor pedófilo de Europa.

Su actividad la llevaba a cabo utilizando una videoconsola, donde contactaba con los menores a través de los juegos *on-line,* donde se ganaba su confianza para

luego lanzar sus campañas de coacciones y amenazas a niños de entre siete y doce años.

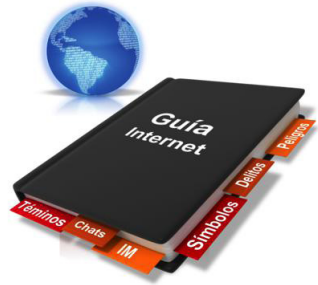
Me gustaría que ésta fuese la última vez que leo este tipo de noticias y que entre todos podamos erradicar estos actos en la Red y podamos decir…: **"¡Lo hemos conseguido!, ningún niño más va a ser abusado en Internet porque todos los padres, tutores y resto de internautas estamos concienciados y JAMÁS dejaremos solo a un menor en la Red sin la protección que necesita".**

¡Qué bonito es soñar! ¿Verdad? Pero entre todos podemos hacer que este sueño se haga un poquito más de realidad y todos podemos contribuir para conseguir 1Red+Segura.

Si topas con un personaje de este tipo en la Red…

¡DENÚNCIALO!

VII
DICCIONARIOS



Todo libro que se precie y que pretenda ser una guía de referencia en cualquier temática más o menos técnica, debe disponer de un glosario o diccionario para que el lector se pueda dirigir en caso de encontrar una palabra de la que desconozca el significado durante su lectura.

X1Rred+Segura: Informando y Educando v1.0 no podría optar a ser una guía de utilidad si no contara entre sus contenidos con un diccionario.

Pero en este caso, dada la "riqueza" de los distintos tipos de lenguajes que se utilizan en la Red, vamos a tener en la presente obra seis diccionarios:

- Términos usados en Internet
- Términos utilizados para identificar a los internautas
- Términos utilizados en los chats
- Términos utilizados en la mensajería instantánea
- Símbolos (emoticonos o *smileys*) que vemos en los contenidos de mensajes y chats
- Términos relacionados con los delitos informáticos

DICCIONARIO DE INTERNET

A

Agente *(agent)*: Pequeño programa inteligente que facilita la operatoria del usuario. Un ejemplo de agente son los asistentes *(wizards)* que existen en la mayoría de los programas modernos.

Ancho de banda *(bandwidth)*: Término técnico que determina el volumen de información que puede circular por un medio físico de comunicación de datos, es decir, la capacidad de una conexión. A mayor ancho de banda, mejor velocidad de acceso; más personas pueden utilizar el mismo medio simultáneamente. Se mide en hertz o bps (bits por segundo), por ejemplo: 32 Kbps, 64 Kbps, 1 Mbps, etc.

Applet (programa): Pequeño programa hecho en lenguaje Java.

Archivo: Unidad de información almacenada en el disco con un nombre específico. Puede contener datos en código máquina, necesarios para la ejecución de un programa, o información común y corriente procesada por el usuario. Tienen una extensión consistente en tres caracteres que lo identifican en su tipo o lo relacionan con un programa determinado.

ARP (*Address Resolution Protocol*-Protocolo de Resolución de Direcciones): Un protocolo de resolución de direcciones electrónicas en números IP que corre en redes locales. Parte del conjunto de protocolos TCP/IP.

ASCII (American Standard Code for Information Interchange-Código Americano Normado para el Intercambio de Información): Conjunto de caracteres, letras y símbolos utilizados en todos los sistemas de computadoras de cualquier país e idioma. Permite una base común de comunicación. Incluye las letras normales del alfabeto, pero excluye la "ñ" y toda letra acentuada. Cada símbolo posee un número asignado que es común en todos los países. Los números van de 0 a 127. Del 128 al 255 cada idioma puede agregar otros símbolos necesarios para su propio lenguaje.

***Attachment* (adjunto):** Se llama así a un archivo de datos (por ejemplo: una planilla de cálculo o una carta de procesador de textos) que se envía junto con un mensaje de correo electrónico. Para que el documento pueda viajar, debe ser codificado de alguna manera, ya que el *e-mail* solo puede transportar códigos ASCII. Entre los formatos de codificación más difundidos están el UUENCODE, MIME y BinHex.

Avatar: Originariamente figura humana de un dios en la mitología hindú. Identidad ficticia, representación física (cara y cuerpo) de una persona conectada al mundo virtual de Internet. Muchas personas construyen su personalidad digital y luego se encuentran en *servers* determinados (por ejemplo, en chats) para jugar o charlar con otros.

B

***Backbone* (columna vertebral):** Conexión de alta velocidad que une computadoras encargadas de hacer circular grandes volúmenes de información. Los *backbones* conectan ciudades o países y constituyen la estructura fundamental de las redes de comunicación. Las redes WAN y los ISP utilizan *backbones* para interconectarse.

Banner: Aviso publicitario que ocupa parte de una página web, en general ubicado en la parte superior, al centro. Haciendo un *click* sobre él, se puede llegar al sitio del anunciante. De este modo, los *banners* en general se cobran en base a los *click-throughs* que se obtienen.

BBS (*Bulletin Board System.* Sistema de mensajería; también llamado erróneamente Base de Datos): Sistema computarizado de intercambio de datos entre un grupo de personas que comparten una misma zona geográfica, donde archivos, mensajes y otra información útil pueden ser intercambiados entre los usuarios. Normalmente se trata de sistemas amateur; son los antecesores aislados de Internet. La mayor de las redes mundiales que comunica a los BBS se llama Fidonet.

Binhex: Estándar para la codificación de datos bajo plataforma Macintosh, utilizado para enviar archivos adjuntos. Similar en concepto al MIME y al Uuencode.

***Bookmark* (señalador o favoritos):** La sección de menú de un navegador donde se pueden almacenar los sitios preferidos, para luego volver a ellos simplemente eligiéndolos con un simple *click* desde un menú.

***Bottleneck* (cuello de botella):** Embotellamiento de paquetes de datos (información) que circulan por una conexión; causa demoras en la comunicación.

Bots: Abreviatura de robots. Son programas muy particulares, inteligentes y autónomos que navegan por el ciberespacio esquivando maniobras para detenerlos. Los *bots* son sumamente ingeniosos y capaces de reaccio-

nar según la situación. No necesariamente son benignos: solo obedecen las órdenes de sus creadores. Muy utilizados para causar caos en los chats.

***Browser/Web browser* (navegador o visualizador):** Programa que permite leer documentos en la Web y seguir enlaces *(links)* de documento en documento de hipertexto. Los navegadores hacen pedidos de archivos (páginas y otros) a los *servers* de web según la elección del usuario y luego muestran en el monitor el resultado del pedido en forma multimedial. Entre los más conocidos se encuentran el Netscape Navigator, Microsoft Explorer y Mosaic. El primer navegador se llamó Line Mode Browser, pero el primer navegador en cuanto a difusión fue Mosaic. Usualmente, a los navegadores se les agrega *plug-ins* para aumentar sus capacidades.

Buscador (*Search Engine,* mal llamado motor de búsqueda): Herramienta que permite ubicar contenidos en la Red, buscando en forma *booleana* a través de palabras clave. Se organizan en buscadores por palabra o índices (como Lycos o Infoseek) y buscadores temáticos o *Directories* (como Yahoo!). Dentro de estas dos categorías básicas existen cientos de buscadores diferentes, cada uno con distintas habilidades o entornos de búsqueda (por ejemplo, solo para médicos, para fanáticos de las mascotas o para libros y revistas).

C

Cablemódem: Dispositivo que permite conectar una computadora a Internet a través de la conexión de coaxial de la televisión por cable. No es realmente un módem ya que no debe modular/demodular porque el sistema es puramente digital. Se perfila como una de las posibilidades de conexión que resolverían la problemática del limitado ancho de banda que se puede obtener a través de una conexión telefónica. *(Ver DirectPC)*

Caché: Almacenamiento intermedio o temporario de información. Por ejemplo, un navegador posee una caché donde almacena las últimas páginas visitadas por el usuario y, si alguna se solicita nuevamente, el navegador mostrará la que tiene acumulada en lugar de volver a buscarla en Internet. El término se utiliza para denominar todo depósito intermedio de datos solicitados con mayor frecuencia. *(Ver Proxy)*

CGI (*Common Gateway Interface*-Interfaz Común de Intercomunicación): Conjunto de medios y formatos para permitir y unificar la comunicación en-

tre la Web y otros sistemas externos, como las bases de datos. Similar al ActiveX.

Chat: Sistema de conversación en línea que permite que varias personas de todo el mundo conversen en tiempo real a través de sus teclados. Existen varios sistemas de chat, uno de los más difundidos es el IRC.

Click-throughs: Sistema de medición que almacena la cantidad de veces que un cliente potencial hace *click* en un *banner* de publicidad y visita el sitio del anunciante. Utilizado como métrica para la venta de espacios de publicidad en los sitios web.

Client side* CGI *script: *Script* CGI que se ejecuta/corre en el cliente. *(Ver Server side CGI script)*

Cliente *(Client)*: Computadora o programa que se conecta a servidores para obtener información. Un cliente solo obtiene datos, no puede ofrecerlos a otros clientes sin depositarlos en un servidor. La mayoría de las computadoras que las personas utilizan para conectarse y navegar por Internet son clientes.

Cliente/Servidor *(Client/Server)*: Sistema de organización de interconexión de computadoras según el cual funciona Internet, así como otros tantos sistemas de redes. Se basa en la separación de las computadoras miembros en dos categorías: las que actúan como servidores (oferentes de información) y otras que actúan como clientes (receptores de información).

***Cookies* (galletitas):** Pequeños archivos con datos que algunos sitios web depositan en forma automática en las computadoras de los visitantes. Lo hacen con el objetivo de almacenar allí información sobre las personas y sus preferencias. Por ejemplo, la primera vez que un navegante visita un *site* y completa algún formulario con sus datos y perfil, el sistema podrá enviarle una *cookie* al asignarle una identificación. Cuando el usuario retorne, el sitio web pedirá a la computadora cliente la *cookie* y, a través de ella, lo reconocerá.

***Cracker* (pirata informático):** Persona que se especializa en violar medidas de seguridad de una computadora o red de computadoras, venciendo claves de acceso y defensas para obtener información que cree valiosa. El *cracker* es considerado un personaje ruin y sin honor, a diferencia del *hacker*. *(Ver Firewall)*

***Cross-platform* (multi-plataforma):** Programa o dispositivo que puede utilizarse sin inconvenientes en distintas plataformas de *hardware* y sistemas operativos. Un programa en lenguaje Java posee esta característica.

***Cybermoney* (ciberdinero):** Formas de pago virtuales alternativas que se están desarrollando en Internet. En este momento, la falta de mecanismos de pago que garanticen el intercambio de dinero es la principal barrera para el desarrollo del comercio electrónico. Actualmente, existen distintas alternativas en experimentación como CyberCash, Cybercoin y los mecanismos para el pago de sumas muy pequeñas, llamados micropagos.

***Cyberspace* (ciberespacio):** Es la denominación del espacio virtual (no físico) donde las personas se reúnen en Internet. También denomina a la cultura, usos y costumbres de la comunidad electrónica. Término inventado por el escritor de ciencia ficción William Gibson, en su obra *Neuromancer. (Ver Netiquette)*

D

***Default* (acción por omisión):** Opción que un programa asume si no se especifica lo contrario. También llamado "valores predeterminados".

Dial-in: Conexión a Internet que se establece a través de un módem y una línea telefónica. A cada usuario se le asigna un número IP dinámico, es decir, un número otorgado solo durante la comunicación. Para establecer la conexión se utiliza algún estándar adecuado, como por ejemplo el PPP, SLIP o CSLIP.

Dial-up: Término actualmente utilizado como sinónimo de *dial-in.* Anteriormente definía una conexión a Internet donde no se asignaba número IP.

Dirección electrónica *(electronic address)*: Serie de caracteres que identifican unívocamente un servidor (por ejemplo, hotmail.com), una persona (contacto@hotmail.com) o un recurso (un sitio web como http://www.hotmail.com) en Internet. Se componen de varias partes de longitud variable. Las direcciones son convertidas por los DNS en los números IP correspondientes para que puedan viajar por la Red.

Directory: Buscador organizado por temas.

DirectPC: Nueva forma de conexión a Internet, basada en el uso de una antena satelital conectada a la computadora durante las veinticuatro horas. Se perfila como una de las posibilidades de comunicación que resolverían

la problemática del limitado ancho de banda que se puede obtener en una conexión telefónica. *(Ver Cablemódem)*

DNS (*Domain Name System/*Server-Servidor de Nombres de Dominios): Sistema de computadoras que se encarga de convertir (resolver) las direcciones electrónicas de Internet (como http://www.hotmail.com) en la dirección IP correspondiente y viceversa. Componen la base del funcionamiento de las direcciones electrónicas en Internet y están organizados jerárquicamente. *(Ver Internic, ARP)*

Download: Es el proceso de bajar (traer) un archivo desde algún lugar en la Red a la computadora de un usuario*. (Ver Up-load,* el proceso inverso)

Driver: Significa controlador. Es el *software* adicional necesario para controlar la comunicación entre el sistema y un cierto dispositivo físico, tal como un monitor o una impresora.

***Dynamic IP* (IP dinámico):** Se dice así cuando el número IP de una computadora conectada a un proveedor de servicio vía *dial-in* es otorgado en el momento de la conexión en lugar de ser un número fijo.

E

EFF (Electronic Frontier Foundation): Organismo civil sin fines de lucro de Internet. Su objetivo es: "Civilizar la frontera electrónica, hacerla útil no solo para la elite técnica, sino también para el resto de la humanidad y lograr esto conservando las mejores tradiciones de nuestra sociedad: el flujo libre y abierto de información y comunicación" (EFF Mission Statement, abril de 1990). Más datos en http://www.eff.org/.

***E-mail* (*electronic mail* o correo electrónico):** Servicio de Internet que permite el envío de mensajes privados (semejantes al correo común) entre usuarios. Basado en el SMTP. Más rápido, económico y versátil que ningún otro medio de comunicación actual. También utilizado como medio de debate grupal en las *mailing lists.*

Emoticonos (o *smilies*): Conjunto de caracteres gráficos que sirven para demostrar estados de ánimo en un medio escrito como el *e-mail*. Por ejemplo, los símbolos :-), vistos de costado, muestran una cara sonriente y pueden significar chiste, o buenos deseos.

Enlaces *(links)*: Conexiones que posee un documento de la Web (escrito en HTML). Un enlace puede apuntar a referencias en el mismo documento,

en otro documento en el mismo *site*; también a otro *site,* a un gráfico, vídeo o sonido. *(Ver Hipertexto)*

Encriptación *(Encryption)*: Método para convertir los caracteres de un texto de modo que no sea posible entenderlo si no se lo lee con la clave correspondiente. Utilizado para proteger la integridad de información secreta en caso de que sea interceptada. Uno de los métodos más conocidos y seguros de encriptación es el PGP.

Entorno gráfico: Sistema operativo en el que la información que aparece en pantalla aparece representada en forma gráfica, como es el caso de Windows.

Escáner: Dispositivo periférico que copia información impresa mediante un sistema óptico de lectura. Permite convertir imágenes, por ejemplo de fotografías, en imágenes tratables y almacenables por la computadora. El proceso de conversión se denomina digitalización. El término inglés *scanner* significa 'explorar' o 'rastrear'.

Extranet: Utilización de la tecnología de Internet para conectar la red local (LAN) de una organización con otras redes (por ejemplo, proveedores y clientes). *(Ver Intranet)*

F

FAQ (*Frequently Asked Questions*-Preguntas Frecuentes): Conjunto de preguntas y respuestas habituales sobre un tema determinado. Utilizadas para despejar las dudas de los neófitos.

Farming* o *farm server: Servidor externo que se alquila para alojar información y ponerla a disposición de los navegantes de la Red. Sinónimo de *Hosting*.

Fidonet: La red que intercomunica a la mayor cantidad de BBS amateurs del mundo, nacida en 1982. Reúne a unas treinta mil personas.

Finger: Comando que permite obtener información sobre una persona en la Red (por ejemplo, dirección de *e-mail,* dirección postal, hobbies), buscando ciertos datos que ésta pudo dejar en un formulario de consulta.

