

LA CARA OCULTA DE INTERNET

Ricardo Fornas Carrasco

Introducción.

Internet se ha revelado como la auténtica revolución de la información que ha surgido a finales del siglo XX. Es necesario matizar que no hay una única Internet sino varias y su multiplicidad refleja por extensión la compleja sociedad en la que vivimos. Hablar de la cara oculta de Internet es idéntico al análisis de aquellas cuestiones candentes de la sociedad en el que se entremezclan actos reprobables desde un punto de vista ético junto a acciones claramente ilegales o criminales. Este artículo pretende exponer aquellas áreas de sombra que se manifiestan en Internet. Esta situación es un tanto difusa puesto que no hay una clara demarcación entre la Internet legal o la Internet alegal o ilegal. Recordemos que la red de redes es un fenómeno mundial y proyecta sobre la misma la gran diversidad de culturas, sistemas políticos o creencias. La versión oculta o criminalizada que intentaremos ofrecer responde a aquellas cuestiones que se consideran como tales desde nuestra perspectiva cultural, cuestiones que se abordarían de manera diferente desde otros ámbitos. Podríamos relatar multitud de ejemplos para demostrarlo. Así, para una mujer de la Unión Europea, la igualdad de sexos es un derecho fundamental, pero no sucede lo mismo en otras culturas. La exhibición de una foto de un niño desnudo en España puede considerarse pornografía infantil pero no lo es en otros países. La ciencia ficción es considerada una religión en Estados Unidos pero una secta perseguible en Alemania. En suma, ¿qué nos ofrece Internet?, su capacidad de comunicar, de compartir información. Un fenómeno que se está transformando en la nueva arma estratégica del siglo XXI. Intentaremos exponer en este artículo un estado general de la cuestión en aspectos que afectan directamente a la defensa de las libertades y el derecho a la privacidad, los *cibercrímenes* o la vulneración de sistemas legislativos. Cuando se expone el discurso de las facetas *ocultas* de la Red deberemos huir del tópico de considerar este tema como asunto exclusivo de *hackers* adolescentes e irresponsables, ni campo de acción para individuos de conducta antisocial o seres con apetitos sexuales reprobables. No hay que negar que estas situaciones ocurren pero no son las únicas, habría que adjuntar acciones ilegales de empresas de sólida reputación o de gobiernos autoproclamados como ejemplos de la libertad y de la democracia.

¿Cuántas Internets existen?

Desde el punto de vista de la información es razonable establecer una serie de distinciones y no considerar a Internet un único medio global de comunicación. En realidad ningún internauta tiene acceso a *todo* Internet. Existen situaciones de inaccesibilidad a determinados contenidos y áreas de la red y conviene que sepa distinguirlos.

- Internet global:
Definiremos ésta como aquella Red de información libre y gratuita que es accesible teóricamente mediante la interconexión de ordenadores. La forma de acceso se realiza mediante programas navegadores, Chats, mensajería o intercambio de protocolos (FTP, P2P)¹.
- Internet invisible:
Responde a todos aquellos contenidos de información que están disponibles en Internet pero que únicamente son accesibles a través de páginas generadas dinámicamente tras realizar una consulta en una base de datos. Esta particular naturaleza les hace inaccesibles a los

procesos habituales de recuperación de la información que realizan buscadores, directorios y agentes de búsqueda. Pero podemos acceder a las mismas mediante nuestras habituales herramientas de navegación, correo, etcétera. La única condición es saber exactamente la dirección de acceso (URL o FTP)

- Internet oscuro:
Se define como los servidores o *host* que son totalmente inaccesibles desde nuestro ordenador. Según un estudio de la compañía [Arbors Networks](#) esta situación sucede esto en el 5% de los contenidos globales de la Red. La causa principal (78 % de los casos) se debe a zonas restringidas con fines de seguridad nacional y militar. No olvidemos que Internet es un invento militar. El porcentaje restante, (22%) obedece a otros motivos: configuración incorrecta de routers, servicios de cortafuegos y protección, servidores inactivos y finalmente “secuestro” de servidores para utilización ilegal.

Una vez establecida esta distinción de las Internets existentes vamos a abordar la cuestión real de la cara “oculta” de la Red. Esta situación se solapa entre las diferentes Internets y para evitar confusiones hablaremos de los contenidos en sí y no tanto del canal específico donde se desenvuelve.

Estableceremos tres grandes campos de análisis en el que iremos desglosando este tipo de actividades: comunicación, información, compra-venta y servicios.

COMUNICACIÓN

Existen varios mecanismos *ocultos* de Internet para controlar y espiar las comunicaciones que se realizan en cualquier sesión de conexión. En Internet, definiremos comunicación como el sistema de intercambio de información y transmisión de datos que se realiza entre ordenadores interconectados. Es el servicio donde se realizan más actividades ocultas y son especialmente graves porque siempre se realizan sin el conocimiento del usuario.

