Delito.com

Algunas notas de la delincuencia *online*

COLECTIVO ARCION

Surge en el año 2008, equipo interdisciplinario de investigadores en el campo de lo Criminológico-criminalístico, su actividad científica coadyuva al desarrollo y consolidación del modelo educativo CLEU. "Investigar para la libertad". Representa su filosofía de batalla.

RESUMEN

Es evidente el constante desarrollo experimentado en las filas de la delincuencia, pues en éstas se han generado modalidades delictivas otrora inconcebibles. Sin lugar a dudas, internet, la informática y la programación han sido explotadas por los delincuentes en su provecho dándole el espacio necesario al establecimiento de la delincuencia *online* (*ciberdelincuencia*), orillando tanto a los cuerpos y aparatos de administración y procuración de justicia, especialistas en la materia, así como de los individuos en común a hacerle frente a esta latente amenaza en línea. Pero antes de dar marcha a cualquier acción de respuesta es necesario estar al tanto de las herramientas, medios y técnicas que los agresores han sabido hacer uso, pues es de esta manera como se tendrán los conocimientos pertinentes en cuanto a la amenaza a la que se enfrenta. Por esto el presente trabajo pone de manifiesto a los lectores algunos rasgos significativos de esta forma de delinquir.

> "Al unísono en que se desarrolla una nueva tecnología es casi probable que se esté desarrollando una paralela con fines delictivos."

INTRODUCCIÓN

Internet[1] ha proporcionado en nuestros días nuevas formas de interactuar entre las personas dando lugar a espacios virtuales de encuentro y en estos la frecuente e intensa compartición y transferencia de datos e información. Una imagen, un comentario, un *link*[2] compartido o quizás un archivo de cualquier naturaleza, son en definitiva datos e información.

Tal información y datos pueden ser o no de carácter restringido, pues depende de la importancia y valor que pueda poseer para quién la emite, porque de alguna manera esa realidad virtual tiene implicaciones en la realidad como tal, es decir, que todo ese cúmulo de archivos que trafican en un ir y venir por las 'autopistas' del ciberespacio tienen efectos directos y proporcionales en la vida y realidad de los individuos, junto a las implicaciones que en ésta se generen.

1 Es un sistema global interconectado de redes de computadoras para servir a miles de millones de usuarios en todo el mundo. Se trata de una red de redes que consiste en millones de éstas de tipo privado, público, académico, empresarial y de gobierno de alcance local a global que están unidos por una amplia gama de tecnologías de redes electrónicas, inalámbricas y ópticas.

2 Un hipervínculo (también llamado enlace, vínculo, o hiperenlace) es un elemento de un documento electrónico que hace referencia a otro recurso.

Por lo anterior, de modo alguno encontraríamos que existe un vínculo de cierta medida de nuestra realidad reflejada en el ciberespacio, todo esto debido a la cada vez más creciente comunidad de usuarios de internet –que en provecho de los beneficios de este medio- han optado por su incorporación en el uso de la red informática como una forma de asociarse a ese 'mundo', a sus 'habitantes', a sus 'espacios' y como ya se infirió a sus ventajas como medio de comunicación.

Delincuencia *online*

Tomando en cuenta lo expuesto en los párrafos anteriores es conveniente señalar que buena parte de las actividades sociales y demás que se llevan a cabo en nuestra realidad pueden ser realizadas vía internet: desde enviar un saludo a un amigo y que éste responda dentro de un *chat room*[3] hasta realizar conexiones a través de Red Privada Virtual[4] (VPN por sus siglas en inglés) para la práctica de una cirugía a distancia, pasando por las innumerables transferencias bancarias electrónicas, así facilitando estas operaciones sin sacar físicamente el dinero. Pero a pesar de todas estas ventajas que nos ofrece este medio sería aceptable cuestionarse qué tan seguro es transitar por estas 'autopistas' y si no lo son, qué riesgos se pueden encontrar en el 'camino'. Sólo el hipotético escenario en que una mala conexión exista en una telecirugía supondría un riesgo de alto alcance.

Internet ha proporcionado indiscutiblemente beneficios a la sociedad, sin embargo, a su vez ha traído consigo peligros en los que se puede caer en nuestra 'navegación' por la red, muchos de ellos no son tan sólo errores técnicos o humanos, sino también los hay intencionales. Es bien sabido que en esta comunidad –la virtual como suele llamársele- de usuarios de internet existen quienes sacan partida de esta interacción no presencial para poner en práctica -por diversas razones principalmente las de lucro- sus conocimientos en informática y programación al servicio de la delincuencia para atentar en contra de la seguridad y confidencialidad de los demás miembros de esa comunidad. Desde luego que estaríamos hablando de personas, organizaciones e instituciones de las más diversas índoles hasta naciones como víctimas y por su parte a este usuario mal intencionado como victimario, pues irrumpe en los recursos informáticos ajenos.

Todos estos miembros de la red pueden ser víctimas de estos 'delincuentes informáticos', pero al igual como sucede en la vida tal cual: los más vulnerables en estas embestidas son las personas o individuos comunes.