***Firewall* (pared a prueba de fuego):** Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada. Es utilizado para proteger los recursos de una organización de consultas externas no autorizadas.

Firmware: Son pequeños programas que por lo general vienen en un chip en el *hardware,* como es el caso de la ROM BIOS.

***Flame* (llamarada):** Ataque personal insultante. Mensaje de correo electrónico ofensivo.

Formateo: Proceso por el que se adapta la superficie magnética de un disco para aceptar la información bajo un sistema operativo determinado. En el proceso de formateado se colocan las marcas lógicas que permitirán localizar la información en el disco y las marcas de sincronismo además de comprobar la superficie del disco.

***Frame* (cuadro, marco):** Instrucciones en el lenguaje HTML (utilizado para diseñar las páginas web); una forma de dividir la pantalla del navegante en varias zonas, cada una con autonomía de movimiento. Por ejemplo, se puede dividir una pantalla de modo que haya un frame vertical que ocupe el lado izquierdo de la pantalla durante toda la navegación, que contenga el menú de un sitio web. Los frames son un agregado al HTML estándar inventado por la empresa Netscape y luego adoptados como norma.

Frame-relay: Tecnología de transporte de datos por paquetes muy utilizada en las conexiones por líneas dedicadas.

Freeware: Política de distribución gratuita de programas. Utilizada para gran parte del *software* de Internet. En general, estos programas son creados por un estudiante o alguna organización (usualmente una universidad) con el único objetivo de que mucha gente en el mundo pueda disfrutarlos. No son necesariamente sencillos: muchos de ellos son complejos y han llevado cientos de horas de desarrollo. Ejemplos de *freeware* son el sistema operativo Linux (un Unix) o el PGP (Pretty Good Privacy, un *software* de encriptación), que se distribuyen de este modo.

FTP (*File Transfer Protocol*-Protocolo de Transferencia de Archivos): Es un servicio de Internet que permite transferir archivos *(upload* y *download)* entre computadoras conectadas a Internet. Método por el cual la mayoría del *software* de Internet es distribuido.

Full-Duplex: Característica de un medio de comunicación por el que se pueden enviar y recibir datos simultáneamente. *(Ver half-duplex)*

G

Gateway: Dispositivo de comunicación entre dos o más redes locales (LAN) y remotas, usualmente capaz de convertir distintos protocolos, actuando de traductor para permitir la comunicación. Como término genérico es utilizado para denominar a todo instrumento capaz de convertir o transformar datos que circulan entre dos medios o tecnologías.

Gopher: Servicio de Internet que organiza la información y permite acceder a ella en forma sencilla. Es precursora de la Web y actualmente está cayendo en desuso. Creada en la Universidad de Minessotta, su nombre hace referencia a la mascota del lugar, que es un topo. Otros, sin embargo, sugieren que es una deformación de la frase *goes-fer* ('busca'). El Gopher resolvió el problema de cómo ubicar recursos en Internet, reduciendo todas las búsquedas a menúes y submenúes. Con el tiempo, el Gopher fue perdiendo popularidad frente a la World Wide Web, gracias a la ventaja de tener contenido multimedial de imágenes y sonido.

Gurú: Persona con muchos conocimientos sobre un tema, en general, técnico.

H

Hacker: Experto técnico en algún tema relacionado con comunicaciones o seguridad informática; de alguna manera, es también un gurú. Los *hackers* suelen dedicarse a demostrar fallos en los sistemas de protección de una red de computadoras, casi como un deporte. Los *hackers* son muy respetados por la comunidad técnica de Internet, a diferencia de los *crackers*. *(Ver Capítulo I. Internet: Internet y sus moradores. Los hackers)*

Half-Duplex: Característica de un medio de comunicación por la cual no se pueden enviar y recibir datos simultáneamente. A diferencia del *full-duplex,* se debe esperar que una parte termine de transmitir para poder enviar información por el mismo medio. En cierta forma, hablar por teléfono es un proceso de comunicación *half-duplex*, donde por momentos se habla y por momentos se escucha, pero donde se hace difícil establecer una comunicación si los dos participantes hablan a la vez.

Hardware: Componente físico de la computadora. Por ejemplo: el monitor, la impresora o el disco rígido. El *hardware* por sí mismo no hace que una máquina funcione. Es necesario, además, instalar un *software* adecuado.

Hipermedia: Combinación de hipertexto y multimedia. Uno de los grandes atractivos de la Web.

Hipertexto: Concepto y término inventado por Ted Nelson en 1969. Nelson era un famoso visionario de la informática que investigó durante veinticinco años las posibilidades de interacción entre las computadoras y la literatura. Uno de los conceptos básicos para el desarrollo de la WWW. El hipertexto es una forma diferente de organizar información. En lugar de leer un texto en forma continua, ciertos términos están unidos a otros mediante relaciones (enlaces o *links*) que tienen entre ellos. El hipertexto permite saltar de un punto a otro en un texto y a través de los enlaces (con un simple *click* sobre las palabras subrayadas y en negrita), permite que los navegantes busquen información de su interés en la Red, guiándose por un camino distinto de razonamiento. Algunos programas muy difundidos, como la Ayuda de Windows o las enciclopedias en CD-ROM, están organizadas como hipertextos.

***Hit* (acceso o pedido):** Unidad de medición de accesos a determinados recursos. Forma de registrar cada pedido de información que un usuario efectúa a un server. Por ejemplo, en el caso de un sitio web, la solicitud de cada imagen, página y frame genera un *hit.* Por lo tanto, para conocer en realidad cuántos accesos hubo, debe dividirse la cantidad de hits por la cantidad de objetos independientes (texto, *frames* e imágenes) que una página contiene, o usar un contador de accesos.

***Home page* (página principal o de entrada):** Página de información de la web, escrita en HTML. En general, el término hace referencia a la página principal o de acceso inicial de un *site.*

Host: Actualmente, sinónimo de servidor.

***Hostname* (nombre de un *host*):** Denominación otorgada por el administrador a una computadora. El *hostname* es parte de la dirección electrónica de esa computadora y debe ser único para cada máquina conectada a Internet.

HTML (*HyperText Markup Language*-Lenguaje de Marcado de Hipertextos): Lenguaje que define textos, subgrupo del SGML, destinado a simplificar la escritura de documentos estándar. Es la base estructural en la que están diseñadas las páginas de la World Wide Web. Su definición está a cargo del Web Consortium.

HTTP (*HyperText Transfer Protocol*-Protocolo de Transferencia de Hipertexto): Es el mecanismo de intercambio de información que constituye la base funcional de la World Wide Web.

***Hyperdocuments* (Hiperdocumentos):** Documento que tiene estructura de hipertexto, pero contiene además referencias a objetos multimediales (como sonidos, imágenes, vídeos).

Hyperlink: Enlace entre dos nodos de un hipertexto.

I

IMO (*In My Opinión*-En Mi Opinión): Una de las siglas utilizadas en los mensajes de Internet. También **IMHO (*In My Humble Opinion*-En Mi Humilde Opinión).**

***Impressions* (visualizaciones):** Unidad de medida que verifica cuántas veces un navegante ve un determinado *banner* de publicidad.

Inteligencia Artificial (*Artificial Intelligence* o AI): Rama de la computación que analiza la computadora y sus posibilidades de poseer inteligencia. La IA estudia las habilidades inteligentes de razonamiento, capacidad de extracción de conclusiones y reacciones ante nuevas situaciones de las computadoras y sus programas. El razonamiento es parecido al del cerebro humano (no es lineal, se aprende de cada situación). Existen dos ramas de la IA: la fuerte *(strong)* sostiene que llegará el día en que puedan construirse programas que sean realmente inteligentes y computadoras pensantes. La débil *(weak)* considera que las computadoras solo pueden ser diseñadas para convertirse en importantes herramientas para modelar y simular el pensamiento humano.

***Interface* (Interfaz):** Cara visible de los programas. Interactúa con los usuarios. La *interface* abarca las pantallas y su diseño, el lenguaje usado, los botones y los mensajes de error, entre otros aspectos de la comunicación computadora/persona.

ISA (*Industry Standard Arquitecture*-Arquitectura Estándar de la Industria): Es la arquitectura adoptada en las PC compatibles y que define como deben ser las tarjetas que pueden conectarse a ellas.

Internet Adress: Sinónimo de número IP. Número asignado que identifica a un *server* en Internet. Está compuesto por dos o tres partes: número de

red, número opcional de sub-red y número de *host. (Ver direcciones electrónicas, DNS)*

Internet Worm: Programa similar a un virus de computadora creado por Robert Morris, un estudiante de Cornell University que fue famoso en 1988. El Worm se aprovechó de una falla de seguridad de un programa de *e-mail* muy utilizado y causó desastres al reproducirse sin límite, infectando y luego dejando catatónicas a la mayor parte de las computadoras conectadas a Internet. El pánico causado por el virus fue tan grande que generó el nacimiento de varios organismos dedicados a investigar las fallas de seguridad de los programas.

Internets: La red de computadoras más extendida del planeta, que conecta y comunica a más de cincuenta millones de personas. Nació a fines de los años sesenta como ARPANet y se convirtió en un revolucionario medio de comunicación. Su estructura técnica se basa en millones de computadoras que ofrecen todo tipo de información. Estas computadoras, encendidas las veinticuatro horas, se llaman servidores y están interconectadas entre sí en todo el mundo a través de diferentes mecanismos de líneas dedicadas. Sin importar qué tipo de computadoras son, para intercomunicarse utilizan el protocolo TCP/IP. Las computadoras que utilizan las personas para conectarse y consultar los datos de los servidores se llaman clientes, y acceden en general a través en un tipo de conexión llamado *dial-in*, utilizando un módem y una línea telefónica.

Internet: Denomina un grupo interconectado de redes locales, que utilizan un mismo protocolo de comunicación.

InterNIC (*Internet Network Information Center*-Centro de Información de Red de Internet): Centro de información que almacena documentos de Internet: RFC y borradores de documentos. Organismo que se ocupa de otorgar grupos de números IP y direcciones electrónicas a cada organización que desee conectarse a Internet, garantizando que sean únicas. Más datos en http://www.internic.net/ .

Intranet: Utilización de la tecnología de Internet dentro de la red local (LAN) y/o red de área amplia (WAN) de una organización. Permite crear un sitio público donde se centraliza el acceso a la información de la compañía. Bien utilizada, una intranet permite optimizar el acceso a los recursos de una organización, organizar los datos existentes en las PC de cada individuo y extender la tarea colaborativa entre los miembros de equipos de trabajo. Cuando una *intranet* extiende sus fronteras más allá de los límites de la

organización, para permitir la intercomunicación con los sistemas de otras compañías, se la llama *Extranet*.

IP *(Internet Protocol)*: Protocolo de Internet definido en el RFC 791. Confirma la base del estándar de comunicaciones de Internet. El IP provee un método para fragmentar (deshacer en pequeños paquetes) y rutear (llevar desde el origen al destino) la información. Es inseguro, ya que no verifica que todos los fragmentos del mensaje lleguen a su destino sin perderse en el camino. Por eso, se complementa con el TCP.

IP Número o dirección *(IP address)*: Dirección numérica asignada a un dispositivo de *hardware* (computadora, *router,* etc.) conectado a Internet, bajo el protocolo IP. La dirección se compone de cuatro números, y cada uno de ellos puede ser de 0 a 255, por ejemplo 200.78.67.192. Esto permite contar con hasta 256 (elevado a la cuarta potencia) números para asignar a los diferentes dispositivos conectados: cerca de cuatro mil millones. Las direcciones IP se agrupan en clases. Para convertir una dirección IP en una dirección electrónica humana (por ejemplo, http://www.hotmail.com) se utilizan los DNS.

IRC *(Internet Relay Chat)*: Uno de los sistemas más populares de charlas interactivas (chats) de múltiples usuarios vía Internet. Permite que miles de personas de todo el mundo se reúnan a "conversar" simultáneamente en forma escrita.

ISDN (*Integrated Sevices Data Network*-Red Digital de Servicios Integrados): Tecnología rápida de conexión para líneas dedicadas y transmisión de datos. Se utiliza para tener acceso a Internet o a una videoconferencia. Si bien esta tecnología existe hace varios años, aún se encuentra poco difundida.

ISP (*Internet Service Provider*-Proveedor de servicios de Internet): *(Ver Provider)*

J

Java: Lenguaje de programación creado por Sun Microsystems. Desde su aparición, Java se perfila como un probable revolucionario de la Red. Como lenguaje es simple, orientado a objetos, distribuido, interpretado, robusto, seguro, neutral con respecto a la arquitectura, portable, de alta performance, multithreaded y dinámico. Java es un lenguaje de programación, un subset seguro de C++. Subset, porque algunas instrucciones (como las que

tienen que ver con la administración de memoria) no se pueden usar. Seguro, porque agrega características de seguridad a los programas. Un applet de Java se baja automáticamente con la página web y es compilado y ejecutado en la máquina local. Permite, entre otras cosas, agregar animación e interactividad a una página web, pero su característica más importante es que un programa escrito en Java puede correr en cualquier computadora. Para más datos http://java.sun.com/.

Javascript: Lenguaje de *scripts* para utilizar en páginas web desarrollado por Netscape. Permite aumentar la interactividad y la personalización de un sitio.

L

LAN (*Local Area Network*-Red de Área Local): Red de computadoras interconectadas, distribuida en la superficie de una sola oficina o edificio. También llamadas redes privadas de datos. Su principal característica es la velocidad de conexión. *(Ver WAN y MAN)*

Línea dedicada *(Leased line)*: Forma de conexión a Internet (con acceso las veinticuatro horas) a través de un cable hasta un proveedor de Internet. Esta conexión puede ser utilizada por varias personas en forma simultánea.

List serv: *Software* robot usado para la administración de un servidor de *mailing list.* Ampliamente utilizado.

Log: Archivo que registra movimientos y actividades de un determinado programa *(log file)*. Utilizado como mecanismo de control y estadística. Por ejemplo, el *log* de un Web server permite conocer el perfil de los visitantes a un sitio web.

Login: Proceso de seguridad que exige que un usuario se identifique con un nombre *(user-ID)* y una clave para poder acceder a una computadora o a un recurso. Ver Telnet.

Linx: *Browser* de web en modo texto, que no permite ver imágenes. Aún es ampliamente utilizado por quienes navegan desde estaciones UNIX.

M

***Mail Robot* (autoresponder):** Programa que responde *e-mail* en forma automática, enviando al instante información. Simplifica la tarea de admi-

nistrar un correo. Los programas utilizados para administrar *mailing lists* son un tipo de *mail robots.*

***Mailing List* (listas de interés):** Modo de distribución de *e-mail* grupal. Mecanismos de debate grupales entre distintas personas interesadas en un determinado tema. Similares en concepto a los *newsgroups,* pero no es necesario utilizar un servidor especial ya que los mensajes son recibidos por el usuario como correo electrónico.

Majordomo: Uno de los *software* de tipo *mail robot* usado para la administración de una *mailing list*.

MAN (*Metropolitan Area Network*-Red de Área Metropolitana): Red que resulta de varias redes locales (LAN) interconectadas por un enlace de mayor velocidad o *backbone* (por ejemplo de fibra óptica) en varias zonas. Es el tipo de estructura de red que se utiliza, por ejemplo, en un campus universitario, donde se conectan los diversos edificios, casas de estudiantes, bibliotecas y centros de investigación. Una MAN ocupa un área geográfica más extensa que una LAN, pero más limitada que una WAN.

MIME (*Multipurpose Internet Mail Extensions*-Extensiones Multipropósito para *e-mail)*: Formato específico de codificación para la transferencia de correo electrónico y attachments entre dos computadoras; contiene cualquier tipo de datos. Más moderno que el UUEncoding; aunque menos difundido.

***Mirror Site* (Sitio espejado o duplicado):** *Site* que hace una copia regularmente o en forma sistemática de toda la información de otro *site.* Se utiliza para disminuir y repartir la cantidad de accesos a un sitio web muy visitado o solicitado.

Módem (Modulador/Demodulador): Dispositivo que se utiliza para transferir datos entre computadoras a través de una línea telefónica. Unifica la información para que pueda ser transmitida entre dos medios distintos como un teléfono y una computadora. La velocidad del módem se mide en una unidad llamada baudios (bits por segundo), por ejemplo, 28.800 baudios. Cuanto más rápido es el módem, más datos pueden viajar por él en menos tiempo.