1. Control gubernamental

Los estados hace tiempo que aplican la tecnología para la vigilancia y control de individuos y de otros gobiernos. Son los únicos que poseen la infraestructura y recursos para movilizar un gran número de efectivos y equipos. Sus actividades se centran en espionaje de la actividad que realizamos desde nuestro ordenador (utilización de programas, manejo del correo electrónico, tipo de conexiones) y conocer los contenidos que alojamos en él (textos, imágenes, sonidos). El ejemplo paradigmático de esta actividad *oculta* es «*Echelon*», un proyecto de espionaje a gran escala gestado por la NSA (Agencia Nacional de Seguridad de los Estados Unidos) en el que participan EE.UU., Canadá, Gran Bretaña, Australia y Nueva Zelanda y que tiene sus orígenes en un acuerdo secreto firmado en 1948 entre Estados Unidos y Gran Bretaña para espiar las comunicaciones. Desde entonces ha ido evolucionando con la incorporación de nuevas tecnologías y extendiendo su radio de acción a todo el mundo. El *Proyecto Echelon*, cuya denominación correcta es Sistema de Espionaje de Señales de los Estados Unidos (United States Sigint System USSS), surgió en la década de los 70 para facilitar las tareas de espionaje de los satélites de comunicaciones. Es un sistema que permite *vigilar y detectar* todo tipo de comunicaciones (fax, teléfono, Internet, señales de radio) mediante satélites espía, estaciones de escucha y ordenadores. La informática incrementó las prestaciones de detección de comunicaciones, confeccionando programas específicos, por ejemplo *Carnivore*, para seleccionar todo tipo de mensajes que contuviesen determinadas palabras clave, algo muy semejante a la función que realizan los buscadores. Se trata un sistema de procesamiento enorme que sólo puede ser llevado a cabo mediante

procesos automatizados y técnicas de inteligencia artificial. Su función de espionaje se centra en el sector civil de la sociedad: (gobiernos, empresas, organizaciones o individuos) y en el área de Internet funciona a pleno rendimiento en sectores como el correo electrónico, Chat o grupos de noticias. A pesar de que *Echelon* es el más conocido no es el único. La Unión Europea creó en 1995 ENFOPOL. Rusia también dispone del *SORM* mediante el cual ha obligado a todos los proveedores de Internet rusos la instalación de sistemas de monitorización exclusivos para sus servicios secretos. No pensemos que se trata de actividades típicas de superpotencias, un país tan discreto como Suiza posee también su propia red denominada *Satos3*. Sin duda, ha logrado ser más invisible que los otros proyectos que hemos mencionado. Ni si quiera un buscador como Google le facilitará más de 4 ó 5 direcciones que la informen de la misma.

2. Troyanos

Son programas que se instalan maliciosamente en su ordenador y permiten a un usuario externo tomar el control del sistema, manipular ficheros o transferir información. Suelen introducirse mediante software, archivos adjuntos de correo electrónico o aprovechar vulnerabilidades de navegadores de Internet, clientes de correo o similares.

Existen dos tipos de troyanos:

- Troyanos destructivos: su único propósito es borrar ficheros o formatear el disco duro. Tienen un comportamiento bastante semejante a los virus pero a diferencia de éstos no se reproducen ni contaminan a otros ordenadores.
- Troyanos de control remoto: sus tareas más conocidas son monitorizar y averiguar de manera remota qué actividades realiza un usuario con su ordenador: facilita la captura de pulsaciones de teclado lo que permite al *espía* acceder a todo tipo de servicios y actividades que requieran el uso de contraseñas y palabras clave. Otra actividad muy común de los troyanos es el envío de capturas de pantalla que permiten obtener una instantánea de las actividades que realizábamos en el monitor.

No existen muchos directorios especializados en troyanos y suelen formar parte de directorios más genéricos sobre seguridad. Para hacerse una idea aproximada del tipo de troyanos existentes puede visitar:

Simovits Consulting

<http://www.simovits.com/nyheter9902.html>

Desde esta dirección podrá acceder a amplios listados de troyanos detectados. Se pueden localizar por nombre, tipo de sistema operativo, país, lenguaje de programación, etcétera. La descripción de cada uno es muy completa.

3. Sniffer

Un sniffer es una aplicación informática que analiza el tráfico de datos que pasa por un punto concreto de la red. Sus múltiples utilidades y aplicaciones le dotan de una gran versatilidad. En el mundo oculto de la red, los *hackers* la han desarrollado para que sea capaz de capturar determinados paquetes de información de algunos protocolos empleados en determinados puertos de comunicación de los ordenadores cuando enviamos o recibimos información. Cualquier paquete de información que no esté encriptado puede ser leído, interpretado y utilizado por aquel individuo o grupo que ha lanzado ese sniffer.

4. KeyLoggers

El keylogger es una aplicación informática que monitoriza la actividad de un ordenador y la almacena en un archivo de registro denominado *log*. Es un programa capaz de captar los "clics" del ratón y todas las teclas utilizadas en una sesión.

5. Virus

Son uno de los elementos más destructivos de un ordenador. La interconexión de la red de redes y los puntos débiles de programación en aplicaciones como el correo electrónico, contribuyen a que el problema se torne en una seria amenaza. Su ordenador debería estar dotado de un programa antivirus para prevenirse de los efectos del virus, pero el auténtico problema es que en muchos casos la rapidez de penetración de los virus en Internet es superior a la capacidad de reacción de estos programas. Para estos casos, es necesario disponer de alguna página de carácter independiente en que le puedan informar en tiempo real de todas las incidencias. Son especialmente útiles:

Asociación de Internautas

<http://seguridad.internautas.org/3C/es/alertvir.php>

Portal español independiente que se ocupa de cuestiones relacionadas con la seguridad y privacidad. Esta Asociación dispone de un programa gratuito que informa en cada sesión que nos conectemos a la red o cada 12 horas de alertas de seguridad vigentes.