Algunos de los espacios virtuales de los que se ha servido esta modalidad de la delincuencia son las redes sociales, pues su acelerada y cada vez creciente afiliación de nuevos miembros[5] hacen de éstas un amplio repertorio de posibles víctimas de sus fechorías, además que en esto espacios es posible encontrar una gran cantidad de datos e información de utilidad para el delincuente, ya que en ella se pueden describir los gustos, preferencias, condiciones socioeconómicas, 'movimientos' y otras particularidades de un miembro en específico que pueda resultar atractivo.

Es necesario establecer qué es lo que hace de las redes sociales sitios encantadores y propicios para que el delincuente actúe. Aunque una cuenta en estos dominios pueda contener información no fiable –llamémosle chatarra-, cabe la posibilidad que en medio de toda esa falaz 'ficha técnica'del afiliado exista datos a manera de indicios que nos acerque un poco a éste –como analogía tomemos el ejemplo cuando se hurga en medio de la basura para conocer un poco más al objetivo- en cambio, existe otro tipo de afiliado más 'transparente' que en diferente magnitud se muestra tal como es.

TABLA 1
EVOLUCIÓN DE NÚMERO DE USUARIOS ACTIVOS DE *FACEBOOK*

Año	Usuarios activos en millones
2004	Nace Facebook 1
2005	5.5
2006	12
2007	50
2008	100
2009	350
2010	500
2011	750

Fuente: http://facebook.com/press

TABLA 2
REDES SOCIALES MÁS POPULARES EN MÉXICO

Porcentaje de usuarios mexicanos	Red Social
39%	Facebook
28%	You Tube
20%	Twitter
6%	Hi5

3 Cualquier forma de conferencias sincrónicas y en ocasiones asincrónicas. El uso principal de una sala de chat es el de compartir información a través de texto con un grupo de otros usuarios. En términos generales es la capacidad de conversar con varias personas en la misma conversación. La diferencia de las salas de chat de los programas de mensajería instantánea, es que los últimos son típicamente diseñados para uno-a-uno.

4 "Red Privada Virtual". Wikipedia la enciclopedia libre. [consultado: 23 de enero de 2012].

5 Facebook. "Biografía", [en línea]. 2012, [consultado: 23 de enero de 2012]. Disponible en la Web: http://www.facebook.com/press/info.php?timeline De acuerdo a la cifra presentada por el portal de Facebook es cercana a las 750 millones de cuentas de usuarios activos en julio de 2011.

3%	Badoo
2%	Sonico
1%	MySpace
1%	Linkendln

Fuente: Diario Milenio. Corona, Jessica. 'Facebook es la red social más usada por los mexicanos; Twitter, la tercera'. 17 mayo 2011, [consultado: 23 de enero de 2012]. Disponible en la web: http://www.milenio.com/cdb/doc/noticias2011/58c0b884bd6410700b50e014116375b1

TABLA 3
SUSCRIPCIONES DE INTERNET (TOTALES) POR CADA 100 HABITANTES. SERIE ANUAL

Año	Suscripciones por Cada 100 Habitantes
2000	1.1
2001	1.9
2002	2.1
2003	2.4
2004	3.0
2005	3.7
2006	4.6
2007	5.5
2008	7.7
2009p/	9.4
2010p/	10.8

Fuente: Comisión Federal de Telecomunicaciones (COFETEL), Secretaría de Comunicaciones y Transportes. 'Suscripciones de Internet (totales) por cada 100 habitantes. Serie Anual', [en línea]. 2010, [consultado: 23 de enero de 2012]. Disponible en la web: http://siemt.cft.gob.mx/SIEM/#!prettyPhoto/84/

TABLA 4
COMPARATIVO INTERNACIONAL DE SUSCRIPCIONES DE INTERNET DE BANDA ANCHA POR CADA 100 HABITANTES. SERIE ANUAL

País	2008	2009 p/	2010 p/
Alemania	27.49	30.31	31.59
Argentina	8.02	8.67	9.56
Australia	23.94	23.25	23.19
Austria	20.73	22.06	23.85
Brasil	5.37	6.09	7.23
Canadá	29.53	30.51	29.81
Chile	8.5	9.76	10.45
China	6.24	7.79	9.42
Colombia	3.27	4.43	5.66
Corea del sur	33.35	35.03	36.63
Dinamarca	36.48	37.18	37.38
España	20.06	21.27	22.96
Estados Unidos	24.82	26.23	26.34
Finlandia	30.43	29.31	29.07
Francia	28.71	31.76	33.92
Irlanda	20.29	21.8	22.82
Islandia	33.38	33.93	34.65
Italia	18.84	20.42	22.13
Japón	23.8	25.01	26.91
Malasia	4.79	5.98	7.32
México	7.07	9.05	10.54
Noruega	33.19	33.87	34.6
Nueva Zelanda	21.39	22.69	24.93
Perú	2.55	2.81	3.14
Reino unido	28.19	30.4	31.38
Rusia	6.48	9.02	10.98
Singapur	22.45	23.67	24.72
Suecia	31.43	31.63	31.59
Uruguay	6.8	8.96	11.37
Venezuela	4.74	4.72	5.37

Fuente: Comisión Federal de Telecomunicaciones (COFETEL), Secretaría de Comunicaciones y Transportes. 'Comparativo Internacional de suscripciones de Internet de Banda Ancha por cada 100 habitantes. Serie Anual', [en línea]. 2010, [consultado: 23 de enero de 2012]. Disponible en la web: http://siemt.cft.gob.mx/SIEM/#!prettyPhoto/91/

Como menciona este trabajo al iniciar: una imagen, un comentario, un *link* compartido o archivo cualquiera puede decir o contener mucho o poco, pero el caso es que si se pone atención a esos 'movimientos informáticos hablan más' que de la razones por los que fueron concebidos por el cibernauta que las emitió y usó.