Mosaic: Primer *browser* de gran difusión, utilizado para navegar la Web. Desarrollado en febrero de 1993 por Marc Andreseen, fundador luego de la empresa Netscape.

***Mudd (Multi user Dungeons & Dragons*-castillos multi-usuarios):** Conjunto de juegos virtuales de texto para jugar a través de Internet. Originados en las universidades y basados en los llamados juegos de rol (*role-playing games*). Consisten en "universos" virtuales con cientos de partes, definidos por programadores, donde los participantes deben resolver acertijos y enigmas, muchas veces con la ayuda de otros jugadores.

Multimedia: Combinación de varias tecnologías de presentación de información (imágenes, sonido, animación, vídeo, texto) con la intención de captar tantos sentidos humanos como sea posible. Previamente a la existencia de la multimedia, el intercambio de información con las computadoras estaba limitado al texto. Luego, con el nacimiento de las interfaces de usuario gráficas y los desarrollos en vídeo y sonido, la multimedia permitió convertir el modo de comunicación entre personas y dispositivos aumentando la variedad de información disponible. El uso de la multimedia fue la razón principal por la que la World Wide Web facilitó la difusión masiva de Internet.

N

Navegador: *(Ver Browser/Web browser)*

Navegar: Recorrer la Web, sin destino fijo, siguiendo enlaces o direcciones.

Netiquette: Reglas de etiqueta, usos y buenas costumbres de Internet. Surgieron como una serie de políticas informales de "buen comportamiento" y se difunden de usuario en usuario para mantener vivo el espíritu de respeto propio de la Red. Un ejemplo de estas reglas es no escribir mensajes de correo electrónico todo en letras MAYÚSCULAS, ya que equivale a ¡GRITAR!

***Newsgroups* (grupos de debate):** Mecanismos de debate grupales entre personas de todo el mundo interesadas en un determinado tema. Permiten crear mensajes públicos, que los usuarios pueden crear, leer y contestar. Son distribuidos diariamente por toda Internet. También es el área en la que se agrupan los mensajes públicos según su temática. Similares en concepto, aunque no en funcionamiento, a las *mailing lists.*

***Nickname* (*Nick*, sobrenombre o alias):** Nombre de fantasía que un usuario de Internet utiliza, por ejemplo, para participar de un chat.

NNTP (*Network News Transfer Protocol*-Protocolo deTransferencia de Noticias de la Red): Protocolo normado de Internet utilizado para el intercambio y transferencia de *newsgroups* entre servidores.

Norma (o estándar): Conjunto de reglas sobre algún producto o servicio que garantiza uniformidad en todo el mundo en cualquier sistema en el que se implemente. Existen dos tipos de normas: la estándar (o normada), generada por comités especiales, y la *de facto* (o impuesta), que se acepta cuando un producto, debido a su uso, se convierte en universal. Los tres organismos más activos en el desarrollo de normas son: la ISO (International Standards Organization), la IEE (American Institution of Electrical and Electronic Engineers) y la CCITT (International Telegraph and Telephone Consultative Comitee). Las normas son la base de los sistemas abiertos.

NSLookup (antiguamente conocido como *Yellow Pages*): Programa que consulta al DNS para resolver direcciones IP en las direcciones de dominio correspondientes.

O

***Off-line* (fuera de línea):** Estado de comunicación diferida, no en tiempo real.

***On-line* (en línea):** Estado de comunicación activa, también llamado "en tiempo real".

Overhead: Desperdicio de ancho de banda, causado por la información adicional (de control, secuencia, etc.) que debe viajar además de los datos en los paquetes de un medio de comunicación. Afecta al *throughput* de una conexión.

P

Página *(page o Webpage)*: Unidad que muestra información en la Web. Una página puede tener cualquier longitud, si bien equivale por lo general a la cantidad de texto que ocupan dos pantallas y media. Las páginas se diseñan en un lenguaje llamado HTML y contienen enlaces a otros documentos. Un conjunto de páginas relacionadas componen un site.

***Password* (clave o contraseña):** Palabra utilizada para validar el acceso de un usuario a una computadora servidor.

PGP (*Pretty Good Privacy*-Muy Buena Privacidad): *Software* de encriptación *freeware* muy utilizado, desarrollado por Paul Zimmerman. Se basa en un método de clave pública y clave privada y es óptimo en cuanto a seguridad. Su eficacia es tal que los servicios de inteligencia de varios países ya lo han prohibido. Más datos en http://www.pgp.com/.

***Ping* (Unix):** Herramienta que permite averiguar si existe un camino (comunicación) de TCP/IP entre dos computadoras de cualquier parte de Internet.

***Pipe* (caño):** Término informal para conexión, cable, línea dedicada.

Plug & Play: Tecnología que permite agregar dispositivos a una computadora (por ejemplo, CD-ROM o placas de sonido) que se conectan y configuran automáticamente.

***Plug-in* (agregado):** Programa que extiende las habilidades de un navegador, permitiéndole mayor funcionalidad. Por ejemplo, se puede agregar un *plug-in* que permita ver vídeos, jugar un juego grupal o realizar una teleconferencia.

***Port* (puerto):** Conexión lógica y/o física de una computadora, que permite comunicarse con otros dispositivos externos (por ejemplo, una impresora) o con otras computadoras. Los servicios de Internet (como el *e-mail* o la web) utilizan ports lógicos para establecer comunicaciones entre una computadora cliente y un servidor.

Postmaster: Administrador humano de un servidor Internet. Cuando se desea efectuar una consulta sobre algún usuario de ese *server,* se envía un *e-mail* al *postmaster*, quien responderá la consulta. *(Ver Sysop y Webmaster)*

PPP *(Point to Point Protocol)*: Protocolo serial de acceso telefónico a Internet *(dial-in)*. Más moderno que el SLIP. Estándar normado (RFC 1134), multiprotocolo y que admite algoritmos de compresión y autenticación de los datos que viajan. Aún no es soportado por algunos *softwares* de conexión.

Programa: Sinónimo de *software*. Conjunto de instrucciones que se ejecutan en la memoria de una computadora para lograr algún objetivo. Creados por equipos de personas (llamados programadores) en lenguajes especiales de programación y se les diseña una *interface* de usuario para que puedan interactuar con las personas que los utilicen.

Protocolo: Conjunto de reglas formuladas para controlar el intercambio de datos entre dos entidades comunicadas. Pueden ser normados (definidos por un organismo capacitado, como la CCITT o la ISO) o *de facto* (creados por una compañía y adoptados por el resto del mercado).

***Provider* (Proveedor, ISP o Intermediario):** Empresa que actúa de mediador entre un usuario de Internet y la Red en sí misma. Ofrece el servicio de conexión *dial-in* o dedicado y brinda servicios adicionales como el *web hosting*.

***Proxy Server* (intermediario, mediador):** Utilizado en relación a Internet, hace referencia a un servidor que media entre el usuario (su computadora) y otro servidor de la Red. El *proxy server* puede hacer, por ejemplo, un pedido de información para un cliente en lugar de que el cliente lo haga directamente (método usado para salir de un *firewall*). También pueden actuar como traductores de formato de archivos (por ejemplo, convertir toda imagen GIF que pase por ellos en un BMP, o traducir del inglés al castellano, o convertir los *attachments*), o como cachés (almacenando en un directorio los archivos más pedidos últimamente, para entregarlos ante una nueva solicitud sin necesidad de que el usuario los busque por toda Internet), verificar la seguridad (virus, accesos permitidos, etc.), entre otras muchas tareas.

R

Red *(network)*: Dos o más computadoras conectadas para cumplir una función, como compartir periféricos (impresoras), información (datos, sistema de ventas) o para comunicarse (correo electrónico). Existen varios tipos de redes. Según su estructura jerárquica se catalogan en: redes cliente/servidor, con computadoras que ofrecen información y otras que solo consultan información, y las *peer-to-peer,* donde todas las computadoras ofrecen y consultan información simultáneamente. A su vez, según el área geográfica que cubran, las redes se organizan en LAN (locales), MAN (metropolitanas) o WAN (área amplia).

***Request* (pedido):** Solicitud de información o datos que una computadora cliente efectúa a un servidor.

RFC (*Request For Comment*-Pedido de Comentario): Documentos a través de los cuales se proponen y efectúan cambios en Internet, en general con orientación técnica. Los RFC son formularios con una estructura determinada, que pueden ser generados y distribuidos por cualquier persona que tenga una buena idea para cambiar o mejorar algún aspecto de Internet. Las

propuestas que contienen estos documentos se analizan, modifican y se someten a votación. Si resultan útiles, son puestas en práctica, convirtiéndose así en normas de Internet. La mayoría de los aspectos técnicos de la Red nacieron primero como RFC, por eso hoy en día hay cientos de ellos. Se puede consultar una base de datos en hipertexto de los RFC en http://www.auc.dk

R-login (Remote Login): Acceso a un *server* desde un sistema remoto. *(Ver Telnet)*

***Router* (ruteador):** Dispositivo de conexión y distribución de datos en una red. Es el encargado de guiar los paquetes de información que viajan por Internet hacia su destino. *(Ver TCP/IP, LAN)*

ROT13: Método de pseudoencriptación de datos en un mensaje público, utilizado para disimular el envío de un texto que pueda molestar a algunas personas. Para leerlo, reemplazar cada letra con la que está trece lugares antes en el alfabeto, ejemplo: la "n" por "a", etc. Por ejemplo, la frase: "Esto está codificado con ROT13" se leería: "Rfgb rfgn pbqvsvpnqb pba EBG13". Muchos programas de *newsgroups* realizan este proceso de conversión en forma automática.

S

Script: Programa no compilado realizado en un lenguaje de programación sencillo. *(Ver JavaScript)*

Server side CGI script: *Script* CGI que se ejecuta/corre en el servidor. *(Ver también Client side CGI script)*

***Server* (servidor de información):** Computadora que pone sus recursos (datos, impresoras, accesos) al servicio de otras a través de una red. *(Ver Host, Cliente/Servidor)*

SET (*Secure Electronic Transactions*-Transacciones Electrónicas Seguras): Un estándar para pagos electrónicos encriptados que está siendo desarrollado por Mastercard, Visa y otras empresas. Similar al SSL.

SGML (*Standard Generalized Markup Language*-Lenguaje de Marcado Generalizado Normado): Superconjunto de HTML. Lenguaje que define a otros lenguajes con tags, base del HTML utilizado en la Web.

Shareware: Política de distribución de programas donde se tiene derecho a probar un *software* por un determinado período antes de decidir

comprarlo. El importe a abonar por el programa es en general bajo, prácticamente nominal. *(Ver Freeware)*

Sistema operativo: Conjunto de programas que se encarga de coordinar el funcionamiento de una computadora, cumpliendo la función de *interface* entre los programas de aplicación, circuitos y dispositivos de una computadora. Algunos de los más conocidos son el DOS, el Windows, el UNIX.

Sistemas abiertos: Conjunto de computadoras de distintas marcas interconectadas que utilizan el mismo protocolo normado de comunicación. El protocolo estándar más difundido es el TCP/IP.

***Site* (sitio):** En general, se utiliza para definir un conjunto coherente y unificado de páginas y objetos intercomunicados, almacenados en un servidor. Formalmente es un servicio ofrecido por un server en un determinado *port.* Esta definición no siempre hace corresponder a un solo *site* con un *server;* por ejemplo: varios *servers* pueden responder a un mismo *site,* como los ocho *servers* que componen el buscador Yahoo! y también es posible que un solo *server* atienda simultáneamente varios *sites,* como sucede en los *servers* de los proveedores de *web hosting*.

SMTP (*Simple Mail Transfer Protocol*-Protocolo Simple de Transferencia de Correo): Protocolo estándar de Internet para intercambiar mensajes de *e-mail.*

***Snail mail* (correo caracol):** Modo en que el correo postal común es conocido en Internet. Juego de palabras por su lentitud comparada con la inmediatez del *e-mail.*

Software: Componentes intangibles (programas) de las computadoras. Complemento del *hardware.* El *software* más importante de una computadora es el sistema operativo.

Spam: Mensaje electrónico no solicitado enviado a muchas personas. Considerado una mala práctica de márketing directo por quienes desconocen las reglas de *Netiquette.*

***Spiders* (arañas):** Complejos programas autónomos que recorren la Web siguiendo enlace tras enlace en cada página; almacena estas últimas para que más tarde sean catalogadas en las enormes bases de datos de los índices de búsqueda.

SSL (*Secure Socket Layer*-Capa de Seguridad): Estándar para transacciones electrónicas encriptadas que está siendo ampliamente utilizado para hacer negocios vía la Red. *(Ver SET)*

***Streaming* (Transferencia contínua):** Sistema de envío continuo de información, que permite, por ejemplo, ver un vídeo a medida que se baja de la Red.

***Style sheets* (hojas de estilo):** Novedosa facilidad de HTML, similar a la que poseen los procesadores de texto, que permite definir un parámetro de diseño que se repite en todas las páginas de un sitio.

***Sysop (System operator*-operador del sistema):** Persona encargada de la administración y el mantenimiento de un *host. (Ver Postmaster y Webmaster)*

T

***Tag* (etiqueta):** Código marcador de estructura de lenguaje HTML utilizado para estructurar las páginas de la Web.

TCP (*Transmission Control Protocol*-Protocolo de Control de Transmisión): Conjunto de protocolos de comunicación que se encargan de la seguridad y la integridad de los paquetes de datos que viajan por Internet. Complemento del IP en el TCP/IP.

TCP/IP (*Transmission Control Protocol/Internet Protocol*-Protocolo de Control de Transmisión/Protocolo Internet): Conjunto de casi cien programas de comunicación de datos usados para organizar computadoras en redes. Norma de comunicación en Internet compuesta por dos partes: el TCP/IP. El IP desarma los envíos en paquetes y los rutea, mientras que el TCP se encarga de la seguridad de la conexión, comprueba que los datos lleguen todos, completos y que compongan finalmente el envío original.

Teleconferencia: Sistema que permite conversar con una o varias personas simultáneamente, viendo su imagen en movimiento (vídeo) además de la voz.

Telnet (Unix): Programa que permite el acceso remoto a un *host*. Utilizado para conectarse y controlar computadoras ubicadas en cualquier parte del planeta.

***Thread, threaded messages* (hilación, mensajes hilados):** Mensajes de correo electrónico (de un *newsgroup* o una lista de interés), relacionados al mismo tema o que son respuestas a un mismo asunto.

Throughput: Rendimiento final de una conexión. Volumen de datos que una conexión brinda como resultante de la suma de su capacidad y la resta de los overheads que reducen su rendimiento. *(Ver Red)*

U

Unix: Sistema operativo diseñado por los Laboratorios Bell y refinado en Berkley entre otros lugares, que soporta operaciones multiusuario, *multitasking* y estándares abiertos. Ampliamente difundido en Internet, es utilizado para ejecutar en los servidores.

Upgrade: Actualización de un programa.

***Upload* (subir):** Proceso de enviar un archivo desde su computadora a otro sistema dentro de la Red. *(Ver Download, FTP)*

***URL* (*Uniform Resource Locator*-Localizador Uniforme de Recursos):** Dirección electrónica (por ejemplo: iworld.com.ar). Puntero dentro de páginas HTML que especifican el protocolo de transmisión y la dirección de un recurso para poder acceder a él en un server de web remoto.

User Account: Cuenta de usuario. Similar a *user ID.*

User ID: Identificación de usuario en una computadora. Relacionado con una clave de acceso o *password.*

UUEncoding: Mecanismo de conversión que permite adjuntar *(attachment)* cualquier tipo de archivo a un mensaje, codificando el archivo en caracteres ASCII para que los sistemas en Internet lo puedan entender y transmitir. Similar al MIME, aunque menos moderno y más difundido.