Virus Encyclopedia

<http://www.antivirus.com/vinfo/virusencyclo/>

Como expresa el mismo título es una auténtica enciclopedia sobre los virus. Podrá realizar consultas por nombre, tipo de infección ocurrida, daños potenciales y fecha de aparición o de activación del mismo.

INFORMACIÓN

El aserto clásico de que “información es poder” también es aplicable a Internet. La red de redes se reduce a un diminuto soporte físico de átomos (ordenadores y cables) que sustentan un auténtico mundo de bits donde la información es la principal cadena de valor.

Existen múltiples ejemplos que lo evidencian, incluso en casos de confrontación bélica. En una guerra la neutralización del enemigo es prioritaria y por ello se atacan sus sistemas de defensa, vías de transporte, fábricas de armamento, estaciones de energía y demás elementos logísticos. Resulta interesante señalar que durante el conflicto de Kosovo, la OTAN evitó en todo momento dañar sistemas vitales de conexión a Internet para que la población serbia tuviera la posibilidad de acceder a fuentes externas de información y contrarrestar el control propagandístico del gobierno de la radio y la televisión. Aunque es difícil estructurar sistemáticamente un campo tan abigarrado e impreciso como es la información abordaremos la cuestión desde la perspectiva del espionaje, la información *sensible*, la desinformación y la información privilegiada.

1. Espionaje y criptología

Anteriormente hemos citado algunos sistemas de espionaje aplicados a las comunicaciones (proyecto Echelon, sniffers, troyanos, etcétera). La amenaza contra la privacidad genera sistemas de defensa y prevención como la generación de cortafuegos (*firewalls*) o el desarrollo de sistemas criptográficos. Por cuestiones de espacio no podemos desarrollar con amplitud este tema pero podrá encontrar abundante información en el [Rincón de Quevedo](#) una página de Internet en el que efectúa un amplio recorrido de la historia, principios teóricos y programas de uso en Internet para aplicaciones criptográficas.

Aunque se debate sobre la potencia y seguridad de estos sistemas suelen ser un método muy recomendable para preservar la información de acciones de espionaje.

Uno de los sectores que tienen más necesidad de utilizar la criptología son aquellos que realizan actividades perseguibles por los gobiernos como cibercriminales, terroristas o narcotraficantes). Su uso para estos grupos resulta contraproducente porque señala claramente que “alguien” intenta ocultar “algo”. Una de las normas básicas en cuestiones de seguridad es que se deben utilizar procedimientos tan “normales” que no llamen la atención. Por ejemplo, el continuo flujo de mensajes cifrados desde una dirección de correo electrónico localizado en una *madrassa* pakistaní (especie de seminario religioso musulmán) es el mejor reclamo para que las potentes agencias de espionaje fijen su atención en ellos. Por tanto se recurren a procesos más invisibles:

Esteganografía

Consiste en ocultar un mensaje secreto dentro de otro mensaje que es abierto y de acceso público. En Internet es habitual la utilización de formatos de imágenes para intercalar texto sin alterar las propiedades esenciales de la imagen. Inicialmente este método se aplicaba para proteger los derechos de propiedad de imágenes porque si alguien la copiaba de manera fraudulenta es posible que ignorara que en la propia imagen constaban datos del propietario original.

Hacking

La otra tendencia es un poco más complicada y arriesgada y es recurrir al *hacking* para introducirse en determinados servidores. El asaltante no pretende ni explorar ni espiar los contenidos del sistema vulnerado. Pretende introducir solapadamente contenidos propios (instrucciones, consignas, mensajes) que permitan una comunicación entre los seguidores de estos cibercriminales o terroristas sin despertar las sospechas de quien los vigile. Imaginemos que un *ciberterrorista* entran en el servidor de un medio de comunicación o el de una universidad y cuelga un directorio nuevo con sus propios documentos. El resto del grupo ciberterrorista sólo tiene que visitar estas páginas expresamente creadas para ellos. Es un sistema que permite burlar la vigilancia de espionaje que controle todos sus movimientos en la red ya que un análisis de *logs* pertenecientes a un diario como “La Vanguardia” o de una página del ayuntamiento de Ávila no despertaría sospechas de alojar precisamente información o consignas de cibercriminales.

Spyware

El spyware es una aplicación informática instalada inadvertidamente en nuestro ordenador para monitorizar toda nuestra actividad de navegación por la red y remitir todos esos datos directamente a la empresa propietaria del programa. Aunque parezca paradójico son los propios usuarios quienes instalan este tipo de aplicaciones sin saberlo, ya que siempre están asociados a algún programa gratuito o *shareware* que por su utilidad o eficacia gozan de la aceptación general. Un ejemplo habitual son los programas de intercambio de archivos o *peer to peer* como el denominado [Kazaa](#). Una vez instalados estos programas en nuestro ordenador se activan las aplicaciones *spyware*. Estos programas suelen ser propiedad de empresas de publicidad y mercadotecnia que de este modo obtienen una preciosa información sobre nuestros gustos y hábitos de consumo. A diferencia de los troyanos y los virus, su presencia en el ordenador no menoscaba ninguna de sus funciones y no pone en peligro ni el sistema operativo ni de los contenidos. Para defensa del internauta existe una utilidad altamente recomendable:

Spychecker

<http://www.spychecker.com/>

Base de datos que recopila este tipo de archivos espía. Sólo hay que introducir el nombre de una aplicación cualquiera, por ejemplo KazaA y nos facilita el nombre del programa y su compañía propietaria.