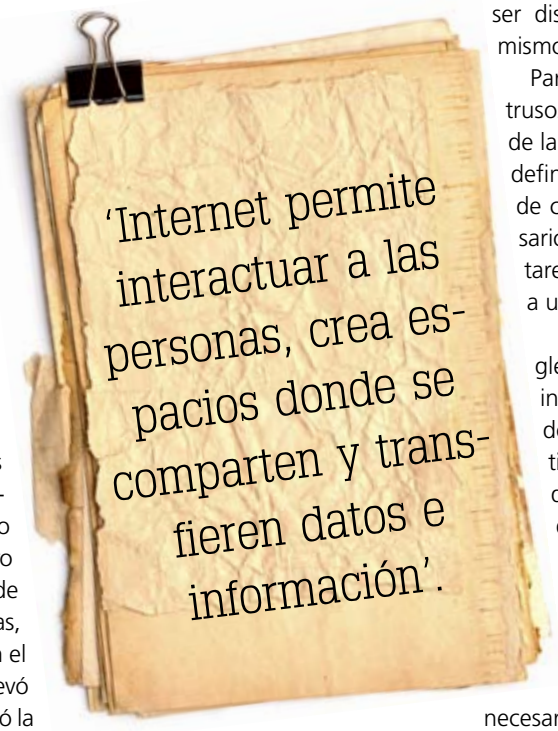
Con anterioridad son descritos algunos de los motivos que llevan a estos '*ciberdelincuentes*' a elegir estos espacios, pero no sólo están a la espera de que puedan conocer a su víctima por los recursos que ésta le proporciona indirecta e indiscriminadamente, sino que ellos de manera activa son impulsores a que existan las condiciones para el robo de información y datos de utilidad para él mismo, pues dependiendo de su ingenio y conocimientos técnicos puede tomar dos vías posibles. Por una parte tendría lugar una manipulación en una interacción social victima-victimario, aunque dependería en gran medida

de que tal dinámica pudiese llevarse a cabo y mantenerse. Existen diversos escenarios posibles que llevarían a la misma y diferentes consecuencias, pero es de resaltar el factor de manipulación en que por medio de un juego de emociones anómalas inducidas sobre el receptor –donde el delincuente es el emisor- es posible que durante un determinado tiempo en el *chat room* o en cualquier otro sitio de encuentro pueda este emisor ganar simpatía y consiguientemente la confianza sin que su interlocutor conozca sus verdaderas intenciones. Resumamos esta idea de la siguiente manera, por una parte tendríamos a un actor con una capacidad superior en la dinámica social sobre otro que es sometido y manejado en su contra.

Es pertinente rescatar para este asunto esa noticia que apareció en algunos diarios en la que dos jóvenes del municipio de Nogales fueron detenidos por citar a una persona por medio de *Facebook* con la intención de asaltarla y luego asesinarla[6]. La fuente nos dice que los dos jóvenes contactaron a un hombre de 41 años del que conocían sus actividades. De acuerdo al informe dado por el Procurador de Justicia del Estado los dos fueron detenidos por ser presuntos autores de aquel asesinato perpetrado tras darle un disparo en el tórax a la víctima después de haberle quitado sus pertenencias, posteriormente fue sepultada en el patio del domicilio donde se llevó el encuentro. Además se presentó la noticia de la existencia de un tercer inculpado del que se desconoce su identidad. La nota anterior es muestra clara de aquellos encuentros indeseados que pueden darse en torno a las redes sociales como medio o herramienta para los delincuentes.

Por otra parte resulta ingenioso y de requerimientos más especializados en el campo informático al usar conocimientos en cuanto a informática[7] y programación[8] a favor de la delincuencia. Ya que de esta forma se pueden desarrollar una variedad de virus informáticos y otros software mal intencionados con las más diversas finalidades, una de ellas infiltrarse en una computadora sin el consentimiento de su propietario con el objetivo de sólo dañar el buen funcionamiento del equipo atacado o resultar molesto, realizar una broma hasta recopilar información de un ordenador y transmitirla al origen como sucede con los denominados *spyware*[9]. Este último resulta una amenaza en contra de la seguridad en cuanto a la confidencialidad informática de los usuarios de la red.

A continuación se presenta una breve descripción de los *softwares* malintencionados o *malware* más comunes. Cabe mencionar que en un principio éstos fueron elaborados como un experimento, una broma o algo molesto hasta llegar al punto de ser diseñados para sacar beneficios con los mismos.