V

Virus: Pequeños programas de computadora que tienen la capacidad de autoduplicarse y parasitar en otros programas. Una vez que se difunden, los virus se activan bajo determinadas circunstancias y, en general, provocan algún daño o molestia. *(Ver Worm)*

W

W3C (World Wide Web Consortium): Organización que desarrolla estándares para guiar la expansión de la Web. Organizado por el CERN y el MIT

y apadrinado por varias empresas. Su *website* es: http://www.w3.org/. *(Ver Sistemas Abiertos)*

WAN (*Wide Area Network*-Red de Área Amplia): Resultante de la interconexión de varias redes locales localizadas en diferentes sitios (distintas ciudades o países), comunicadas a través de conexiones públicas (líneas dedicadas). La conexión puede ser física directa (un cable) o a través de un satélite, por ejemplo. La conexión es más lenta que una LAN. Ver MAN, RED.

Web: *(Ver World Wide Web)*

Webmaster: Administrador y/o autor de un sitio web. *(Ver Postmaster)*

WebTV: Dispositivo que cruza entre una PC simple y un televisor. Tiene como objetivo abaratar los costos de acceso a la Red y simplificar su uso. Si bien fue lanzado en diciembre de 1996, hasta ahora ha tenido poca difusión. Más datos en: http://www.webtv.com/.

***White Pages* (páginas blancas):** Listado de direcciones electrónicas de usuarios de Internet.

***Whiteboard* (pizarrón blanco):** Programa especial para trabajo en grupo que permite que varias personas trabajen a la vez en un proyecto. Aunque las personas no estén físicamente en un mismo lugar, pueden trabajar a la vez desde cualquier punto del planeta a través de Internet. *(Ver Groupware)*

***Workstation* (estación de trabajo):** Puesto de trabajo o computadora de un usuario. Similar al concepto de Cliente. También se llama así a pequeños servidores con gran capacidad gráfica, como los de Silicon Graphics.

World Wide Web o W3 o WWW: Conjunto de servidores que proveen información organizada en *sites*, cada uno con cierta cantidad de páginas relacionadas. La web es una forma novedosa de organizar toda la información existente en Internet a través de un mecanismo de acceso común de fácil uso, con la ayuda del hipertexto y la multimedia. El hipertexto permite una gran flexibilidad en la organización de la información, al vincular textos disponibles en todo el mundo. La multimedia aporta color, sonido y movimiento a esta experiencia. El contenido de la web se escribe en lenguaje HTML y puede utilizarse con intuitiva facilidad mediante un programa llamado navegador. Se convirtió en el servicio más popular de la Red y se emplea cotidianamente para los usos más diversos: desde leer un diario de otro continente hasta participar de un juego grupal.

***Worm* (gusano):** Tipo de programa similar al virus que se distribuye en una red. Su objetivo es generalmente afectar o dañar el funcionamiento de las computadoras.

X

X25: Uno de los tantos protocolos estandarizado bajo normas internacionales, de comunicación *packet-switching*. Utilizado ampliamente en redes públicas de comunicaciones.

Y

***Yellow Pages* (páginas amarillas):** listado de direcciones electrónicas de comercios en Internet. *(Ver White Pages)*

DICCIONARIO DE USUARIOS DE LA RED

A

Arqueólogo: Se llama así a los usuarios que "reavivan" mensajes anticuados dejando comentarios insustanciales, solo para colocar los viejos hilos en los primeros puestos e incomodar a los demás usuarios del foro.

B

Bigot: Aquellos usuarios que son intolerantes con ciertas características de una persona, ya sea raza, edad, sexo, religión...

Blogger: Es el nombre que reciben los usuarios que tienen y mantienen un blog o espacio virtual. Existen múltiples variaciones como *floggers* (creadores de Fotologs o *flogs*) o *vloggers* (creadores de Videoblogs o *vlogs*). Los creadores de sitios webs con fines meramente publicitarios o de *spam (splogs)* se les llama *sploggers.* Cuando se trata de una página más genérica se les llama *webmaster,* aunque este último es más general y engloba a todos los usuarios responsables de la gestión del sitio web.

BOFH. Proviene del inglés: ***Bastard Operator From Hell*** **('maldito administrador del infierno'):** Es aquel usuario (generalmente administrador o técnico jefe de un grupo de usuarios) que actúa de forma agresiva con los usuarios inexpertos *(Ver Lusers)* divirtiéndose a costa de su posición y la falta de conocimiento de los inexpertos.

C

Chater: Se denomina así a los usuarios que abusan del lenguaje chat, así como los *smileys,* lenguaje SMS o expresiones de chat.

Cheater: Procede del inglés **('tramposo'):** Se trata de aquellos usuarios que en los juegos, usan trucos o trampas para conseguir sus objetivos. A veces aprovechando *bugs* del juego, a veces con programas externos u otros medios más o menos complejos. Son bastante frecuentes en comunidades de juegos *on-line* o *multiplayer.*

Cracker. Procede del inglés: *crack* **('romper')** y hace juego con las palabras *criminal hacker:* Usuarios que, generalmente, se encargan de (solo y

exclusivamente) "romper" sistemas de seguridad de aplicaciones mediante *cracks,* seriales (números de serie) o *keygen* (generadores de claves). El término también engloba a aquellos usuarios que violan sistemas de seguridad en beneficio propio o en perjuicio del sistema comprometido, pudiendo o no, robar información.

D

Domainers: Son aquellos usuarios que se dedican a comprar y registrar dominios (nombres.com) para monetizarlos y ganar grandes sumas de dinero. Suelen poner bastante atención en registrar dominios tras eventos importantes o creaciones de marcas relevantes para una posible posterior reventa.Una variante, bastante peligrosa, se dedica a montar empresas que ofrecen un servicio de comprobación de disponibilidad de dominios, que cuando es utilizado, lo compra para una futura reventa.

F

Fandom. Proviene del inglés: ***fan kingdom***: Aunque el anterior término se ha "estirado" hasta abarcar la definición de personas obsesionadas de forma fanática un tema, hobby o pasatiempo, *fandom* engloba especificamente esta última definición.

Flamer. Del inglés: ***flame*** **('llama', 'incendiar'):** Usuario que intenta interrumpir el curso o discusión de una comunidad con un mensaje no constructivo, generalmente de insulto, con el único propósito de desviar la discusión (y posible creación de temas interesantes) para generar enfrentamientos inútiles *(flamewar)* entre distintos usuarios. También se denomina *holywar* a las discusiones banales que generalmente son preferencias personales como Linux-Windows, PC-Mac, vim-emacs, etc.

Friki. Del inglés: ***freak*** **('raro'):** Término que ha sido adoptado para denominar a personas que tienen un comportamiento o apariencia fuera de lo habitual.

G

Gamer. Proviene del inglés: ***game*** **('juego'):** Usuarios que pasan horas diarias delante de juegos, diferenciándose de otros jugadores porque intentan sacar las máximas puntuaciones posibles, conseguir encontrar todos los

finales alternativos en juegos que los tengan, etc. Por otra parte, también existen los *proGamers,* que son aquellos jugadores profesionales y expertos que se dedican a participar en torneos oficiales y ganar dinero solo por participar, o los gosu, aquellos que además de fanáticos son considerados grandes expertos.

Geek: Aquellos usuarios, generalmente extrovertidos, que sienten gran atracción por la tecnología y la informática hasta el grado de fanatismo. También suelen ser denominados *digerati.*

H

Hacker. El término procede del inglés: ***hack*** **('recortar')** haciendo alusión a las modificaciones que hacían ciertos expertos para mejorar funcionamientos. Frecuentemente utilizada de forma errónea, son aquellos usuarios que son considerados expertos en una cierta materia, normalmente relacionada con la informática (redes, seguridad informática, criptoanálisis, inteligencia artificial...).

Este término ha sido muy desprestigiado con el tiempo a través de la prensa, y los medios de comunicación, hasta que en la actualidad, se suele hacer mención a *hacker* como un concepto que engloba a *hackers* y *crackers*. De forma burlona se suele denominar *juanker*.

Para paliar en cierta forma la confusión de términos, dentro de la categoría *hacker* se usan los términos *whiteHat* (sombrero blanco) a los *hackers* "buenos" (los que no realizan acciones destructivas) y *blackHat* a aquellos que encajan mejor en el concepto de *cracker*.

Hoaxer: Son los usuarios que crean bulos o correos en cadena que usualmente mencionan con engaños y falsas amenazas de que si no se reenvian ocurrirá alguna desgracia.

Normalmente solo intentan propagarse aprovechando la ausencia de experiencia de los usuarios que lo reciben y no tienen ningún fin monetario ni de otro tipo.

Hoygan: Usuarios con bajo nivel cultural (faltas de ortografía exageradamente numerosas) y en muchos casos de muy corta edad son denominados bajo este término. Proviene en forma de parodia a la palabra oigan, que muchos utilizan para pedir ayuda o decir frases sin sentido aparente.

Suelen saltarse todo tipo de reglas como no escribir en mayúsculas, insultar u otras. Suele utilizarse bastante en Latinoamérica (en España oigan no se suele usar mucho), por lo que inventaron el sinónimo *bengatio* como variante española.

L

Lamer: Son aquellos usuarios que presumen de tener ciertos conocimientos que realmente no tienen. Habitualmente son personas con falta de madurez, poca sociabilidad o habilidades que buscan una forma falsa de destacar sobre los demás.

Este término procede de un virus para Commodore Amiga (Lamer Exterminator) que sobreescribía en disco la palabra LAMER! ochenta y cuatro veces hasta volverlo inservible.

Leecher. Del inglés: ***leech*** **('sanguijuela'):** Usuario de espíritu egoísta que es dado a aprovecharse de la bondad de los demás al compartir recursos. Su antónimo se denomina *seeder.*

Por ejemplo, el perfil de los usuarios *leechers* son aquellos que restringen la subida de los programas P2P (para descargar pero no enviar), retiran los archivos una vez descargados para no compartirlos o prefieren la descarga directa o programas como P2M para solo beneficiarse él mismo y no compartir.

Lurker. Del inglés: ***lurk*** **('acechador'):** Se llama así a los usuarios que participan de forma silenciosa en una comunidad, solo leyendo sin contribuir con comentarios o aportar información. Generalmente, los *lurkers* no muestran su opinión por miedo a ser ridiculizado por *trolls,* por creer no tener nada interesante que decir, perder el anonimato u otras causas. Este término suele ser usado para personas benévolas o sin ánimo de maldad. *(En caso contrario: Ver leecher)*

Luser. Del inglés: combinación de ***loser*** **('perdedor')** y ***user*** **('usuario'):** Es la forma despectiva de referirse a usuarios sin los conocimientos avanzados (generalmente informáticos) que posee el que lo dice.

N

Nerd: Se trata de aquellos usuarios con el ideal "científico", que son activamente inteligentes, interesados por la adquisición de nuevos conocimien-

tos pero muy torpes a nivel social, sin reflejos para mantener conversaciones fuera de sus temas de interés, etc.

Newbie. Proviene del inglés: ***New boy:*** Concepto que se utiliza para denominar a aquellos usuarios que son principiantes o novatos en una comunidad. Son considerados *newbies* los usuarios que, por ejemplo, ingresan a una comunidad haciendo preguntas:

- Obvias o sencillas: Por ejemplo cómo configurar el emule, en un foro donde ya hay más de un mensaje explicándolo.
- Extensas en pocas palabras: Por ejemplo cómo montar un ordenador por piezas sin tener conocimientos informáticos.

Existen varias categorías dentro de los *newbies*:

- ***Noobs*** o ***n00bs:*** Forma despectiva de tachar a los *newbies* que presumen de conocimientos que no tienen.
- ***Nirjil:*** *newbies* con conocimiento mayor que los *noobs,* pero generalmente obsoletos, con información cierta, pero inútil o muy torpes.

O

Otaku. Proviene del japonés: ***otaku*** (algo así como 'mucho tiempo en casa honrando su hobby'): Idéntico al *fandom,* pero solo en torno a fanáticos de películas de género *anime* o animación japonesa.

P

Pharmers: Usuarios que se encargan de explotar problemas y vulnerabilidades de DNS (resolución de dominios a IP) para que al intentar acceder a una página legítima redireccione a una falsa, mostrando el mismo nombre de dominio. A diferencia de los *phishers* (que suelen utilizar nombres de dominio diferentes a la web legítima, aunque tampoco tiene por qué ser así), se hace referencia a los *pharmers* cuando intentan engañar simulando el mismo nombre de dominio. Por el contrario los *phishers* intentan engañar por apariencia del sitio web.

Phisher. Proviene del inglés, **'estafa'** o **'fraude':** Son aquellos usuarios que intentan adquirir información confidencial ajena por un medio que aparente ser legítimo y por lo tanto, la víctima no se percate del engaño. Los

phishers crean páginas webs de bancos, gestores de correo o compañías importantes, de modo que al ponerse en contacto con la víctima, ésta acceda a la página falsa, se registre enviando los datos al sitio falso y ser enviado de forma transparente al sitio verdadero. Esto se conoce como *phishing.*

Phreaker: Se engloba en esta categoría aquellos usuarios que son una especie de *crackers* de tecnología de telefonía. Intentan estudiar sistemas de telefónicos, VoIP, Bluetooth... para obtener algún tipo de beneficio. Estos primeros tres términos suelen confundirse bastante a menudo y englobarse en la misma categoría.

Pirata informático: Usuario que utiliza una serie de recursos (de forma ilegal) y gracias a ello, conseguir lucrarse. Este concepto sí está bastante extendido y correctamente, aunque muchas veces se desconoce que si no existe ánimo de lucro no suele catalogarse como tal.

Poseur: Muy similar al *wannabe,* salvo que a éste solo le interesa aparentar ser miembro del grupo, sin importarle realmente los ideales, el conocimiento o cualquier otra cosa del mismo.

A diferencia del anterior, este se aplica mucho más en el "mundo real", como por ejemplo, las personas que hacen uso de determinados estilos musicales o modas y apariencias para autoconvencerse ser miembro de la misma.

S

Script Kiddie: Exactamente similar a los anteriores, salvo que estos usuarios presumen ser malvados *crackers.* Se caracterizan por utilizar programas desarrollados por otras personas (no saben lo que hacen) y utilizar la ignorancia (y sobre todo, el miedo) de personas inexpertas para conseguir sus objetivos amenazándolos con *"hackearlos"* en caso contrario.

Una forma más despectiva de denominarlos es h4x0r, haciendo burla a ciertos detalles que utilizan bastante como reemplazar ciertas letras por números: escritura *leet* (de élite). Incluso Google ha publicado su propia burla: Google h4x0r.

Snob: Son personas que imitan los gestos, opiniones y/o apariencia de aquellos a los que idolatran o consideran de clase social alta, para aparentar ser como ellos. Son referenciados de forma despectiva como *sn0b.*

Spammer: Son aquellos usuarios que utilizan los distintos medios a su alcance o comunidades para enviar mensajes no deseados (generalmente publicitarios).

Normalmente se hace de forma automática y masiva, para hacer llegar al mayor número de personas posible.

Spoofer: Se llama así a los usuarios que utilizan técnicas de suplantación de identidad. El más conocido es el IP Spoofing, que se trata de manipular los paquetes IP (generalmente desde un elemento intermedio) para que al enviarlos desde un sistema a otro, cambiar la dirección de destino a un destinatario diferente y obtener la información.

T

Trolls: Los *trolls* realizan acciones destructivas como aportar información errónea para causar confusión, usuarios "anónimos" que dejan varios mensajes simulando ser distintas personas, etc. Se suele decir la frase "no des de comer al *troll*" para hacer referencia a que no hay que hacerles caso.

W

Wannabe. Proviene del inglés: ***Want to be*** **('quiero ser'):** Usuario aficionado a un determinado tema y que quiere formar parte de un grupo de especialistas de dicha actividad. Se trata de una persona con conocimientos por encima del promedio, pero consciente de que no está a la altura del nivel del grupo y que debe aprender más.

DICCIONARIO DEL CHAT

A

ACG, del inglés: *A call get,* 'recibí la llamada'. Usado para avisar de que se recibió una llamada.

AEMJEFE: Kid nab de haloce.

ACM1PT: 'Haceme un pete', es decir, pedir sexo oral. Término utilizado en Uruguay, Argentina y Chile, popularizado por el personaje uruguayo de Internet "El bananero" como ofensa hacia otros.

AFAIK, del inglés: *As far as I know,* 'Hasta donde sé'. Usado para dar una información más bien escasa.

ASAP, del inglés: *As soon as possible,* 'lo más pronto posible'. En español se usa cuando algo es prioritario. *Ejemplo:* "Cojan la bandera ASAP".