Los satélites e Internet

La sociedad civil está en disposición de generar y procesar información que en tiempos pretéritos estaba reservada a servicios gubernamentales y militares. Hoy día cualquier grupo de expertos independientes pueden corroborar o desmentir acusaciones de un gobierno o corporación sobre determinadas actividades ilícitas. Por ejemplo, las acusaciones de Estados Unidos, basadas en satélites espía, de que Irak está elaborando un plan de fabricación armamentística pueden ser evaluadas de manera independiente. Cualquier empresa o particular puede adquirir imágenes de idéntica naturaleza a compañías como [Space Imaging](#) o [Digital Globe](#) a un precio de 250 dólares la unidad. Usted mismo puede comprobar que tipo de imágenes afectan a la seguridad accediendo a la página de el [Institute For Science And International Security](#) (Instituto en pro de la Ciencia y la Seguridad Internacional), que publica estas fotos procedentes de satélites comerciales. Aunque los expertos militares aducen que la resolución de estas imágenes son muy bajas en comparación con los satélites militares o espía, al menos evitan su manipulación o simplemente falsificación.

2. Información sensible

La facilidad de acceso y anonimato de multitud de contenidos fomenta la preocupación de gobiernos, empresas e individuos por un tipo de información *sensible* cuyo uso malicioso puede ser una poderosa arma de individuos antisociales, grupos antisistema o bandas terroristas. Existen numerosos ejemplos de información *sensible* y aquí nos limitaremos a enumerar algunos cuantos y que servirán para precisar el estado de la cuestión:

Explosivos:

Uno de los patrones clásicos de información “peligrosa” son las instrucciones para fabricar todo tipo de artefactos explosivos o armamento. Internet no añade nada nuevo. Desde los años 70 era posible acceder a los fundamentos teóricos de cómo fabricar una bomba atómica con los materiales surtidos en una buena biblioteca pública pero olvídense del clásico artículo “[How to build a bomb](#)” que prolifera tanto en la Red, es una broma y ha sido objeto de ridículas especulaciones en la guerra contra los talibanes y Al Queda en Afganistán.

Un experto en información potencialmente peligrosa sabe que existen procesos fáciles y muy baratos para fabricar bombas biológicas o agentes químicos cuyo efecto destructivo no es nada desdeñable. El atentado del 11 de septiembre a las Torres Gemelas de Nueva York ha obligado a Estados Unidos a revisar la potencial información *sensible* que estaba expuesta en la Red. Ha resultado ser un amplio cajón de sastre que afecta a las diversas agencias y departamentos gubernamentales desde los mapas de oleoductos y depósitos de agua hasta la información sobre plantas químicas.

Armas biológicas

En otros campos supuestamente más inofensivos resultan ser potencialmente más peligrosos cuando determinada información *sensible* puede ser reorientada hacia actividades terroristas o criminales. Los avances en genética suelen ser publicados en Internet. Por ejemplo, el desciframiento del genoma de determinadas bacterias que es accesible desde la Red, podría ser aprovechado como arma biológica. Terroristas o gobiernos hostiles deberían reclutar a individuos que tuviesen la suficiente formación como para

transformar y procesar esta información y transformar un avance científico en un arma. Este tema ha sido objeto de atención de gobiernos e instituciones académicas y ha supuesto la revisión de todos estos estudios biológicos para evitar que determinados contenidos no se expongan en un medio como Internet.

Estupefacientes

En el controvertido tema de las drogas se evidencia la falta de una política unitaria de valorar qué información o contenidos deberían ser cuestionados para sus accesos públicos y cuáles no. Existen países donde hay gran permisividad e incluso amparo legal sobre algunas drogas que, en cambio, es fuertemente perseguido en otros. Pueden encontrarse auténticos portales temáticos sobre la drogas con información muy diversa [[La Marihuana.Com](#)] o auténticos manuales de química y farmacología sobre drogas sintéticas [[Rhodium](#)]

Atentados contra la propiedad

En este apartado específico prima la información que se genera en foros y grupos de noticias donde se exhibe toda una panoplia de recomendaciones para todo tipo de actividades ilícitas: debilidades de sistemas de alarma y antirrobo, trucos sobre cómo abrir un coche, asaltar una casa, sabotajes, etcétera. Una auténtica escuela de ladrones, aunque es cierto que suelen combinarse mensajes irónicos, absurdos o de mofa junto a otros caracterizados por *ideas* más centradas en el tema propuesto.

3. Desinformación e información privilegiada

Aunque son términos contrapuestos, manifiestan dos caras de la misma moneda. La cuestión de la desinformación podría abordarse desde varios puntos de vista, como veremos a continuación.

Ausencia de información

En este caso son una serie de noticias que no reciben la audiencia o la atención debida en los medios de comunicación tradicionales y grupos multimedia. La casuística es muy variada:

- Atención local de los medios de comunicación, de modo que se ocupan de temas que sólo interesan regionalmente y se olvidan de otras cuestiones candentes (por ejemplo, es probable que ignore muchos de los conflictos bélicos que desgarran a los países del Tercer Mundo).
- Acciones gubernamentales secretas o reservadas (el *Proyecto Echelon* que hemos mencionado anteriormente).
- Intereses de carácter comercial (cualquier medio de comunicación silenciará o minimizará informaciones que cuestionen la actividad o moralidad de su principal inversor publicitario). Por ejemplo, el problema de la explotación del trabajo infantil por parte de conocidísimas marcas de artículos deportivos.