Para empezar con el listado de estos 'intrusos' vale presentar qué es un *software*[10] de la forma más sencilla posible, para esto lo definiremos como un conjunto de programas de cómputo de componentes lógicos necesarios que hacen posible la realización de tareas específicas basadas en instrucciones a un ordenador.

Malware[11] *(malicious software* en inglés) es un tipo de *software* diseñado para infiltrarse en el sistema de una computadora o bien para dañarla sin el consentimiento de su propietario. Es considerado como tal de acuerdo a las intenciones de su creador y de éstas los efectos que tengan sobre equipos informáticos ajenos. El término *malware* es usado para incluir a los virus, gusanos, troyanos y algunos *rootkits, spyware, adware* intrusivo, *crimeware* y otros más. Es necesario diferenciar un *malware* de un *bug* o *software* defectuoso el cual resulta igualmente peligroso pero de carácter no intencional.

Malware infeccioso

Virus informáticos son aquellos programas que al ejecutarse se propagan y afectan a otros *software* del equipo alterando su buen funcionamiento. A la vez hay una variedad que contienen un *payload*[12] que realiza una acción maliciosa como borrar archivos.

Gusano informático tiene la característica de duplicarse a sí mismo, éste no altera a los archivos de los programas instalados, sino que atacan

6 El Universal. Beyliss, Marcelo /corresponsal. "Lo contactan por Facebook para robarlo y asesinarlo", [en línea]. Hermosillo/ sábado 14 de enero de 2012, [consultado: 23 de enero de 2012]. Disponible en la Web: http://www.eluniversal.com.mx/notas/822601.html

7 Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores. Este término se le define como la información que se genera de manera automática y de manera digital a través de un sistema de cómputo. Conceptualmente, se puede entender como aquella disciplina encargada del estudio de métodos, procesos, técnicas, desarrollos y su utilización de computadoras con el fin de almacenar, procesar y transmitir información y datos en formato digital.

8 La programación es el proceso de diseñar, escribir, depurar y mantener el código fuente de programas computacionales. El proceso de escribir el código requiere frecuentemente conocimientos en varias áreas distintas, además del dominio del lenguaje a utilizar, algoritmos especializados y lógica formal. El propósito de la programación es crear programas que exhiban un comportamiento deseado por el programador.

9 "Spyware". Wikipedia la enciclopedia libre. [consultado: 23 de enero de 2012].

10 "Software". Ibídem.

11 "Malware". Ibíd.

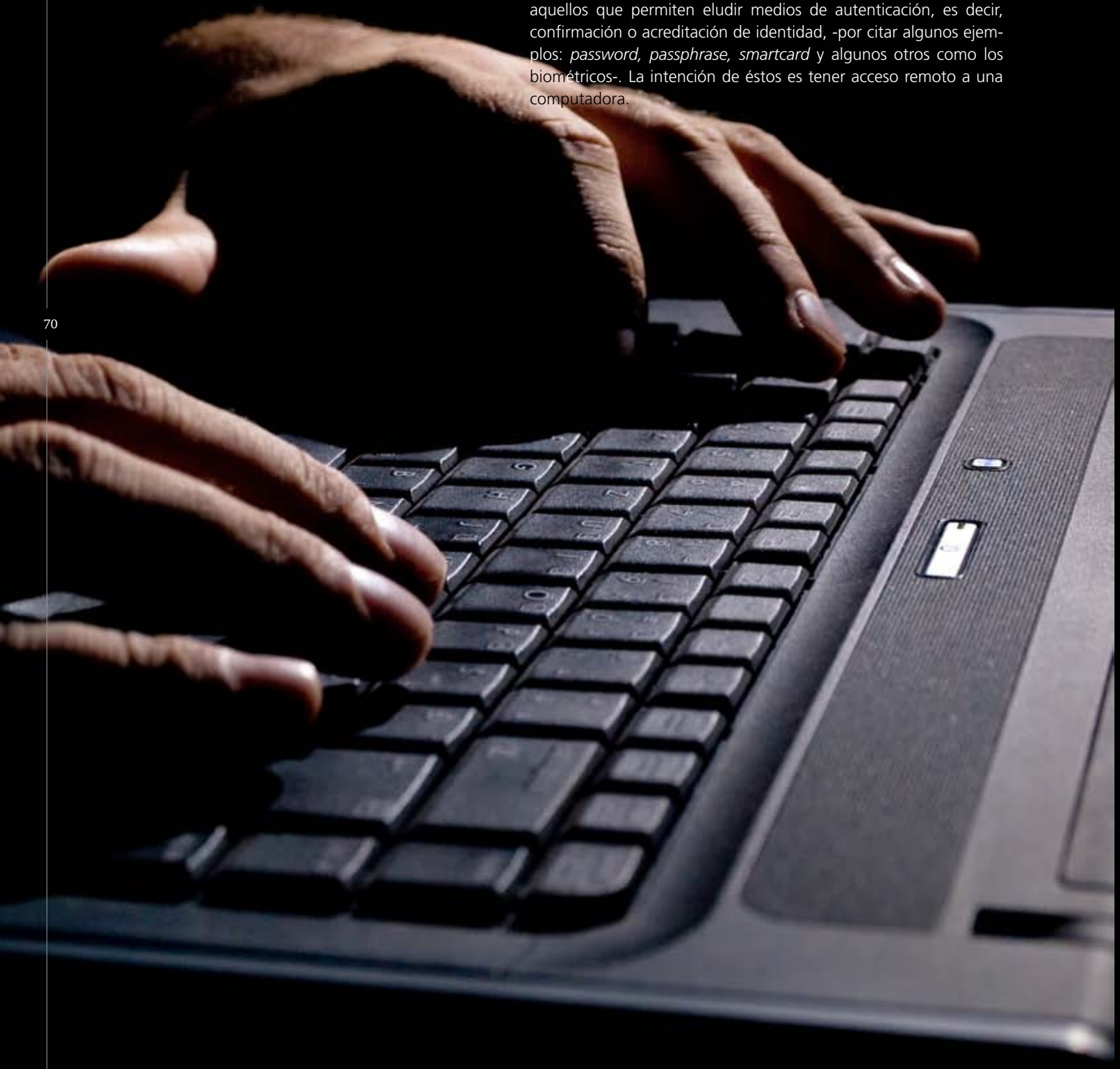
12 Payload en seguridad informática se refiere a la parte de un virus que realiza una acción maliciosa.