A4AF, del inglés: *Asking for another file,* 'se le ha pedido otro archivo'. Se usa en los programas P2P, cuando se está pidiendo un archivo y el usuario al que se le pide muestra A4AF en su estado. *Ejemplo:* eMule.

AFK, del inglés: *Away from keyboard,* 'lejos del teclado'. Normalmente se usa en MMORPG con jugadores que están ausentes.

ASL, del inglés: *Age, sex, location,* 'edad, sexo, localización'. Utilizada en los chats para dar a conocer estos datos o preguntárselos a alguna persona.

Admin: Apócope de *Administrator*/Administrador. Dícese de la persona que alguien elige para controlar un servidor, ya sea de un juego, un foro, etc. Esta persona posee el poder de *banear, kickear* y hasta eliminar a los usuarios que estén en su servidor.

AFRW, del inglés: *Away from real world,* 'lejos del mundo real'. Se emplea para dirigirse a personas que se imaginan que son parte y están dentro del juego.

AKA, del inglés: *Also known as,* 'también conocido como'.

APLH, de 'Apaga y prende la hueva'. Apaga y enciende el computador/servidor después de un fallo/error no recuperable.

ASDF: Se dice cuando no se tiene nada que decir pero se quiere tener la última palabra o para crear *spam* en los foros de Internet.

B

Banear: Españolización del verbo inglés *to ban,* 'expulsar'. Impedir el acceso a un usuario de un foro o un sitio por parte de la administración. Generalmente un usuario es *baneado* por incumplimiento reiterativo de las normas del lugar.

Brb, del inglés: *Be right back,* 'vuelvo enseguida'.

BBL, del inglés: *Be back later,* 'vuelvo más tarde'.

BBQ: Conjunto de letras que dichas en inglés vienen a significar 'barbacoa'; en inglés *barbacue.*

BFF, del inglés: *Best friends forever,* 'mejores amigos/as para siempre'.

BILF, del inglés: *Boy I'd like to fuck!,* 'chico con el que me gustaría hacer el amor'.

BSoD: Siglas de *Blue Screen of Death,* 'pantallazo azul de la muerte'. Pantalla que aparece generalmente en Windows cuando ocurre un error grave que impide que el sistema pueda continuar funcionando.

BTW, del inglés *By the way,* puede traducirse como 'a propósito de...', 'hablando de...', o simplemente 'por cierto'.

Bug: Palabra inglesa utilizada en cualquier *software* para referirse a fallos en su programación.

B4: *Before*, en español 'antes'.

BKN, de la jerga chilena *bakán* 'genial', '*cool*'. Conocido por primera vez desde la teleserie con el mismo nombre.

BS, del inglés: *Bullshit,* 'mentira', 'tontera' e incluso literalmente 'mierda'. Se usa comúnmente cuando sucede algo muy improbable dentro de un juego favoreciendo a uno de los dos jugadores.

Bestie: abreviación de: *Best friends,* equivalente a **BFF.**

Bot: palabra que puede significar robot y que se designa a usuarios de foros y, sobre todo, chats y salas de charla *on-line,* que no son usuarios humanos, sino usuarios mecánicos establecidos en el servidor y programados para que hablen automáticamente respondiendo a los comandos programados.

B7, significa: *Besets,* 'besitos'.

Bn: Acrónimo de 'bien'.

BB, del inglés: *Bye bye,* 'adiós'; también usado como bebé.

C

CASTER: Personaje que se ocupa de hacer daño a distancia. También se usa en los videojuegos de rol.

COCHA: Término empleado para hablar de la "cocha", que es algo que no se puede describir por su grado de asquerosidad.

C8, del inglés: *Ceigth,* 'cretino'. Utilizado pocas veces en chats, foros, MMORPG.

Carroñero: Usado en los juegos PvP. Dícese de la persona que elimina (derrota) a un jugador que estaba siendo atacado por otro en el momento en que dicho jugador ya se encontraba débil. *(Véase también "fragear" (Latinoamérica))*

Cheat, derivado del inglés: 'trampa'. Usado normalmente por los llamados *noobs,* jugadores principiantes, para ganar fácilmente una partida. Existen algunos que solo con un *click* hace ganar la partida, hay otros que sin siquiera mover un dedo hace ganar todas las partidas. Se usa para ganar experiencia en juegos de rol, o para hacerse notar en juegos FPS, pero ya sabiendo que es un cheater o cheto.

CTM: Acrónimo interpretado principalmente en Chile por 'concha de tu madre' *(Conchetumadre* es pronunciado). También se puede interpretar en México como 'chinga tu madre', 'checa tu mail', 'cago en tu madre'.

CHTM: Acrónimo de 'chinga tu madre'.

Crashed: Hace referencia al apagado del ordenador de golpe, sin previa preparación.

CSM: Acrónimo de 'conchesumadre', con el mismo significado de **CTM**, pero referido a una tercera persona.

CU2MORO, del inglés: *See You tomorrow, '*mañana nos vemos'.

Cya: Significa *See ya!,* '¡nos vemos!'.

CUL8R, del inglés: *See you later!,* '¡hasta después' o 'nos vemos después'.

CTF, del inglés: *Capture the flag,* 'captura la bandera', comúnmente usado en videojuegos multijugador bélicos o de guerra.

D

Deface/Defacement: Romper la seguridad de un sitio web y cambiar la página principal.

Delay, del inglés; en español: 'retraso'. El *delay* en los videojuegos quiere decir que las acciones están retrasadas, es decir, que se hace un movimiento y el juego se demora cierto tiempo en realizarlo, generado por la distancia del usuario al servidor *(ping).*

DND, del inglés: *Do not disturb,* 'no molestar'. Esta frase es generalmente usada en programas de mensajería instantánea para indicar el estado en el que se encuentra el usuario.

DPS, del inglés: *Damage per second,* 'daño por segundo'. También se usa en los videojuegos MMORPG para un jugador cuya principal función es la de hacer una gran cantidad de daño a los enemigos.

Dew, del catalán *Adéu,* 'adiós'. Utilizado en los MMORPG y en chats.

DNCER: Significa 'del Nido, cómeme el rabo'. Muy usado en Bilbao.

Dw, del inglés *Don't worry,* 'no te preocupes'.

E

Edith: Se emplea cuando se quiere insultar a una persona muy negra de origen japonés, también si se quiere referir a los pies con ácido.

:B: Se utiliza para mostrar una cara en la que los dos puntos (:) son los ojos y la B es una boca que enseña los dientes con cara alelada o poco inteligente.

Su significado puede ser similar al de xDDD o cuando se quiere mostrar una ironía.

Edit, del inglés: *Edit* o *edited,* 'editado'. Utilizada en juegos *on-line* para decir que alguien tiene un personaje editado de forma que hace uso ilegal del personaje, beneficiándose sobre otros.

Élite: Palabra que designa superioridad tanto para jugadores como para NPC (personajes no jugadores).

F

Farm, del inglés 'granja'. Dícese del jugador que por su inexperiencia o impericia en un juego, hace que otros jugadores se aprovechen de él, ganando experiencia o recursos a su costa. O aquel que se aprovecha de una falla del juego para sacar puntaje extra.

FD: En español: 'fuertes declaraciones'.

Flood, del inglés: 'inundación'. Programa o *script* diseñado para saturar a base de repetición de un texto, generalmente *spam*. Un usuario también puede realizar esta acción.

Frags: Proviene originalmente del juego Unreal (de 1998 posterior a Quake y predecesor del Unreal Tournament), donde a cada punto obtenido por matar a otro jugador se le llamaba de esta forma. Actualmente se utiliza este término en muchos juegos de acción con la misma dinámica (matar otros jugadores).

Freeze: Hace referencia a 'tildar', 'colgar' o 'congelar', pero habiendo la posibilidad de que luego, de un instante, continúe. *Ejemplo:* "Se *freezo* el juego" (léase como: "se congeló el juego").

F2P, del inglés: *Free to play* (El 2 sugiere el sonido del artículo inglés *"to",* al ser éste muy similar con el de dicho número "*two")*. Se utiliza para etiquetar los servidores de juego gratuito, especialmente para juegos MMORPG.

FILF, del inglés: *Father I'd like to fuck*, 'me follaría a tu padre'.

FTW, del inglés *For the win*, que vendría a significar literalmente 'por la victoria'. Se utiliza cuando apoyas algo.

FYI, del inglés: *For your information*, es decir, 'para tu información' o 'para tu conocimiento'. Es utilizado para retransmitir o reenviar información o *e-mails* de interés.

Fake, del inglés: 'falso'. Se utiliza para engañar virtualmente a la gente por Internet, es muy parecido al Xploit.

FoF: 'Foto o *fake'*. Se utiliza cuando ingresan nuevos miembros femeninos en una comunidad de foros. En otras palabras, se pide una 'foto o *fake*' para comprobar que dicha persona es realmente una mujer. También se utiliza en caso de alguna noticia o hecho en el que se tenga que demostrar que es realidad y no algo falso.

Flooder, del inglés: *Flood,* 'inundación'. Persona que escribe mucho y seguido (en vez de un solo envío con comas) o haciendo *flood* normal.

FUD, del inglés: *Fear, uncertainty and doubt,* 'miedo, incertidumbre y duda'. Definición que describe una estrategia comercial, basada en el miedo, cuyo objetivo es el de perjudicar a un competidor. Dicha técnica consiste en difundir información negativa, falsa, vaga o sesgada.

FUF: 'Festejen uruguayos, festejen'. Se utiliza solo cuando se logra algo importante que hace años (o mucho tiempo) que se buscaba y no se podía obtener. También se utiliza irónicamente cuando no hay nada que festejar.

FFA, del inglés: *Free for all,* 'libre para todos'. Todos pueden atacar a los distintos objetivos sin respetar turnos o llegadas.

FPS: Puede significar *First person shooter, '*juego de acción en primera persona. Otro significado es *Frames per second,* 'fotogramas por segundo', referente a la cantidad de imágenes por segundo de un videojuego.

FAIL, del inglés; en español 'fallo'. Suele indicar una acción penosamente realizada, aunque también se usa para crear incomodidad en alguna situación real.

G

GR8, del inglés: *Great,* 'genial', 'magnífico'.

Gamer: Persona apasionada por los juegos, ya sean de ordenador, Internet o videoconsolas.

***Game master/*GM:** Persona que se ocupa del buen funcionamiento de un juego *on-line* y de solucionar problemas con los jugadores.

Gayer: Adjetivo utilizado para designar a una persona no decidida a realizar una acción ya sea en una realidad virtual o no.

Geek: Persona con una gran fascinación por la tecnología e informática, abarcando los diferentes tipos de *geek* desde un nivel de fascinación normal hasta niveles obsesivos.

Gg, del inglés: *Good game,* 'bien jugado'. Al finalizar una partida se utiliza para mostrar que ésta ha sido una buena partida o felicitar al ganador de esta.

GILF, del inglés: *Girl I'd like to fuck,* 'chica con la que me gustaría follar'.

GIYF, del inglés: *Google is your friend,* 'Google es tu amigo'. Esta suele ser la respuesta que recibe cualquier pregunta que hubiera sido fácilmente respondida buscando en el motor Google. También puede indicar (no obligatoriamente) que quien responde se siente ofendido y considera una falta de respeto que la persona que pregunta no se tome el trabajo de leer y buscar por su cuenta, caso en el cual, encontraría fácilmente la solución a su interrogante.

Gl, del inglés: *Good luck,* 'buena suerte'. Se dice antes de empezar una partida para desear suerte a los otros jugadores de ésta. Suele ir acompañada de **hf** *(Have fun/*'diviértete').

Glitch: *Bug* que beneficia al que lo realiza.

Googlear: Buscar cosas en Internet, más especificamente en la plataforma de Google.

GTFO, del inglés: *Get the fuck out, '*vete a la mierda'.

Gj, del inglés: **Good job,** 'buen trabajo'. Su intención es similar a **Gg.**

GZ: Significa enhorabuena por un logro obtenido, también suele decirse *"Gratz".*

GvG: Significa *Guild vs Guild,* 'Clan vs Clan'.

Gf: Acrónimo de *Girlfriend* que en español significa 'enamorada', 'novia'. Generalmente se usa en juegos MMORPG para invitar a una chica a estar con el usario. También puede querer decir (dependiendo del contexto) *Good fight*

'buena pelea', después de haber librado un duelo o pelea con otro usuario, en juegos como por ejemplo el Jedi Knight multijugador . Es una muestra de respeto (ya se gane o se pierda).

g2g o gtg: Significa: *Going to go,* es decir, 'estarse yendo'.

GAMEAR: Variación de jugar.

GWS, del inglés: *Get well soon,* 'recupérate pronto'.

H

Hack: Derivado del inglés *(Véase hacker (informática)).* Casualmente se usa para nombrar trampas en juegos. *Auto-aim, no-recoil, speedhack,* se los usa comunmente en juegos de ROL y FPS.

Hav: Se pronuncia *"hab".* Viene de la palabra en inglés: *Have,* 'tener'. Es una variación de la misma.

HDSPM: 'Hijo de su puta madre', término vulgar despectivo de alguna persona.

Healer: 'Sanador', personaje que ocupa el rol de curación.

HNFI: Acrónimo de *Have no fucking idea, '*no tener ni puta idea'.

HF: Acrónimo de *Have fun,* 'diviértete'. Utilizada para desear a los jugadores de una partida que se diviertan jugándola.

Hacker: Dícese de la persona que utiliza *hacks.*

Hoygan: Persona que en foros con normas en las que se prohíbe pedir u ofrecer *warez,* lo pide, entre otras peticiones, como exigir algunas cosas que son absurdas. Se suele destinar también a personas que escriben estilo SMS y con faltas de ortografía en exceso.

HUNTED: Es una amenaza, da a referir que te asesinará el otro *player,* por ejemplo, si te dice "estás *hunted!"* es que te intentará matar.

HDP: 'Hijo de puta'. Término vulgar despectivo hacia alguna persona.

H8, del inglés: *Hate,* 'odio'.

HDC, del inglés: *Hide doesn't count,* 'esconderse' o 'esconder algo no vale'.

I

IDC, del inglés: *I don't care,* 'no me importa'.

IDK, del inglés: *I don't know,* 'no lo sé'.

IGM, del inglés: *In game message,* 'mensaje dentro del juego'.

IGN, del inglés: *In game name,* 'nombre dentro del juego'.

IKR, del inglés: *I know right?,* 'lo sé, ¿verdad?.

IMHO: Acrónimo de *In my humble opinion,* 'en mi humilde opinión'.

IMO, del inglés: *In my opinión,* 'en mi opinión'.

ILY, del inglés: *I Love You,* 'te amo'.

ILU, del inglés: *I love U (You),* 'te amo'.

IRL, del inglés: *In real live,* 'en la vida real'. ***IRL**

IMBA: Acrónimo del término *Imbalanced,* 'ser poderoso'.

J

JK, del inglés: *Just kidding,* 'solo estoy bromeando'. Utilizado cuando se quiere dejar algo claro.

JD: Igual que 'fuertes declaraciones' pero dicho *"juertes*" declaraciones.

Jamer: (equivalente a KS). Usado en los MMORPG *(Massive Multiplayer Online Role Playing Game)* para referirse a la gente que termina el enfrentamiento que otra persona empezó, arrebatándole así los beneficios y los puntos de experiencia (puntos ganados del en el encuentro que sirven para crecer al personaje).

Juanker: Usado despectivamente contra alguien que se piensa *hacker.* Proviene de la unión de *"juas"* y "*hacker".*

Jabberiano: Se emplea para nombrar a un usuario del servicio de mensajería instantánea abierto XMPP/Jabber.

JcJ: Se usa en juegos de rol *on-line* para activar los modos jugador contra jugador.

Jumi: Se usa en juegos muy *frikis,* y se dice de la persona más imbécil del juego.

K

Kaker: Se utiliza despectivamente para llamar a las personas que dicen ser *hackers,* es el equivalente de *juancker.* Es muy usado en Taringa, debido a un *"hacker"* que decía haber hackeado miles de tarjetas de créditos.

Kick: Se utiliza para expulsiones de un chat especialmente. A diferencia de un *ban,* un *kick* te permite volver a entrar nada más ser expulsado.