Afortunadamente, en la Red, pese a las amenazas que se ciernen sobre ella (proyectos estatales de control, desembarco del gran capital para reconducirla a intereses mayoritaria mente comerciales, etcétera), persisten espacios de difusión donde se practica la libertad de expresión. Estas páginas de información no gozan de la audiencia de los otros medios y suelen ser descalificadas como marginales y antisistema. Suelen formar parte de organizaciones no gubernamentales muy diversificadas, que van desde la denuncia de destrucción de la selva amazónica a la impugnación del sistema de organización comercial y de producción de materias primas que deja al Tercer Mundo indefenso frente a las todopoderosas multinacionales de diverso pelaje (energía, productos farmacéuticos, ropa deportiva, etcétera). Deberá

formarse su propio criterio con la información que pueda recabar, y para ello le proponemos algunas direcciones que rompen la tónica informativa habitual.

Disinformation

<http://www.disinfo.com/>

Este servidor estadounidense es un auténtico buscador informativo atípico en el sentido que hemos comentado anteriormente. Trata de una variada gama de temas que abarcan la política, la ciencia, la contracultura o la espiritualidad. Proporciona noticias, artículos y dossieres donde se estudia un tema con una propuesta de direcciones para profundizar desde diversos puntos de vista.

Rebellion.Org

<http://www.rebellion.org/portada.htm>

Se autodefine como el periódico electrónico de información alternativa que publica las noticias que no son consideradas importantes por los tradicionales medios de comunicación. Uno de sus apartados [Mentiras y Medios](#) denuncia las falsedades y manipulaciones informativas de estos últimos.

Observatorio de crisis

http://observatorio.barcelona2004.org/observatorio/home_e.htm

Publicación electrónica con información de conflictos y crisis que acontecen en el mundo. Imprescindible para profundizar en aquellos conflictos "olvidados" o relegados por los medios de comunicación tradicionales de prensa, radio y televisión. Recoge amplia información y opiniones en torno a ellos, con una selección de dossieres que dan a conocer los datos más importantes y las claves de interpretación de los conflictos (antecedentes, evolución y posibles líneas de solución).

Información parcial o falsa

Esta modalidad se asocia normalmente con la rumorología. Atiende a múltiples frentes y su particularidad reside en que es difícil establecer cuál es su grado de credibilidad. Puede que en algunos casos adopte un tono amable e incluso resulte entretenida, sobre todo con las denominadas leyendas urbanas, que no son más que bulos y difusiones sobre los temas más variopintos (marcianos secuestradores, vampiros sueltos, etcétera). En otros casos deberá tener un criterio más definido para separar lo que es noticia e información verídica de los rumores.

The AFU & Urban Legends

<http://www.urbanlegends.com>

Página que recopila todo tipo de leyendas urbanas. Desde un menú desplegable puede seleccionar entre más de una veintena de temas, como salud, alimentación o televisión. Facilita una amplia información de FAQs (preguntas más frecuentes), procedente del grupo de noticias alt.folklore.urban.

Mail spoofing

Con este procedimiento se pretende suplantar el correo electrónico de un usuario o crear correos electrónicos supuestamente verídicos a partir de un dominio para poder enviar mensajes como si formasen parte de esa entidad. Imaginemos que tenemos la entidad BBVA (Banco Bilbao Vizcaya Argentaria) que dispone de un servicio de correo electrónico identificado con el siguiente dominio [ejemplodenombre@bbva.es](#). Si intentásemos difundir información financiera de intoxicación o falsa, el agente malicioso debería romper la seguridad del sistema informático del banco y crear una cuenta de correo electrónica falsa, por ejemplo [inversiones@bbva.es](#). A continuación, enviaría un mensaje a clientes del banco con cualquier mensaje, por ejemplo "a causa

de la crisis argentina el banco va a retener los fondos de sus depositantes durante un año para afrontar la grave carencia de liquidez de la entidad". Puede imaginarse el efecto que una noticia así tendría sobre clientes e inversionistas que inicialmente pensarían en su credibilidad ya que el remitente de correo proviene de de «inversiones @bbva.es». Ciertamente es un ejemplo exagerado pero perfectamente trasladable a empresas pequeñas o medianas que tal vez no dispondrían de la capacidad de maniobra o agilidad para reaccionar a un caso tan flagrante de manipulación informativa.

La alternativa más común es que el *mail spoofing* se emplee como estratagema de ingeniería social para solicitar el número de tarjeta de crédito a determinados usuarios confiados éstos en que la procedencia del mensaje se deriva supuestamente de la propia empresa de la que son clientes. Algo que ha sucedido recientemente con los clientes de Yahoo!.

Últimamente su ámbito de actuación ha pasado desde el ámbito de los negocios a la política donde se persigue el desprestigio de determinados grupos o personas al difundir supuestos mensajes de tono ofensivo o solicitando dinero.

Hoax

Prácticamente todos los internautas han recibido inquietantes noticias en torno a virus muy nocivos y totalmente destructivos que proliferan por Internet. La alarma que causan hace que se multipliquen los mensajes, formando una monumental cadena de transmisión de información que puede ser totalmente falsa. Para evitarlo hay servicios en la Red que le informarán de aquellos nombres de virus que son un bulo y de cuáles debe tomarse en serio, como la página descrita a continuación.

F-Secure: Security Information Center

<http://www.f-secure.com/virus-info/hoax/>

Directorio y buscador originario de Finlandia que facilita información de los falsos virus más conocidos, como Hoax. También es útil para otro tipo de historias y peticiones difundidas a través del correo electrónico. Lo único que se echa en falta es un mayor grado de actualización, ya que sólo realiza nuevas incorporaciones a la lista una o dos veces al mes.