a la memoria al punto de alentar el equipo computacional, a su vez causan problemas en la red consumiendo ancho de banda. También son usados como medio de propagación de algún otro *software*.

Malware oculto

La condición subrepticia de un *malware* de esta clase es su principal arma, pues es de esa manera en la que actúa para alcanzar sus objetivos sin que el usuario del equipo atacado pueda eliminarlo antes de que empiece a realizar las operaciones programadas en el mismo.

Backdoors también conocidos como puertas traseras son aquellos que permiten eludir medios de autenticación, es decir, confirmación o acreditación de identidad, -por citar algunos ejemplos: *password, passphrase, smartcard* y algunos otros como los biométricos-. La intención de éstos es tener acceso remoto a una computadora.



Drive-by Downloads estos son instalados al acceder a algún sitio que instala spyware o códigos que dan información del equipo sin autorización del usuario. Se puede decir que existen páginas o sitios web[13] maliciosos.

Rootkits permiten el acceso continuo a un equipo manteniéndose activamente ocultos para extraer información, además de ocultarse a sí mismo permiten ocultar a otros malware que mantienen tal conexión.

Troyanos son programas que se presentan disfrazados para resultar atractivos e inofensivos al usuario -como los instaladores de programas y archivos adjuntos- invitándolo a ejecutarlo en un segundo plano, así permite la administración remota creando muchas veces *backdoors* que pueden causar efectos negativos como el robo de datos bancarios o información personal. Algunas de las funciones que realizan los troyanos están la instalación de otros programas maliciosos, captura de pulsaciones de teclado, impresiones de pantalla y borrado de archivos.

Hasta este punto se han descrito de manera básica las operaciones que realizan estos programas maliciosos, sin embargo es oportuno hacer algunas observaciones en cuanto a su uso, pues como lo mencionábamos anteriormente surgen como un experimento o una burla informática, pero al unísono del paso del tiempo han sido incorporadas en actividades criminales y de espionaje. Estos son los nombres que aparecen en escena: *spyware* o programa espía, *adware* y el *hijacking*.

Los *spyware* son aquellos programas que utilizan una conexión de internet para recopilar información de una computadora y transmitirla a otra sin que el propietario de la primera esté por enterado, monitorean la navegación en la red, cambian la configuración de los equipos provocándoles que se ralenticen tanto en memoria como en conexión a la red.

Adware son los programas que de manera automática se ejecutan y muestran publicidad web –anuncios, ventanas emergentes y otros similares-. Algunos de estos realizan un seguimiento de información personal retransmitiéndola a terceros sin consentimiento del usuario dando así el carácter de *spyware*.

Hijacking o secuestro son todas aquellas técnicas ilegales que pretenden robar algo, es un término muy amplio, aunque por lo regular se aplica cuando se ha efectuado un secuestro de conexiones de red, sesiones de terminal, módems y cualquier otro tipo de servicios informáticos.

13 En informática, la World Wide Web (WWW) o Red informática mundial es un sistema de distribución de información basado en hipertexto (nombre que recibe el texto que en la pantalla de un dispositivo electrónico permite conducir a otros textos relacionados pulsando con el ratón en ciertas zonas sensibles y destacadas) o hipermedios enlazados y accesibles a través de Internet. Con un navegador de Internet, uno puede ver páginas web que pueden contener texto, imágenes, videos y multimedia para navegar entre ellos a través de hipervínculos o enlaces.

Delitos informáticos y otros ataques

Hasta ahora se han presentado las herramientas –por así llamarlas- y las modalidades más frecuentes para irrumpir en la privacidad y estabilidad informática que en su conjunto formulan actividades delictivas que en términos informáticos denominan a un delito específico en agravio de algunos de los miembros de la comunidad virtual por parte de los malhechores como a continuación se muestra:

Crimeware es un *software* que ha sido específicamente diseñado para cometer delitos financieros en conexiones a la red con el objeto de robar la identidad de un usuario para tener acceso a los servicios financieros que una compañía ofrece. El término es aplicado cuando la finalidad de este programa es producir pérdidas económicas al afectado.