Kickear: Proviene de la palabra *Kick,* significa echar a alguien de un chat, una pelea, etc. Se utiliza comúnmente en juegos *on-line.*

KK: Abreviación de *Okok* usada en algunos chats.

KS, del inglés: *Kill stealing.* Usado en los MMORPG para referirse a la gente que termina el enfrentamiento que otra persona empezó, arrebatándole así los beneficios y los puntos de experiencia (puntos ganados del en el encuentro que sirven para crecer al personaje).

Kiter: Aparte de que cuando se bota a alguien de la sala *(kick)*, si en medio de un juego alguien se sale, sin motivo alguno, se le refiere *kiter.*

KMYA, del inglés: *Kiss my ass,* 'besa mi trasero'. Término usado para reflejar poca importancia con respecto a un tema.

KTM: Abreviatura de mentada de madre, 'conche tu madre', usada en el Perú. Usado en los MNORPG.

L

Lag: Dificultad producida por el retraso de una comunicación normalmente ocurrida por fallos en la conexión de Internet. En los videojuegos se tiende a confundir *lag* con *delay. Lag* es cuando la fluidez del movimiento del juego es alterada por fallos en la conexión y eso causa que la animación sea a trompicones y no fluida.

Lamer, del inglés: *Lammer* que significa 'manco', 'sin brazos', en los juegos de FPS *(First Shooter Person)*. Persona de pocas luces (lo contrario de *hacker,* no sabe utilizar la informática) que además hace ostentación de saber. También se utiliza en los juegos *on-line* para denominar a aquellos jugadores que obtienen puntuación matando jugadores indefensos (sin armas), sin conexión o con *lag* y también a aquellos que no saben jugar o novatos. En el juego Warcraft 3 es usado para las personas que atacan la base oponente si estar acompañados por *creeps* manejados por la computadora.

LDT: Acrónimo de 'lejos del teclado'.

Leecher, proviene de la palabra inglesa *Leech:* 'sanguijuela'. Persona que se aprovecha de los recursos de los demás sin aportar nada a cambio, un parásito. Como ejemplos tenemos vincular imágenes de otros servidores sin permiso, o en el caso de los P2P, persona que baja muchas cosas pero comparte muy pocas o ninguna, personas que en juegos *on-line* dejan sus personajes dentro de *partys* estando AFK para así obtener experiencia sin ningún esfuerzo.

Leet /lit/: En un principio l33t o 1337 en ASCII, significa 'élite', persona o grupo muy apto en cuestiones de informática.

LOL: Acrónimo de *Laughing out loud, lots of laughs* o *Laugh out loud,* 'risa a carcajadas'. En otros ámbitos también significa *Lots of love,* 'mucho amor'. También algunas personas piensan que es una palabra de ofensa. En otros casos como una exclamación a algo que te ha parecido extraño parecido al OMG o algo que tendría que hacer gracia y no te ha hecho.

LOLZ: Plural de la palabra y/o expresión **LOL** *(Laughing Out Loud)*.

LMFAO: Acrónimo de *Laughing my fucking ass off, '*partirse el puto culo de risa'. También existe una versión más corta: **LMAO,** *Laughing my ass off*, 'partirse el culo de risa'.

LMPP: Acrónimo de 'lo más pronto posible'.

LMLT: Acrónimo de *Look my last twitt*, 'mira mi último *twitt'*. Es usado para decirle a alguien que ponga atención a tu última actualización en Twitter.

LAT: Acrónimo de *Living apart together,* equivalente a la frase en español 'juntos, pero sin compartir lavadora' o 'juntos, pero no revueltos'.

LAWL: Derivado de *lol* que en inglés se pronuncia como lo leemos en español.

L8er, del inglés: *Later* 'más tarde'.

LPM: Acrónimo de 'La puta madre'.

LPQTRMP: Acrónimo de 'La puta madre que te re mil parió'.

LCTM: Acrónimo de 'La concha de tu madre'.

LRCTM: Acrónimo de 'La re concha de tu madre'.

lB: Acrónimo de 'un beso'. Utilizado para expresar amor o para despedirse (normalmente entre chicas...).

luv: se pronuncia*"lob"* viene de la palabra inglesa *Love* que significa 'amor'. Es una variación de la misma.

LETG: Acrónimo de 'Le echaba tol grumo' (tol = 'todo el'). Frase del sur de Madrid.

LETGELT: Acrónimo de 'Le echaba tol grumo en las tetas'. Frase del sur de Madrid.

M

MANKO: Se denomina así a la persona que no sabe jugar a un juego, es muy común usarlo en juegos (PvP).

MORTI: Abreviación de 'Morticia' (asquerosidad viviente).

MANZA: usado para decirle *"joto"* a alguien.

MADAFAKA: Acrónimo de *Mother fucker,* 'hijo de puta'.

MCTM: Acrónimo de 'Maraco conche tu madre'.

MILF, del inglés: *Mother I'd like to fuck,* 'Madre con la que me gustaría tener sexo'.

MMGB: Acrónimo de 'Mamaguevo', 'Mamá huevo'.

MMORPG: Acrónimo de *Massive Multiplayer On-line Role Playing Game,* 'Juego de rol *on-line* multijugador masivo'.

MQMF: Acrónimo de 'Madre que me follaría'. Equivalente al **MILF.**

MTFBWY: Acrónimo *May the force be with you,* 'que la fuerza te acompañe'.

MTF: Acrónimo de *Mother fucker ,* 'Hijo de puta' o 'hijo de perra'.

MMG: Acrónimo de '*Mamaguevo'*, usado comúnmente en Venezuela y República Dominicana.

MLP: Acrónimo de 'Me la pelas', expresión usada en México.

MP: Acrónimo de *Message private,* 'mensaje privado'.

MSLGR: Acrónimo de 'Se me saltan las lágrimas de la risa' que corresponde a la traducción de **LOL**.

MW: Acrónimo de 'Maricón weon', expresión chilena.

MRD: Acrónimo de 'mierda', expresión de arrepentimiento: "oh!, mierda[mrd]".

MK: 'Marica'.

MVM: Acrónimo de 'Me vale madre', expresión de 'A mí qué me importa' pero un poco más grosera (usada comúnmente en México).

N

ND, del inglés: *Nicely done,* 'bien hecho'. Tiene el mismo significado y uso que "N1".

Newbie //Niubi//: Palabra inglesa destinada para hacer referencia a alguien nuevo en un tema o un ámbito, alguien inexperto.

Newfag: Nuevo en algo (pendejo).

NH, del inglés: *Nice hand* 'buena mano' en juegos de cartas'.

Noob //Nub//: Palabra inglesa con el mismo significado que novato, usado de forma despectiva, para burlarse a alguien que tiene conocimientos inferiores.

NoobBasher: Se refiere a los jugadores con gran grado de experiencia que solo juegan contra jugadores novatos con el fin de obtener una victoria muy fácilmente.

NP: Acrónimo de *No problema, '*no hay problema'.

NPI: Acrónimo de 'Ni puta idea' o 'no poseo información'.

NS: Diminutivo de *Nice*. Se usa para felicitar a un contrincante o compañero por una buena jugada.

NSFW: Acrónimo de *Not safe for work* o 'no seguro para el trabajo'. Hace alusión a que algo posteado en una página de Internet podría meterte en problemas si lo miras desde tu oficina.

NTC: Acrónimo de 'No te creas'.

NTP: Acrónimo de "No te preocupes*'.*

Nuuu...!: Muy usado en tono de gracia cuando algo no sale bien, reemplaza a "Nooo".

NVM, del inglés: *Nevermind,* 'No importa'.

NFS: Acrónimo de: *Not for sale* 'No está a la venta', usado en los MMORPG refiriéndose a que algún objeto que tienes a la vista (equipado) que no está a la venta.

N1, del inglés: *Nice one.* Expresa que has hecho algo bien, es un 'bien hecho'.

Ñuub: Variante léxica de *"noob"* utilizada más comunmente en un ambiente social sin intención de connotaciones negativas.

O

OWNED: Es usado cuando una persona queda humillada públicamente o cuando algo sale mal. También es usado cuando alguien pierde contra un contrincante; él dice "*owned".*

OMC, del inglés: *Oh my science,* 'oh ciencia mía'. Esta frase es más usada por no creyentes.

OMG, del inglés: *Oh my god,* 'oh dios mío', se utiliza cuando algo es sorprendente o impresionante.

OOC: Significa *Out of character*, 'fuera de personaje', usado en juegos de rol para demostrar acciones hechas sin necesidad de "*rolear*".

Orly: Significa: *Oh really?,* 'oh ¿de verdad?'. Ámpliamente utilizado en foros para enfatizar algo que no se cree. Como decir ¿me lo dices en serio?, generalmente es usado sarcásticamente, para denotar falsedad u obvia falacia que normalmente proviene de un *lamer.*

OSOM: Es la pronunciación de la palabra *Awesome*, que significa 'asombroso' o 'impresionante'. La utiliza el luchador de la WWE: The miz en la frase: *"because i'm the miz and i'm OSOM!!".*

OMFG: Significa *Oh my fucking God,* 'Oh mi puto Dios' o *Oh my freaking God, '*Oh mi maldito Dios'.

OMW: Significa *On my way,* 'voy de camino'.

OTP: Significa: *One true pairing,* 'una verdadera vinculación/relación/pareja', los fans de alguna serie u otros la usan para referirse a su pareja favorita de éstas, generalmente colocan los nombres y dicen que es su OTP.

OMGWTFBBQ: Significa *Oh my God what the fuck barbeque*, muy usado en la jerga inglesa, es una combinación entre OMG y WTF, y suele usarse para detonar una sorpresa exacerbada y en cuota de humor. No tiene una traducción exacta.

OMFGMCN: Acrónimo de *Oh my fucking great master Chuck Norris.*

OPD: Significa 'Oh por Dios' en versión latina, por Glanbacheim.

P

P2P: *Peer to peer,* 'comunicación entre pares' que permite la descarga gratuita de programas, imágenes, vídeos y música (se debe tener cuidado con estas descargas, algunas veces pueden estar infectadas con algún virus). O puede ser *Pay to play* que es en los servidores comunmente MMORPG que son pagados.

PAMC: Acrónimo de 'Paja a mano cambiada'.

PJ: Personaje jugable, hace referencia a un jugador en los juegos MMORPG.

PK: *Player Killer,* jugador que se dedica a matar a otros jugadores.

PMS: Usado para *Premenstrual syndrome*. Se usa para hablar de una mujer cuando se comporta muy desagradable.

PnJ: Personaje no jugable (juegos MMORPG).

PnP: Abreviatura de *Plug and Play,* los objetos electrónicos o *hardware* (reproductores de MP3, *pendrives,* joysticks, placas/tarjetas de vídeo/sonido,

etc.) tienen esta función para demostrar que una vez enchufada a una PC, PS2, XBOX, etc. se puede usar en el momento.

PP: *Party pliz*, utilizado en juegos MMORPG, lo utilizan para pedir *party* o invitación a un grupo de jugadores.

PLR: Acrónimo de 'Patá en la raja'('patada en el culo') usado en Chile.

Plz: Abreviación de la palabra en inglés *Please,* 'por favor'.

PPEQLE: 'Puto pendejo el que lea esto' (usado en las salas de chat).

PQD: Significa '¡Pero qué Demonios!' versión latina, por Glanbacheim.

Ps: Abreviación de 'pues', se suele usar mucho al final de una idea.

PSECP: Es la abreviatura de 'Por si estabas con el pendiente'.

PST: Es una abreviatura que se entiende mejor por el sonido. Se usa para llamar la atención de alguien.

PT: Muy utilizado en los MMORPG, se refiere a Grupo, o sea formar un grupo para subir de nivel en equipo. También significa 'Puto'. En argentina significa 'Pete', una forma de insultar a los *low level* en los MMORPG.

PTI: Es la versión en español de **FYI** y vendría a significar 'Para tu información'.

PTM: Muy utilizado en los PnP, se refiere a en castellano a 'Putamare'.

PTP: 'Pico tu padre'.

PvE: Es la abreviatura de *Player versus Enviroment.* (**JcE:** 'Jugador contra entorno'). Se usa en juegos MMORPG.

Pwned: Quiere decir *Powerfuly owned,* o sea, una variación de *Owned,* solo que más "poderoso", por otro lado puede ser un error ortográfico al escribir la palabra, ya que está la "P" junto a la "O".

PvP: Es la abreviatura de *Player versus Player/People versus People* (**JcJ:** 'jugador contra jugador'). Se usa en juegos MMORPG.

S

Scrim: Encuentro formal entre dos clanes, principalmente se da en los FPS.

Spoiler, del inglés: *Spoil* cuyo significado literal es 'estropear(se)', 'echar(se) a perder', etc. Es un BBCode de los foros que oculta parte del contenido de un *post,* haciéndolo visible pulsando un botón. Se suele usar para hablar de argumentos de películas, libros, etc., para no molestar a la gente que todavía no ha visto/leído alguna película o libro.

Smurf: Es cuando un jugador experto se conecta usando una cuenta de novato haciéndole creer a todos que no sabe jugar con el fin de obtener puntos rápidamente en un ranking.

Sk8: *Skate.*

Spam: Correo publicitario no solicitado. En los foros es llamado aquello tópico/post sin sentido, en el cual es el mismo significado que la palabra *"flood".* Proviene del movimiento humorístico masivo de Monthy Phyton en Estados Unidos principalmente, el cual hizo referencia en una de sus actuaciones al *"spice jam"* (mermelada de especias) que se utilizaba masivamente en el Reino Unidos años atrás, por lo que lo exagera pronunciando estas palabras rápidamente hasta formar *SPAM (SPice jAM).*

STFW, del inglés: *Search the fucking web,* en español equivale a 'Busca en la puta web' o 'Busca en la maldita Internet'. Ésta suele ser la respuesta que recibe cualquier pregunta acerca de cómo conseguir algún programa, archivo u otro tipo de información que hubiera sido fácilmente encontrado mediante una búsqueda en Internet usando algún motor de búsqueda como Google o Yahoo!. Al mismo tiempo, también puede indicar (no obligatoriamente) que quien responde se siente ofendido y considera una falta de respeto el hacerle perder su tiempo con una pregunta cuya respuesta es prácticamente obvia y de fácil acceso.

STFU: Viene de la forma vulgar de *Shut Up* y significa *Shut the fuck Up*, algo como 'Cállate de una puta vez'.

Snif...: Sentimiento de tristeza.

Sucker: Se emplea acompañado de algo inicial, y designa a alguien que "apoya" algo que realmente no es bueno, como por ejemplo, *Windows-sucker* sería alguien que apoya Windows maldiciendo. También se puede usar *"Sux",* que sirve para nombrar algo "malo", por ejemplo "maldito *Windows-sux*". Traducido al coloquio español se conocería como "Lameculos".

Seee!: Muy usado en tono de gracia cuando se quiere decir '¡Síii!', por su parecida forma de pronunciar.

SOAB!, del inglés: *Son of a bitch,* significa en español algo como 'Hijo de puta'.

SLCLE: Acrónimo de 'Si la cojo la espachurro', se puede exagerar, diciendo 'Espachiiurrrrro'. También se suele utilizar refiriéndose a la segunda persona, 'Si te cojo te espachurro', es una frase usada al sur de Madrid.

SV: Se usa como abreviación de la palabra servidor.

T

TBM: 'También' (La "m" es reemplazada por la "n").

TGIF, del inglés *Thanks God it's friday,* 'Gracias a Dios es viernes...'.

Tkm: Acrónimo de 'Te kiero mucho', pero que también puede usarse en forma sarcástica para decir 'Te kiero matar'.

Tk: *Team Killer* o 'te kiero'.

Tnx o Thnx: Acrónimo de *Thanks;* en inglés se usa para decir 'gracias'.

TTYS: Significa *Talk to You soon,* 'hablamos pronto'.

TTYL: Significa *Talk to You later*, 'hablamos después'.

TQM: 'Te quiero mucho...'.

TP: 'Tampoco'.

TPM: Acrónimo de 'Tu puta madre'.

TSK: El 'Tsss...'. Como desaprovación o simpatía por algo que se ha dicho.

TT_TT: Una cara que llora.

-_-: Una cara que expresa cuando algo le pareció estúpido.

TTYN, del inglés: *Talk to you never, '*no hablamos más'.