Información privilegiada

Las finanzas, y especialmente la bolsa, han experimentado una gran pujanza debido al éxito del denominado capitalismo popular, en el que personas con unos modestos ahorros e ingresos medianos invierten parte de su capital en el mercado de valores. El problema radica en que su introducción en este juego no va acompañada de las necesarias aptitudes para evaluar la información que reciben (comparación de cuadros estadísticos, análisis sectoriales, etcétera) y tomar las decisiones más correctas. La cuestión de la economía globalizada empeora aún más la cuestión, porque una bajada de la producción de materias primas (por escasez, malas cosechas o agotamiento de recursos), de países remotos, puede repercutir negativamente en algún sector industrial, incidir muy negativamente en sus beneficios y traducirse en una bajada del precio de las acciones. Un ciudadano medio no está en igualdad de condiciones frente a las grandes corporaciones financieras, que disponen de una auténtica legión de especialistas para digerir toda esa información y saber interpretar las tendencias de los mercados. Si sumamos a esa escasa preparación informativa la propagación de todo tipo de rumores, el inversor inexperto se encuentra con un panorama nada halagüeño. ¿Cómo actuar ante un tipo de rumor de esas características? No debe precipitarse porque puede que llegue a lamentarlo. Debe cerciorarse de que es un rumor y no una noticia, luego intente comprobar su veracidad. Si se habla de una fusión entre dos empresas, lo más lógico es que visite la página oficial de las mismas para tener una impresión de primera mano (comunicados, desmentidos, etcétera), y otra acción aconsejable es acudir a medios de comunicación especializados.

Enlazando con el punto anterior nos encontramos ante una de las cuestiones más peliagudas: el tratamiento de la información privilegiada. Si albergaba alguna esperanza de encontrar instrumentos en Internet para obtener información privilegiada deberá desengañarse, a no ser que quiera arriesgarse a cometer actividades delictivas, como la intromisión en ordenadores y redes privadas. A este respecto, sólo podemos decir que en muchos casos puede que exista información a su disposición, debido a fallos de sistemas de seguridad, descuido o simplemente incompetencia, que permiten acceder a información confidencial de una empresa. Es cierto que probablemente no encontrará un enlace que indique desde dónde debe acceder, pero se sorprendería de lo que son capaces de hacer al respecto los buscadores. Sin duda, la información confidencial por antonomasia y que despierta más polémica es la de tipo financiero, por aquello de que con el dinero no se juega, o sí, pero con el de los demás. Cualquier modesto accionista habrá detectado que está inerme y en inferioridad de condiciones frente a los tiburones financieros, que son capaces de manejar información confidencial. Teóricamente este tipo de actitudes son vigiladas por los organismos y entidades creadas a tal efecto. En Wall Street es la SEC (Securities and Exchange Commission) <http://www.sec.gov> y para España es la CNMV (Comisión Nacional del Mercado de Valores) <http://www.cnmv.es>. O las reglas del juego son tan perfectas que nadie escapa a ellas o el proceso de control es deficiente, decida usted lo más conveniente. Pero sorprende, en el caso español, la escasez de expedientes abiertos por prácticas de movimientos en la bolsa auspiciadas por el manejo de información confidencial. No vamos a comentar el cacareado caso y curiosamente *congelado* caso Gescartera. El nuevo equipo manifiesta un celo y una actividad que para sí hubiesen querido los procesados en el caso de Enron. En algunos casos raya en el patetismo. Por ejemplo, se pretende [procesar](#) a un pequeño inversor en desempleo por la divulgación de todo tipo de rumores desde un foro de inversores en aras de aumentar la cotización de un determinado valor bursátil y de este modo revalorizar la participación de sus propias acciones sobre esa empresa – que desde luego no eran muchas comparadas con los grandes inversores o fondos de capital- .

Ejemplo de uso indebido de información confidencial son los procesos de fusión empresarial. Aquellas personas que negocian la fusión o sus colaboradores disponen de la posibilidad de comprar o vender acciones de las compañías afectadas con anticipación a la reacción del mercado, es decir, que les reporta un beneficio seguro. No parece que las autoridades bursátiles sepan o quieran afrontar este fenómeno con toda la energía que requiere.

Los confidenciales

Uno de los fenómenos que ha impulsado Internet es la presencia de publicaciones electrónicas especializadas en noticias "confidenciales" o rumores. Reseñan aquella información que los medios de comunicación no se atreven o no quieren publicar por tratarse de contenidos no debidamente confirmados o de rumores que aparecen en los mentideros habituales de los corrillos político-financieros. En el ámbito español puede encontrar una amplia variedad de las mismas [El Confidencial Digital](#), [Hispanidad](#), [SemanalDigital](#) y las secciones de El Conspirador –[Estrella Digital](#)–, El Confidente –[El Confidencial](#)– El Topo –[PRNoticias.Com](#)–, ConFidencial –[MiCanoa](#)–, El Espacio Dircom –[Dircom Digital](#)– o La Entrada Secreta –[El Mundo](#)–.

Las bitácoras, una especie de diarios virtuales digitales, también aportan contenidos de ámbito confidencial o de reflexión personal de sus autores sobre su profesión o actividad.

ACTIVIDADES FRAUDULENTAS DE COMPRA-VENTA Y SERVICIOS.