Phishing[14] es la denominación que reciben las estafas cibernéticas que intentan obtener nombres de usuario, contraseñas, detalles de tarjetas de crédito, números de seguridad social que tienen como recurso hacerse pasar por entidades de confianza en la transmisión de información electrónica atacando principalmente a usuarios descuidados que hacen uso de las redes sociales –actualmente el blanco principal-, subastas electrónicas, pago en línea y más donde la apariencia en definitiva engaña. Los métodos usados por el *phisher* (nombre que se le da al farsante) para obtener tales datos radica en el engaño o disfraces como una URL[15] (localizador de recursos uniforme) mal escrita haciéndose pasar por los de una organización seria que envía un correo electrónico o con el uso de la arroba en direcciones electrónicas que la contengan para preguntar usuario y contraseña y luego redireccionarlos a otro sitio cuando se accede a internet.

Existen otras formas como el uso de los *Javascrips*[16] en los que se alteran la barra de direcciones cerrando la barra genuina y abriendo una fraudulenta, también está otro método llamado *Cross-site scripting* que consiste en que el atacante utiliza el mismo código de programa del portal de alguna compañía bancaria, de esta forma el usuario inicia su sesión en dicho portal y tiene que verificar sus cuentas con un enlace aparentemente genuino en el que se copian datos valiosos para su posterior uso. Además se conoce otra técnica de engaño -aunque no tan común- en la cual se usan nombres de dominios de tal parecido que no se pueden distinguir fácilmente, ya que suelen cambiar caracteres por otros muy similares, se les conoce como ataques homógrafos, pues en estos casos se cambian letras de una palabra escrita en determinado alfabeto por otras tan parecidas pertenecientes a otro, por citar algún ejemplo están los intercambios del alfabeto latino por caracteres del alfabeto griego o cirílico.

14 "Phishing". Wikipedia la enciclopedia libre. [consultado: 23 de enero de 2012].

15 Localizador de recursos uniforme, más comúnmente denominado URL (sigla en inglés de uniform resource locator), es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vídeos, presentaciones, presentaciones digitales, etc.
El URL es la cadena de caracteres con la cual se asigna una dirección única a cada uno de los recursos de información disponibles en la Internet.

16 JavaScript es un prototipo basado en un lenguaje de programación *(scripting)* de alto nivel que en su uso en las páginas web tiene entre otras funciones la apertura de una nueva ventana su posición y tamaño, validar los valores de un formulario web que permite al usuario introducir los datos que se envía a un servidor para su procesamiento, cambio de imágenes, transmitir información sobre hábitos de lectura y navegación web para seguimiento de anuncios, personalización y más.

Lavado de dinero por actividades delictivas derivadas del uso de *phishing* son oportunidades de trabajo en línea en la que una empresa ficticia oferta vacantes atractivas –por las comisiones recibidas- de trabajo sin salir de casa en las que el contratado tiene la tarea de realizar el depósito de cantidades de dinero en bancos y de hacer varias transferencias electrónicas manteniendo el dinero en movimiento para dificultar su rastreo haciéndolas pasar por ingresos ganados derivados de actividades legítimas para circular en sistema financiero sin ningún problema.

Pharming es aquel ataque que pretende redirigir el tráfico de un sitio web a otro sitio falso, desde luego manejado por una máquina distinta. Este término guarda cierta relación con el de *phishing*.

Spoofing[17] es el término usado para referirse a las técnicas de suplantación de identidad con propósitos maliciosos y de investigación. Existen cinco tipos de estas técnicas dentro de este mismo:

IP *spoofing* suele ser el más conocido y tiene por objeto sustituir una dirección IP[18] por otra a través de programas concebidos para esto que logran ocultar un remitente o simplemente hacerse pasar por otro equipo.

ARP *spoofing* esta modalidad de *spoofing* está basada en la falsificación de la tabla ARP o *Address Resolution Protocol* (Protocolo de resolución de direcciones) que es la encargada de encontrar la dirección hardware[19] que corresponde a una dirección IP determinada, con esto se pretende falsear la relación IP-MAC[20] con lo que consigue enviar paquetes a un *host*[21] distinto al legítimo, en este caso al *host* del atacante.

DNS *spoofing* es el falseamiento por suplantación de identidad por el nombre de dominio, es decir, que se falsea la relación Nombre de dominio-IP o más bien un DNS[22] con una dirección IP falsa o viceversa.

Web *Spoofing* es una página web espuria con función de *proxy*[23] de otra genuina en que la conexión de la víctima es ´enrutada´para que en ella se pueda obtener información y datos.

Mail spoofing se refiere a la suplantación de un correo electrónico ajeno o manipulado en la dirección del remitente y otras partes de la cabecera del correo para que parezca como si el correo electrónico se originó en una fuente diferente, es usado como conducto para el envío de correos electrónicos de tipo *hoax*[24] o bulo con los que es posible obtener una lista de direcciones de correos electrónicos para la difusión de una noticia falaz o algún *malware* a gran escala.