TYVM, del inglés: *Thank you very much,* 'muchas gracias'.

TY, del inglés: *Thank you,* 'gracias'. Se usa para agradecer a la gente en juegos *on-line*.

TQD: 'Te quiero demasiado'.

TPN3: 'Te penetre'.

Troll: Es alguien que se encarga de molestar a la gente en Internet.

U

U: Significa *You* (Tú, Vos, Ustedes).

Uber: Palabra alemana que significa 'superioridad', usado comunmente para marcar las habilidades de una persona/cosa; por ejemplo: "¡Esa persona es *uber!"*.

Ur: Significa *Your*. (Tu, tus, su, sus); *You're* (eres, sos, son).

Ure: Significa *You're* (Eres, sos, son).

V

Ver: Significa *Version,* 'versión', 'edición', etc.

W

WB: Acrónimo de *Welcome Back* 'bienvenido nuevamente'. Generalmente es usado en los chats cuando un usuario se sale y vuelve a entrar en un lapso breve.

WERS: Cuando parece estúpido.

WIP: Acrónimo de: *Web important person,* 'Persona importante en la Red'. Acrónimo de: *Work in progress,* 'Trabajo en proceso'.

WTF: Acrónimo de: *What the fuck.* Exclamación malsonante cuando algo nos sorprende, equivalente al castizo: '¿¡Pero qué carajo/mierda!?', '¿¡Pero qué cojones/coño!?'.

WTFS: Acrónimo de: *What the fucking shit,* '¿¡Qué jodida mierda!?'. Exclamación vulgar o soez cuando algo es pelotudo. Dependiendo de la circunstancia en la que sea utilizada, puede ser o una interrogación o una exclamación. En español significa '¿Qué chucha/mierda/coño es esto?¡.

WTFPWN: De vencer a otro jugador de una manera aplastante, contundente.

WTH: Acrónimo de: *What the hell.* Derivado de **WTF,** equivalente a '¡¿Qué demonios?!'.

WS, del inglés: *Wall Shooting*, haciendo referencia a cuando en juegos MMORPG se ataca a través de muros. Siendo esto un fallo posible de texturas y/o Geodata.

WTB, del inglés: *Want To Buy,* 'quiero comprar', usada en chats de MMORPG para comprar.

WTS, del inglés: *Want to sell, '*quiero vender', usada en chats de MMORPG para vender.

WTT, del inglés: *Want to trade,* 'quiero cambiar', usada en chats de MMORPG para cambiar.

WTD: Acrónimo inglés de: *Want to do,* la traducción literal sería 'quiero hacer', usada en MMORPG, como Voyage Century, para hacer, por ejemplo, una *instance.*

WASD: Letras que corresponden a las flechas direccionales utilizadas en muchos juegos en Internet (W = arriba, A = izquierda, S = abajo, D = derecha) utilizadas por su comodidad para la mayoría de usuarios, que prefieren manipular las flechas direccionales con la mano izquierda.

W8: Acrónimo de *Wait* 'espera'.

WOW: Abreviación del juego en línea World of Warcraft.

WN: Abreviacion de *"Weón"* ('huevón'), usado mayoritariamente en países como Chile, Perú, Venezuela etc.

WYGOWM?: Acrónimo de W*ould you go out with me?,* '¿Quieres salir conmigo?'.

WYSIWYG: Acrónimo de *What you see is what you get*. Usado para describir *software* o diseños que se ven igual en la pantalla como en un medio impreso.

WOF: Acrónimo de *Wait or fuck*. Usado que si alguien no espera que se vaya a la mierda.

X

XVR: Acrónimo de "chévere" en el lenguaje castellano (Latinoamérica) coloquial.

x3: Emoticono que se usa para simular la reacción positiva de alguien al ver algo tierno o lindo.

xD,XD: A pesar de parecer un acrónimo, es un emoticono. Es una pequeña cara cuyos ojos forman una "X" y su boca una "D". Se suele utilizar para expresar risa (PD: No confundir con 'por Dios', esta expresión se escribe en minúsculas la "x" (por) y en mayúscula la "d" (Dios), es decir xD).

XOXO: Besos y abrazos.

xP: Variación de xD, sacar la lengua pero no en modo de burla, signo de complicidad, también se suele poner como ;P

Xploit: Un programa cuyo objetivo es aprovecharse de la vulnerabilidad de otro programa "explotando" ésta, de forma que se consiga un resultado no esperado por el programa víctima, normalmente ejecución de código remoto.

Y

YARLY: "Ya *really"*; utilizado para contestar a la expresión: *Orly?,* 'Sí, de verdad'.

YO: Utilizado por ingleses, significa *Whats up,* '¿Qué pasa?'.

YHBT, del inglés: *You have been trolled,* viene a ser 'te han tomado el pelo'.

YW, del inglés: *You are welcome.* Se utiliza al recibir un agradecimiento. Literalmente 'Eres bienvenido'. En español: 'De nada'.

YNHM: Acrónimo de 'Ya no hablaremos más' utilizado al momento de terminar una relación.

YVJ: 'Ya vio joven'; término utilizado para enunciar una visión.

YT: Acrónimo usado para el nombre dado a la página de Internet YouTube.

Z

ZOMG: Es una variantes del OMG, viene a significar lo mismo, la diferencia es que como el OMG se escribe siempre en mayúsculas pues la gente se confudía al pinchar el *shift* con el dedo y pulsaba la "z", entonces quedaba *"zomg"*, y poco a poco se convirtió en algo igual de usado que el típico OMG, aunque en algunos juegos de terror ZOMG significa *Zombie oh my God.* También se tiene la variante ZOMFG, que viene de la misma idea de pulsar *shift* para escribir OMFG *(Oh my fucking God!).*

DICCIONARIO DE MENSAJERÍA INSTANTÁNEA

A

Acaba: akba
Adiós: a2
Años: aa
Archivo: archvo
Argentina: ARG
Artículo: artclo
Artificial:artfcial
Ataque:ataq
Aterrizar: atrizar

B

Bastante: bstnt
Batería: batry
Beber: bbr
Beso: b
Bien: bn
Brasil: bra
Broma: brma
Bromear: brmar
Botella: botya
Burbuja: brbja

C

Casa: ksa
Cassette: kste
Celebrar: zibrar
Celular: cel
Central: zntral
Centro: zntro

Chat: xat
Chatear: xatr
Chile: chi
Chileno: xilno
Comunícate: cmnkt
Cuál: qal
Cualquiera: qalkera
Cuándo: qndo
Cumpleaños: qmple

D

De: d
Debería: dbria
Decir: dcir
Días: dd
Diccionario: dicnario
Dirección: dir
Domingo:do

E

Ejemplo: ej
Emergencia: emrgencia
Empezar: empzar
Encuentro: enqntro
Entrada: entrda
Escapar: skpar
Esperar: sprar
Estado: stdo
Éste: st
Examen: exam
Excelente: xclnt

F

Favor: fa
Felicidades: flidads
Fiesta: fsta
Final: fin
Firme: firm
Fuerte: frt

G

Generación:gnrcn
General: gral
Generalmente: gral%
Gente: gnt
Gordo: grdo
Gracias: thanx
Grado: gdo
Graduar: grduar
Grande: L

H

Hacer: acer
Hazla: azla
Helado: ala2
Hermano: hno
Hombre:H
Hora:hr

I

Igual: =
Increíble: ncrible

Individual: indval
Información: info
Informal: infrmal
Íntimo: ntimo

J

Jefe: jf
Jueves: ju
Juntos: jnts
Juvenil: jvnil

L

Llámame: yamm
Llave: yav
Lugar: lgr
Lunes: lu

M

Mañana: mñna
Más:+
Mejor: mjr
Mensaje: msj
Menos: -
Mentir: mntir
Meses: mm
Metro: m
Mucho: mxo
M: mujer
M1M: mándame un mensaje luego
MiM: misión imposible
ma: mamá
MK?: ¿me quieres?

msj: mensaje
mto: moto
mv: móvil
mxo: mucho

N

net: Internet
nl: en el/en la
NLC: no lo conozco
NLS: no lo sé
nos: nosotros
NPH: no puedo hablar
NPN: no pasa nada
NSN: no se nada
nsti: insti/instituto
NT1P: no tengo un peso
NV: nos vemos
NVA: nos vemos allí
n: no

Ñ

ñ: año

P

Pa: papá
Pco: poco
PDT: paso de ti/¡piérdete!
PF: por favor
x fa: porfa / por favor
pkñ: pequeño
pls: por favor
pqñ: pequeño

prf: profesor
pscna: piscina
pso: paso
pdo: borrachera
pq: porque

Q

q: que
qirsir?: ¿quieres ir?
q tal?: ¿qué tal?
q tpsa?: ¿qué te pasa?
QT1BD: que tengas un buen día

R

R: responde
rmno: hermano
rptlo: repítelo/no te entiendo

S

s q: es que
s s q: si es que...
salu2: saludos
sbdo: sábado
sbs?: ¿sabés?
slmos?: ¿salimos?
SMS: mensaje corto
spro: espero
srt!: ¡suerte!
ss cl cl: sí, sí, claro, claro
STLD / S2LD: si tú lo dices...

T

t @: te mando un *mail*
t O: te odio
tas OK?: ¿estás bien?
tb: también
tbj: trabajo
TVL: te veo luego
TKI: tengo que irme
tjt: tarjeta
tl: teléfono
tv: televisión
tng: tengo
t q: te quiero
trd: tarde
TQITPP: te quiero y te pido perdón
TQPSA: te quería pero se acabó

U

U: tú
vac: vacaciones
vns?: ¿vienes?
vos: vosotros
vrns: viernes

W

wpa: ¡guapa!

X

x: por
xa: para

xam: examen
xat: chat
xdon: perdón
xk?: ¿por qué?
xka: chica
xko: chico
xo: pero
xq: porque
xx: chica
xy: chico

Y

ymam: llámame

Z

Zzz: me duermo...

DICCIONARIO DE EMOTICONOS

:) Sonrisa
:-)) Muy feliz
:-) Contento
:-(Triste/enojado
:-c Un poco más triste
:-C Triste del todo
:-((Muy triste
(:-(Muy triste
:-S Confundido
:-o zzzzZZ Aburrido
:-e Decepcionado
:-| Serio
:-? Dubitativo
:-o Sorprendido / oh! no!
:-() Sorprendido
:-O Muy sorprendido / Asustado
:') Emocionado
:.) Emocionado
(:-... Tus palabras me emocionan
:-/ Escéptico / Perplejo
:-0 Impresionado
:-t Estoy de mal humor
:-c Soy muy infeliz
:-C Realmente asustado

%+(Apaleado, acabado
:-e Decepcionado
:-I Indiferente
;-) Cómplice
>;-> Cómplice
:-)~~ Baboso
:-T Serio
:- Indeciso/ Dudoso
:-0 Conversador
(:-D Charlatán
:-> Sarcástico
>:-> Diabólico
:-& Con la lengua trabada
:-/ Escéptico
q:-) Canchero
X-(Muerto
-<:-) Loco de remate
<:-) De fiesta
X-) Tímido
:-1 Cara dura
:-! Cara dura
:-II Furioso
>-< Furioso
|-I Dormido
|-(Tengo sueño
|-) Estoy durmiendo
:-7 Sonrisa maliciosa
:ŽŽŽŽ-(Mares de lágrimas
:-)))) Riéndose a carcajadas
X-D Partiéndose de risa.
:-DDD Riendo mucho
:-D Riendo
:*(Llorando
:'-(Llorando
:`-(Llorando
:'''-(Llorando mucho, mucho
:-@! Diciendo malas palabras
:-@ Gritando
:-V Gritando

;-) Guiñando un ojo
I-O Bostezando
:-Þ Sacando la lengua
:-Q Usuario es un fumador
:-i Fumando
:-? Fumando en pipa
:'(Llorando de pena
:.(Llorando de pena
:-)" Babeando
:-)_ Babeando
:-)' Babeando
:-9 Me humedezco los labios
:-} Miro maliciosamente
:*) Estoy resfriado
:-^) Estoy resfriado
R-) Se me rompieron los lentes
|-{ Gran pena
%+(Estampado contra la pared
:-(No me gusto la última frase
>:-> Comentario diabólico
B:-) Los lentes en la cabeza
:-* Usuario comió algo agrio
:'-) Llorando de felicidad
:-& La lengua atada (no puedo hablar)
:-S Usuario está diciendo incoherencias
:-` Escupiendo
:-" Silbando
(-) Necesito un peluquero
|-(Perdí las lentes
;[ ] Tengo hambre
:-)> Barbudo
(:I El usuario es calvo
#8^0-|-< Cuerpo completo
{:-) Raya al medio
:-{} Usuaria tiene la boca pintada
.-) Tuerto
(:I Usuario tiene cabeza de huevo
:-(#) Con ortodoncia
:-)> Con barba

C|:-) Llevo sombrero
:) Usuario tiene la nariz rota
:^) Nariz rota
X-) Ligero estrabismo
&:-) Con el cabello enrulado
:^{ Bigotudo
:-{)= Sonriente con bigotes y barba
:-{) Sonriente con bigotes
|-) Ojos cerrados
[:-) Con *walkman*
%-) Después de 8h frente al monitor
@:-} Recién salido de la peluquería
:-}X Vestido con moño o pajarita
B-) Con lentes (oscuros)
8-) Con lentes (de contacto)
]-) Con lentes de sol
{:-) Con peluca
~:-P Con un solo pelo
:-{} Labios gruesos
:-# Labios sellados
:-” Labios fruncidos
?-(Ojo morado
(:-) Cara grande
(-: Zurdo
|:-) Con las cejas unidas
:-3) Con bigotes
:-#) Con bigote
:-{) Con bigotes
:-(=) Dientudo
}:^) Narigón
H-) Bizco
:-E Dientes de vampiro
I:-) Cejas pobladas
8-O Oh, my God!
:-C Increíble
(:>-< Dice un ladrón: Manos arriba!
@>--->--- Una rosa
@-}--- Una flor
:-X Soy/eres una tumba

:-# Le taparon la boca
:-X Enviar un beso
:-* Beso
[] Abrazos
[]'s Abrazos
3:[Bebe al que nadie le hace caso
3:] Bebé sonriendo.
:-)^< Chico grande
:-)8< Chica grande
8:-) Usuario es una niña
8) Rana
8)~~* Rana atrapando una mosca
{:v Pato
3:-) Vaca
:8) Cerdo
:=) Orangután
<:3)--- Ratón (horizontal)
:= | Mono
<:>== Pavo
~===| Vela
~0)| Taza de café
<3 Corazón
<===~~ Cohete
o.....!!!!! *Bowling* (horizontal)
=^..^= Gato (horizontal)
@>--->---| Rosa
=';'= Perrito
<|-) Soy chino
/:-) Soy francés
O:-) Ángel, Inocente
d:-) Jugador de béisbol con gorra
8(:-) Mickey Mouse
C=:-) Chef
=|:-)= Tío Sam
***:O)** Payaso
+:-) Sacerdote
P-(Pirata
**-=#:-) ** Hada con la varita mágica
5:-) Elvis Presley

@@@@:-) Marge Simpson
(_8(|) Homero Simpson
@:-) Musulmán con turbante
?:^[] Jim Carrey
(8 { John Lennon
:---) Pinocho
+<:-) El Papa
+<:-) Borracho
:*) Borracho
:-[Vampiro
%-) Borracho feliz
***<|:-)** Papá Noel
([(Robocop
}:-) Diablillo
El invisible
=:-(Punk enojado
=:-) Punk
:-: El Mutante
[:] Robot
O-) Cíclope
';' Sorprendido (horizontal)

DICCIONARIO DE TÉRMINOS RELACIONADO CON LOS DELITOS INFORMÁTICOS

A

Adware: Es un *software* que muestra anuncios (viene del inglés, *ad* 'anuncio', *software* 'programa'). Los *adware* se instalan generalmente sin que nosotros lo deseemos, puesto que nadie suele desear que le machaquen con publicidad constantemente.

B

Botnets: Asociación en red *(nets)* de máquinas autónomas (robots) que forman un grupo de equipos que ejecutan una aplicación controlada y manipulada por el artífice del *botnet,* que controla todos los ordenadores/servidores infectados de forma remota y que pueden emplearse para robar datos o apagar un sistema.