HACKING

Bajo esta denominación tan genérica se engloba toda una serie de actividades que tratan básicamente sobre la vulneración de sistemas de seguridad informática, derechos de protección industrial o derecho a la intimidad. Es decir, que engloba bajo una única denominación las diversas facetas ocultas de la Red que hemos intentado explicar: comunicación, información y compraventa de productos y servicios. Por razones de limitación de espacio nos centraremos en cómo se desenvuelve el mundo *hacker* para obtener de manera ilegal y gratuita recursos y aplicaciones informáticas. La actividad *hacking* se caracteriza por la utilización de un vocabulario o jerga muy especializada y por la dificultad en localizar fuentes estables de información y servicios. Resulta difícil apuntar qué páginas pueden proveerle de la información necesaria cuando muchas de ellas tienen una vida efímera, a veces cuestión de horas. Aunque los directorios y buscadores especializados en esta temática que le podamos sugerir suelen ser más estables, tropiezan con el inconveniente de recomendar muchos enlaces que ya no están activos. Los puntos de información más común que proporcionan los buscadores de *hacking* son:

- Contraseñas y números de serie: para la correcta instalación y ejecución de muchos programas se exige cumplimentar los formularios donde se debe incluir un número de serie.
- Cracks: son aplicaciones y sistemas que desprotegen las barreras de seguridad para ejecutar programas.
- Keygen: se trata de una herramienta generadora de claves, creada expresamente por crackers para cumplimentar los formularios que exigen determinados programas antes de instalarse con la petición de un nombre y una contraseña.
- ROMz: es una orientación para poder recrear de forma simulada una serie de programas que inicialmente fueron concebidos para uso exclusivo de determinadas plataformas y dispositivos. Por ejemplo, para que puedan ser reproducidos en un ordenador de sobremesa los juegos de videoconsola.
- Warez: bajo esta denominación se engloba la obtención gratuita por Internet de toda una serie de aplicaciones informáticas que se ejecutan en el ordenador. Presenta un panorama tan diversificado que se ha impuesto a su vez una especialización. Así, tenemos *gamez* para los juegos, *appz* para los programas, *moviez* para películas, *modz* para los juegos de rol, *mp3z* para archivos musicales, etcétera.

Para localizar información especializada de este sector es aconsejable tener presente unas consideraciones previas:

- Antes de buscar esta información tan peculiar deberá dotarse de los conocimientos más elementales para moverse con soltura en este tipo de contenidos. Deberá leerse los correspondientes manuales de iniciación y los diccionarios especializados, del mismo modo que para operar en bolsa tiene que familiarizarse con los términos y jerga del sector.
- Cerciórese de que es posible obtener una respuesta a lo que busca. No puede plantear a priori cuestiones imposibles, como buscar un programa de cracks universal que le permita superar las barreras de protección de cualquier aplicación o ejemplos similares. Naturalmente esta percepción la aporta la experiencia, pero rápidamente se dará cuenta de cuáles pueden ser los límites informativos al respecto.
- La estrategia más habitual para obtener información de hacking es localizar un interlocutor válido. Para localizar un experto debe servirse de los canales de

participación como foros, chats o grupos de noticias. Pero los auténticos expertos del sector se caracterizan por su anonimato y no proliferan en estas secciones. No obstante, la acción combinada de múltiples colaboraciones, consejos y ayudas que surgen en un foro de discusión o un Chat le resultarán muy enriquecedoras, ya que genera una especie de pensamiento y sabiduría colectiva.

El apartado de buscadores específicos de la cara oculta de la informática contiene un listado de direcciones que rompen el habitual monopolio anglosajón de la informática. No se sorprenda si las páginas más populares de este tipo de contenidos son rusas, búlgaras o coreanas ya que corresponden a zonas donde hay una menor presión en la persecución de este tipo de actividades, si las comparamos con las enérgicas acciones legales que se suelen emprender en Norteamérica y parte de Europa occidental. Los buscadores de *hacking* más efectivos son:

Astalavista

<http://astalavista.box.sk>

Es uno de los buscadores más veteranos centrado en cuestiones de seguridad. Su popularidad entre los internautas reside en su capacidad para facilitar contenidos como los que se han comentado más arriba. Tan solo tiene que ingresar su pregunta en la caja de búsqueda y activar el botón de búsqueda. Cuando proponga más de una palabra, éstas deberán estar separadas por un espacio en blanco y el buscador lo interpretará como si fuese el operador booleano AND. Carece de un sistema de búsqueda avanzada y limita la presentación de resultados a un máximo de 30 enlaces por consulta.

La Taberna de Van Hackez

<http://www.vanhackez.com/>

Página en español que facilita una cuidada y elaborada guía de cientos de enlaces relacionados con la seguridad, hacking, phreaking, (pirateo de sistemas de telefonía), virus, troyanos y todo lo relacionado con las actividades más subterráneas de Internet: decodificadores, liberación de teléfonos móviles, duplicación de DVD, etcétera. También proporciona un listado de publicaciones y e-zines relacionados con esta temática y dispone de un foro donde podrá leer y pedir información de aquello que necesite.