Tráfico *online* de contenidos protegidos o piratería

Mientras uno navega en la red puede toparse con algún sitio en los que se puede adquirir y compartir distintos tipos de archivos como música, películas, libros, obras artísticas y otros productos informáticos copiados o falsificados de contenido protegido que no reportan su correspondiente tasa a los propietarios de los derechos de autor o de invención. De esta manera, se estarían violando a los ya indicados –sin que se pueda estar completamente consiente de esta situación- dando lugar a lo que suele denominarse como tráfico *online*[25] de contenidos protegidos o mejor conocida como piratería. Tal situación es similar a la que se vive en el comercio informal en las calles de productos con contenidos de iguales o parecidas condiciones.

Existen distintos y muy diversos factores que promueven esta actividad y su derivado crecimiento y daño a estos propietarios, por citar algunos, tendríamos situaciones como ver la película en cartelera y de recién estreno en la pantalla grande sin tener que salir de casa o tener en nuestro reproductor de mp3 las canciones más escuchadas en la radio sin la necesidad de comprar un álbum o quizás realizar una descarga con su respectivo costo.

La ley SOPA *Stop Online Piracy Act* (Acta de cese a la piratería en línea) o Ley H.R. 3261 es un proyecto de ley presentado en la Cámara de Representantes de los Estados Unidos el 26 de octubre de 2011. Es considerada por sus opositores como un enorme recorte a las libertades de navegación en la red, en cambio los autores o propietarios de los derechos de contenidos protegidos y todos aquellos que se ven implicados apoyan esta medida, ya que la piratería atenta en contra de sus intereses en cuanto derechos de autor o de propiedad intelectual.

Esta ley convierte al *streaming*[26] sin autorización en un delito que viola a los derechos morales y patrimoniales que la ley concede a los autores (copyright) por el sólo hecho de la creación de una obra, esté publicada o inédita.

17 'Spoofing". Wikipedia la enciclopedia libre. [consultado: 23 de enero de 2012].

18 Dirección IP es una tarjeta numérica de identificación de una tarjeta de red de una computadora que usa el protocolo IP (Protocolo de Internet por sus siglas en inglés) que tienen las funciones de enrutamiento de los datos en bloques conocidos como paquetes o datagramas en una conexión de un host (computadora conectada a una red) origen a otro host destino. Esta dirección puede cambiar en una reconexión por lo que se le llama dirección IP dinámica, existen otras, las direcciones IP fijas que no cambian con el tiempo para aquellos sitios de Internet que requieren estar conectados permanentemente.

19 Dirección asignada a la computadora que se conecta a una red. Los cuadros enviados de una computadora a otra deben contener la dirección de hardware del receptor. Las direcciones de hardware también se conocen como direcciones físicas.

20 Se conoce también como dirección física, y es única para cada dispositivo.

21 Computadora conectada a una red.

22 Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

23 Un proxy, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

24 Son noticias falsas que intentan hacerse pasar por verdaderas de divulgación masiva por los medios de comunicación, en la actualidad, son mayoritariamente difundidos vía Internet. Se han encontrado principalmente en foros y cadenas de mensajes –como las ya frecuentes cadenas de la buena suerte-. No buscan fines de lucro en cambio pueden resultar destructivos. Con éstos es posible obtener direcciones de correo electrónico (para enviar virus masivos, mensajes con suplantación de identidad o más de los mismos) engañando al destinatario para aceptarlo, ya que son mensajes que tratan de los más diversos temas de interés y de opinión pública.

25 En general, se dice que algo está en línea, on-line u online si está conectado a una red o sistema mayor.

26 Es la distribución de multimedia a través de una red de computadoras de manera que el usuario consume el producto al mismo tiempo que se descarga. Se aplica habitualmente a la difusión de audio o video.

Se han tomando medidas para detener a las principales webs de intercambio de archivos como la ejecutada por el FBI y dada a conocer recientemente por los medios: la inhabilitación de *Megaupload* que fue un sitio web de servicios de alojamiento de archivos la cual se encontró culpable de violar los derechos de autor, a su fundador y demás involucrados como los responsables –que de acuerdo con el Departamento de Justicia de los EEUU- de "piratería masiva en todo el mundo de diferentes tipos de obras protegidas por derechos de propiedad intelectual"[27].

En relación a la industria musical, para la mayoría de músicos su verdadera fuente actual de ingresos está en la actuación en vivo y no en la venta de discos, de la misma forma la industria cinematográfica ha sufrido los estragos de la piratería y ha optado por manifestarlo[28]. En cambio existen grupos de cibernautas que promueven de alguna manera el libre tráfico de archivos manifestada en la libre expresión e independencia de Internet como la postura que adopta *Anonymous*[29].