Blog (abreviación de *weblog*): Página web que contiene una serie de textos o artículos escritos por uno o más autores recopilados cronológicamente. Normalmente el más actual se coloca en primer plano. Su temática es muy variada. Abundan muchísimo los blogs personales, pero también podemos encontrar otros en formato periodístico. Lo que está claro es que es un modo de comunicarse que está generando diarios en masa. A fecha de hoy los gigantes de Internet se han subido al carro y están aprovechando el tirón para atraer más tráfico hacia sus sitios.

***Bulling* o acoso escolar:** *Bulling* significa en inglés 'maltrato e intimidación entre iguales'. Es el maltrato físico y/o psicológico deliberado y conti-

nuado que recibe un niño por parte de otro u otros en el ámbito escolar, que se comportan con él cruelmente con el objetivo de someterlo y asustarlo. El *bullying* implica una repetición continuada de las burlas o las agresiones y puede provocar la exclusión social de la víctima.

C

Carding: Consiste en la obtención de los números secretos de la tarjeta de crédito, a través de técnicas de *phishing,* para realizar compras a través Internet.

Ciberbullying: estamos ante un caso de *ciberbullying* cuando un o una menor atormenta, amenaza, hostiga, humilla o molesta a otro/a mediante Internet, teléfonos móviles, consolas de juegos u otras tecnologías telemáticas.

Cracker: Es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un *hacker,* solo que a diferencia de este último, el *cracker* realiza la intrusión con fines de beneficio personal o para hacer daño.

***Child Grooming* o acoso infantil a través de la Red:** Acción encaminada a establecer una relación y control emocional sobre un niño/a, cuya finalidad última es la de abusar sexualmente del/la menor. Se lleva a cabo mediante el engaño de una persona adulta a un menor a través de programas de conversación tipo Messenger para obtener imágenes de contenido erótico del menor que después utilizará para coaccionarle, bajo amenaza de difundir esas imágenes a sus conocidos y conseguir así más imágenes o incluso llegar materializar el abuso.

F

Foros: Son una especie de "tablones de anuncios", donde los miembros del mismo pueden escribir mensajes para que los vean todos los integrantes, a la vez que pueden ver y responder los mensajes enviados por los demás. Para que la información quede ordenada se pueden abrir distintos temas o categorías para agrupar los mensajes sobre un tema concreto.

G

Grooming: Es un nuevo tipo de problema relativo a la seguridad de los menores en Internet, consistente en acciones deliberadas por parte de un/a adulto/a de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente por medio de abusos.

Gusano (también llamados ***IWorm*** por su apocope en inglés, *I* 'Internet', *Worm* 'gusano'): Es un *malware* que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la Red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

H

Hacker: Persona que posee elevados conocimientos de sistemas y seguridad informática, son considerados expertos en una cierta materia, normalmente relacionada con la informática (redes, seguridad informática, criptoanálisis, inteligencia artificial...).

Hoax, del inglés: 'engaño' o 'bulo': Se trata de bulos e historias inventadas, que no son más que eso, mentiras solapadas en narraciones cuyo fin último es destapar el interés del lector o destinatario. Dichas comunicaciones pueden tener como finalidad última: conseguir dinero o propagar un virus.

K

Keylogger: Programa o dispositivo que registra las combinaciones de teclas pulsadas por los usuarios y las almacena para obtener datos confidenciales como contraseñas, contenido de mensajes de correo, etc. La información almacenada se suele publicar o enviar por Internet.

M

Malware: El término *malware* (acrónimo en inglés de: *Malcious software)* engloba a todos aquellos programas "maliciosos" (troyanos, virus, gusanos, etc.) que pretenden obtener un determinado beneficio, causando algún tipo de perjuicio al sistema informático o al usuario del mismo.

Moobing: Situación en que una persona o grupo de personas ejercen una violencia psicológica extrema, de forma sistemática, durante un tiempo prolongado sobre otra persona en el lugar de trabajo.

P

Pederastia: Según la Real Academia Española se define como el "Abuso cometido con niños". El término "abuso" significa cualquier uso excesivo del propio derecho que lesiona el derecho ajeno, en tanto que agresión significa acometimiento, ataque; mientras que en el abuso la violencia o intimidación no parece significativa del concepto, en la agresión es inequívoca. La consumación del delito de abuso se produce tan pronto se materialice el tocamiento íntimo o la conducta de que se trate, aunque el sujeto activo no alcance la satisfacción buscada.

Pedofilia: "Atracción erótica o sexual que una persona adulta siente hacia niños o adolescente", sin que llegue a consumarse el abuso.

Pharming: Manipulación de la resolución de nombres de dominio producido por un código malicioso, normalmente en forma de troyano, que se nos ha introducido en el ordenador mientras realizábamos una descarga y que permite que el usuario cuando introduce la dirección de una página web, se le conduzca en realidad a otra falsa, que simula ser la deseada. Con esta técnica se intenta obtener información confidencial de los usuarios, desde números de tarjetas de crédito hasta contraseñas. De manera que si el usuario accede a la web de su banco para realizar operaciones bancarias, en realidad accede a una web que simula ser la del banco, casi a la perfección, logrando los delincuentes, obtener los códigos secretos del usuario, pudiendo materializar el fraude con los mismos.

Phishing: Es la contracción de *password harvesting fishing,* 'cosecha y pesca de contraseñas'. Las técnicas denominadas *phishing* consisten en el envío de correos electrónicos, en los cuales el usuario cree que el remitente se trata de una entidad reconocida y seria (usualmente bancos), en los que

se solicita al mismo que por unos u otros motivos debe actualizar o verificar sus datos de cliente a través, normalmente, de un enlace a una página que simula ser de la entidad suplantada. Una vez el usuario remite sus datos, los delincuentes o estafadores pueden proceder a operar con los mismos.

Pornografía infantil: Se define como "toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño, con fines primordialmente sexuales". Comprende las siguientes actuaciones:

Utilizar menores de edad con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados o financiación de esta actividad. ***(art. 189.1.a del Código Penal)***

Utilizar menores de edad para elaborar cualquier clase de material pornográfico o financiar esta actividad. ***(189.1. a)***

R

Redes sociales: Una red social es una estructura social en donde hay individuos que se encuentran relacionados entre sí. Las relaciones pueden ser de distinto tipo, como intercambios financieros, amistad, relaciones sexuales, entre otros. Se usa también como medio para la interacción entre diferentes como chats, foros, juegos en línea, blogs, etc.

Re-mailer: Servicio de Internet que, utilizando distintas técnicas, oculta la identidad del remitente de un correo electrónico.

Rootkit: Es una herramienta, o un grupo de ellas, que tiene como finalidad esconderse a sí misma y esconder a otros programas, procesos, archivos, directorios, llaves de registro y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible, a menudo con fines maliciosos o destructivos.

S

Spyware: Es un *software* que recopila información de un ordenador y después transmite esta información a una entidad externa, sin el conocimiento o el consentimiento del propietario del ordenador.

***Scam* o *phishing* laboral:** Fraude similar al *phishing*, con el que comparte el objetivo de obtener datos confidenciales de usuarios, para acceder a sus cuentas bancarias. Consiste en el envío masivo de correos electrónicos o la publicación de anuncios en webs, en los que se ofrecen supuestos empleos muy bien remunerados. Cuando el usuario acepta la oferta de trabajo, se le solicita que facilite datos de sus cuentas bancarias, a través de un *e-mail* o accediendo a una web, para ingresarle los supuestos beneficios.

SMiShing: Es una variante del *phishing,* que utiliza los mensajes a teléfonos móviles, en lugar de los correos electrónicos, para realizar el ataque. El resto del procedimiento es igual al del *phishing:* el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falseada, idéntica a la de la entidad en cuestión.

***Spam* o "correo basura":** Todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo se entiende por *spam* cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico. Quienes se dedican a esta actividad reciben el nombre de *spammers.*

Spammer: La persona o compañía que realiza el envío de *spam.*

Spamming lists: Listas comerciales. Listas de direcciones de correo para envío de publicidad de forma masiva.

Spear Phishing: Tipo de *phishing* en el que, en lugar de realizar un envío masivo de correos electrónicos, se envían correos con mayor grado de personalización, a destinatarios concretos, consiguiendo que los mensajes resulten más creíbles que los del *phishing* tradicional.

Spoofing: Hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Tipos:

- **IP *Spoofing:*** suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
- **ARP *Spoofing:*** suplantación de identidad por falsificación de tabla ARP. (ARP son las siglas en inglés de Address Resolution Protocol (protocolo de resolución de direcciones)).

- **DNS *Spoofing:*** Suplantación de identidad por nombre de dominio
- **Web *Spoofing:*** suplantación de una página web real.
- ***Mail Spoofing:*** Suplantación en correo electrónico de la dirección *e-mail* de otras personas o entidades.

Tráfico de menores con fines de explotación sexual: la conducta consiste en favorecer la entrada, estancia o salida del territorio nacional de personas menores de edad con el propósito de su explotación sexual empleando violencia, intimidación o engaño, o abusando de una situación de superioridad o de necesidad o vulnerabilidad de la víctima o para iniciarla o mantenerla en una situación de prostitución. *(188.4 en relación con el 188.2)*

T

Tramas de *"pumd and dump":* En las que los delincuentes acceden a las cuentas de muchos clientes y las utilizan para alzar de forma artificial el precio de acciones modestas y venderlas desde sus propias cuentas.

Troyano (o caballo de Troya, traducción literal del inglés *Trojan horse*): Programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.

V

Virus informático: Es un *malware* que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de éste. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos. Los virus informáticos tienen, básicamente, la función de propagarse, no se replican a sí mismos porque no tienen esa facultad como el gusano informático, depende de un *software* para propagarse, son muy dañinos y algunos contienen además una carga dañina *(payload)* con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas o bloquear las redes informáticas generando tráfico inútil.

Vishing: Fraude que persigue el mismo fin que el *phishing,* la obtención de datos confidenciales de usuarios, pero a través de un medio distinto: la telefonía IP. Los ataques de *vishing* se suelen producir siguiendo dos esquemas:

- Envío de correos electrónicos, en los que se alerta a los usuarios sobre algún tema relacionado con sus cuentas bancarias, con el fin de que éstos llamen al número de teléfono gratuito que se les facilita.

- Utilización de un programa que realice llamadas automáticas a números de teléfono de una zona determinada.

En ambos casos, cuando se logra contactar telefónicamente con el usuario, un mensaje automático le solicita el número de cuenta, contraseña, código de seguridad, etc.

W

Web bug: También se denominan "microespías" o "pulgas" y son imágenes transparentes dentro de una página web o dentro de un correo electrónico con un tamaño de 1×1 pixeles. Al igual que ocurre con las *cookies,* se utilizan para obtener información acerca de los lectores de esas páginas o los usuarios de los correos, tales como la dirección IP de su ordenador, el tipo y versión de navegador del internauta, el sistema operativo, idioma, cuanta gente ha leído el correo, etc.

Web 2.0: El término Web 2.0 fue acuñado por Tim O'Reilly en 2004 para referirse a una segunda generación en la historia de la Web basada en comunidades de usuarios y una gama especial de servicios, como las redes sociales, los blogs, los wikis o las folcsonomías, que fomentan la colaboración y el intercambio ágil de información entre los usuarios.

DESPEDIDA Y CIERRE

Y hasta aquí este libro. ¿Entendéis ahora el título *X1Red+Segura: Informando y Educando V1.0?* Espero que este pequeño aporte haya conseguido haceros llegar el sentimiento de que cualquier internauta puede disfrutar de Internet de forma más o menos segura, simplemente adoptando unas medidas básicas de seguridad y teniendo conciencia de los peligros que nos acechan en la Red. No tenemos por qué ser expertos informáticos, **Internet no es informática, es información, es la vida real presentada en un mundo virtual.**

Hasta ahora afrontabais la vida de forma analógica y aprendíais con los métodos más tradicionales.

La brecha digital ya no debe de ser un obstáculo para vosotros y si tenéis en cuenta lo que se ha intentado transmitir en este libro, ya podéis consideraros preparados para afrontar vuestra nueva "cibervida" digital y disfrutar de tener el mundo a vuestros pies a un simple *click* de ratón.

Simplemente recordad que en Internet...

Nosotros mismos somos nuestra peor vulnerabilidad pero también somos nuestro mejor antivirus.

Y sobre todo que…

Informando y Educando podemos conseguir una Red más segura.

¡Ahora os toca a vosotros difundir el mensaje!

Nos vemos en la Red

X1Red+Segura

BIBLIOGRAFÍA

Como ya habréis comprobado *X1Red+Segura: Informando y Educando v1.0* no es un libro convencional y por lo tanto las fuentes de información del mismo tampoco son las convencionales.

Todo ha evolucionado con Internet, notablemente las formas de informarse.

Para la realización de este libro ha sido primordial la obtención de información en la Red, las consultas al "oráculo", las informaciones de Google.

Estas consultas a la Red han llevado a fuentes de información dispersas en "la nube" en general y en páginas web en particular que se relacionan a continuación:

http://www.aliados.org

http://www.anexom.es

Blog de e-Legales

http://www.cad.com.mx

http://www.cibermanagers.com

http://www.deciencias.net

http://www.delitosinformaticos.com

http://www.elcorreo.es

http://www.elladodelmal.com

http://www.enocasionesveoreos.blogspot.com

http://www.emezeta.com

http://www.wikionary.org

http://www.eset.es

http://www.esklatsocial.blogsopot.com.es

http://www.gdt.guardiacivil.es

http://www.google.es

http://www.ideal.es

http://www.infobae.com

http://www.inteco.es

http://www.kuaest.com

http://www.laopinion.es

http://www.maestrosdelweb.com

http://www.masadelante.com

http://www.mastermagazine.info

http://www.microsiervos.com

http://www.noticiasjuridicas.com

http://www.osi.es

http://www.pantallasamigas.net

http://www.protegeles.es

http://www.tallertic.netau.net

http://www.tectonilogia.com

http://www.vinagreasesino.com

http://www.web.archive.org

http://www.wikipedia.org

http://www.wordreference.com

Internet en general

Y por supuesto la información que proviene de los GRANDES *(ellos se reconocerán)* y que en este libro se ha pretendido "traducir".

X1Red+Segura – Informando y Educando

V1.0

"Internet no es informática, es información, es la vida real presentada en un mundo virtual."

"Ningún internauta está exento de los peligros de la red y menos si no pone los mínimos medios de protección para evitarlos. La primera medida básica de combatir los peligros de la Red es conocerlos, conocer su origen, conocer su funcionamiento, saber su existencia y cómo actúan sus responsables."

Este libro pretende ser una guía en la que se presenta al lector, menos técnico, qué es Internet desde sus comienzos hasta nuestros días. Se presenta de forma detallada y sencilla explicando su funcionamiento y los servicios que nos ofrece, con el fin de que pueda ser accesible a los usuarios internautas más básicos en cuanto a conocimientos técnicos informáticos.

Igualmente, una vez detallados los conceptos básicos de Internet y los servicios que ofrece, se presentan los peligros actuales a los que nos podemos enfrentar en la Red de redes, con ello conoceremos su origen, su forma de actuar, quién los dirige y hacia qué objetivos. Gracias a este análisis aprenderemos a identificarlos en sus distintas formas y "presentaciones" y por consiguiente sabremos defendernos y evitarlos.

Una guía en la que aparecen la inmensa mayoría de las entradas disponibles en "*El Blog de Angelucho*", artículos, alertas y ciberconsejos, relativos todos a la seguridad en la Red y dirigidos a todos los internautas, aunque el objetivo principal es el navegante menos experimentado y por lo tanto con más posibilidades de convertirse en "cibervíctima".

Ni que decir tiene que, aunque los lectores de estos contenidos son mayoritariamente internautas adultos, el principal objetivo a proteger son los navegantes más jóvenes, niños y adolescentes, al ser los más desprotegidos en la Red por desconocimiento de los peligros que les amenazan en muchos de los casos, pero en la mayoría de las ocasiones el problema se da por una considerable ausencia del denominado "Control Parental".

Patrocinado por:

GDT GRUPO DE DELITOS TELEMÁTICOS

blueliv

buguroo offensive security

/Rooted

SmartHC

Revista SIC ciberseguridad, seguridad de la información y privacidad

Akamai