CONCLUSIÓN

En fin son tantas las técnicas, herramientas y modalidades de la delincuencia informática y de tales especificaciones técnicas que es un tanto difícil describirlas todas en este trabajo, ello requeriría de una labor extensa y en constante actualización, pues al unísono en que se desarrolla una nueva tecnología es casi probable que se esté desarrollando una paralela con fines delictivos. Por lo anterior se concluye con lo siguiente: la delincuencia en su desarrollo histórico ha incorporado sin dudar las novedades tecnológicas que cada época le ofrece para lograr su cometido en este caso la web. Por su lado los aparatos de administración y procuración de justicia de nuestro país, así como de la legislación existente para la sanción y penalización de estas actividades no van a la par, pues la modesta voluntad en hacer contemplar su inserción en este ámbito[30] y en algunos otros casos la omisión total del tema como sucede en los códigos penales de las diferentes Entidades Federativas, promueven a que dicha modalidad delictiva se desarrolle sin trabas en la impunidad en línea.

En tanto al Criminólogo-criminalista en su que hacer profesional debe de tomar en cuenta el estudio de los problemas delictivos en la red para estar a la par de las tendencias en el uso de Internet, informática y programación que la delincuencia incorpora día con día. De esa manera, este profesional conseguirá ampliar su campo de acción a la vez mantenerse a la vanguardia, de lo que sólo se exige su constante actualización puesto que el mundo tecnológico evoluciona a pasos agigantados. Cabe aclarar que no se pretende que sea un especialista en la materia, sino que este profesionista posea los conocimientos y herramientas básicas para comprender la problemática.

FUENTES BIBLIOGRÁFICAS

Electrónicas

Código Penal Federal. Ley Federal del Derecho de Autor. Cámara de diputados. [En línea]. [Consultado: 24 de enero de 2012]. Disponible en la web: http://www.diputados.gob.mx

Comisión Federal de Telecomunicaciones (COFETEL), Secretaría de Comunicaciones y Transportes. [En línea]. [Consultado: 23 de enero de 2012]. Disponible en la web:http://siemt.cft.gob.mx

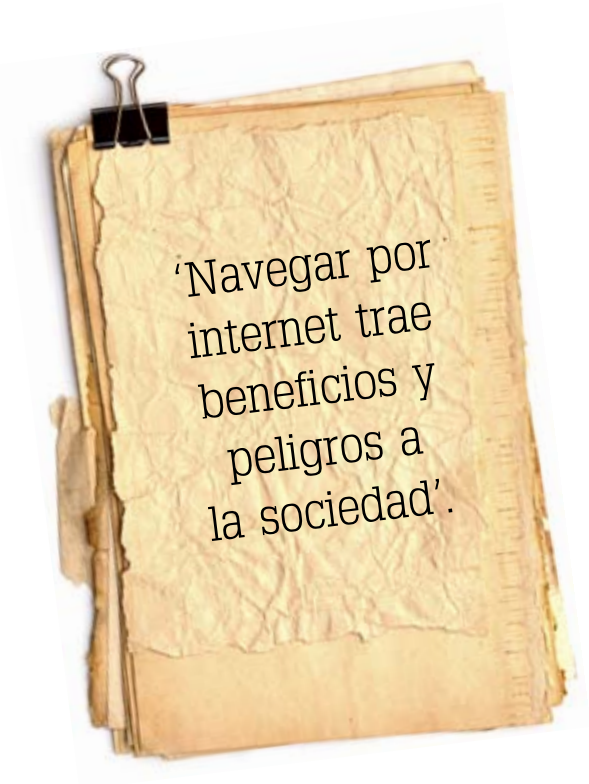
El Mundo. Rodríguez, Sergio. [En línea]. [Consultado: 24 de enero de 2012]. Disponible en la web: http://www.elmundo.es

El Universal. Beyliss, Marcelo /corresponsal. [En línea]. [Consultado: 23 de enero de 2012]. Disponible en la web: http://www.eluniversal.com.mx

Facebook. [En línea]. [Consultado: 23 de enero de 2012]. Disponible en la web: http://www.facebook.com

Diario Milenio. Corona, Jessica. [consultado: 23 de enero de 2012]. Disponible en la web: http://www.milenio.com

Wikipedia la enciclopedia libre. [En línea]. [Consultado: 23 de enero de 2012]. Disponible en la web:http://es.wikipedia.org



27 El Mundo. Rodríguez, Sergio. "El FBI cierra Megaupload, una de las mayores webs de intercambio de archivos". [en línea]. 20 de enero de 2012, [consultado: 24 de enero de 2012]. Disponible en la web: http://www.elmundo.es/elmundo/2012/01/19/navegante/1327002605.html

28 El Universal. García, Patricia. "Se baten en la SOPA". [en línea]. Viernes 20 de enero de 2012, [consultado: 24 de enero de 2012]. Disponible en la web: http://www.eluniversal.com.mx/espectaculos/110743.html

29 Anonymous. Wikipedia la enciclopedia libre.

30 El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos. También es necesario para este fin consultar los artículos 211 bis 2 y 211 bis 3. En cuanto a piratería véase la Ley Federal del Derecho de Autor. Título IV, capítulo IV. Aunque se contempla en la legislación estas actividades existen muchos vacíos, omisiones y sobre todo seguimiento, especificidad y actualización.