Narcotráfico

La nueva generación de narcotraficantes ha sido uno de los grupos que mejor ha asimilado las posibilidades de Internet como campo de sus actividades ya que ésta permite un mayor anonimato y discreción y permite amplias posibilidades de utilización de sus ganancias al aprovechar un nuevo medio carente de las estrictas normas del mundo real para “blanquear” y legitimar sus capitales. Veamos en qué sentido Internet ha facilitado sus operaciones:

- Empleo masivo del correo electrónico como servicio de comunicación más seguro y rápido frente a otros sistemas de mensajería como el teléfono o el fax. Permite coordinarse de forma más ágil y los riesgos de interceptación de la comunicación son menores ya que las huellas que puede dejar una infraestructura internacional eran más detectables mediante el teléfono o fax. Incluso hay *capos* del narcotráfico encarcelados que controlan y dirigen sus redes del exterior a través de Internet.
- Adquisición de equipos de alta tecnología como sistema de contraespionaje, de este modo permiten estar alerta sobre posibles acciones policiales contra ellos. Desde Internet se pueden adquirir aparatos

de última tecnología como escáneres de barrido para captar escuchas de teléfonos y radios empleados por la policía y militares.

- Introducción en el comercio electrónico que permite ampliar su mercado al ofertar por Internet la venta de todo tipo de estupefacientes incluidas las últimas drogas de diseño como el *éxtasis*. Los consumidores pueden efectuar pedidos y son entregados a domicilio.
- Blanqueo de dinero: la banca electrónica permite abrir cuentas, transferir fondos y una movilidad anónima del capital sin parangón con la banca real.

Ciberocupas

Otro de los fenómenos que escapan a la larga acción de la justicia ha sido la disputa por la contratación de dominios en Internet. Se entiende por ciberocupas aquellos individuos o empresas que registran a su propiedad denominaciones de dominios asociados a marcas, empresas o servicios con la intención de obtener un beneficio revendiéndolo a su propietario legítimo. Una vez más se aprovecha el vacío legal existente. Ciertamente este se limita a un medio limitado de marcas y empresas y más difícil es cuando se refieren a otras denominaciones como apellidos o topografías. La situación está en vías de normalización ya que los tribunales progresivamente atienden las demandas planteadas por representantes de empresas y marcas registradas que solicitan el derecho a explotar por sí mismas esos nombres de dominio. En determinados casos se combina la ciberocupación y la compra fraudulenta de dominios como sucedió en el caso de Sex.Com que ha supuesto largos y costosos litigios para dirimir la propiedad de este dominio.

Cibersexo

El sexo siempre se ha asociado como uno de los negocios que mejor ha sabido adaptarse a Internet como lo demuestra el hecho de ser uno de los escasos negocios que son rentables realmente. La facilidad de acceso y el supuesto anonimato le han otorgado un mayor peso específico en el sector en detrimento de los sex-shops, los peep-shows, guía de contactos, videoclubes, etcétera. En nuestra exposición sólo mencionaremos aquellos aspectos polémicos o las prácticas fraudulentas que operan en este sector:

a) Pornografía infantil

Algunos expertos elevan su voz advirtiendo que la difusión de la pornografía en Internet ha supuesto un incremento de los ataques sexuales a menores de todo el mundo. El fácil acceso a contenidos o información de pedofilia sirve de acicate a determinados individuos a experimentar por sí mismos aquello que leen u observan en la Red y que en la era anterior a Internet podía estar reprimido o en estado "congelado".

Internet también sirve a pederastas la oportunidad de aproximarse a sus víctimas utilizando los servicios de Chat para ganar su confianza y dispuestos a contactar físicamente con ellos. La reprobación pública y la presión policial han transformado a estos grupos de individuos en una comunidad cohesionada, algo impensable antes de Internet, y en el que se intercambian todo tipo de argucias y consejos para evitar ser detectados.

Para las autoridades y organizaciones que combaten este fenómeno no es fácil afrontarlo ya que, por ejemplo, la edad legal de un infante puede ser distinta según la normativa de cada país. También existían vacíos legales que hacían más ineficaz la lucha policial, por ejemplo, hasta 1.999 Japón no aprobó una ley de prohibición de fabricación y distribución de material pornográfico.

b) Servicios de sexo.

La prostitución es el oficio más antiguo del mundo pero ello no obsta para que en la mayoría de los países sea considerada una actividad ilegal. Ello no

impide que desde cualquier directorio o buscador específico de sexo existan las habituales secciones de contactos o servicios. Una modalidad que sí que es propia del nuevo medio son las "Web Cam Girl" pionero en la implantación de las videoconferencias. Desde el punto de vista *oculto* de la red se constata el fenómeno de algunas adolescentes que han descubierto cómo el exhibicionismo puede reportarle ingresos y regalos. No hay que asociarlo necesariamente como un método de prostitución. Simplemente instalan una cámara en directo en su habitación y la conectan a la Red y desde la que ávidos internautas les sugieren acciones y situaciones que proponen previa "recompensa" en dinero o regalos.

d) Sex password

El sexo en Internet está altamente comercializado y abundan los servicios de pago y de acceso restringido mediante contraseñas e identificadores de usuario. La picaresca de los internautas ha desarrollado todo un sistema de intercambio de información para obtener las contraseñas y acceder a los servicios que ofrecen (imágenes, películas, Chats, webcams o relatos) de manera gratuita. No es difícil localizar directorios, foros, ni grupos de noticias de intercambio de contraseñas. Muchas de las empresas afectadas no son capaces de detectar el fraude con inmediatez y transcurren horas o días hasta que cancelan la contraseña vulnerada. Se trata de una información que requiere rapidez así que se han desarrollado directorios y buscadores exclusivos como [IPasssearch](#) o [Passwordsearch](#) que recopilan todas las páginas que facilitan este tipo de contraseñas con un nivel de actualización constante en horas. Ningún otro sector de servicios por Internet se ve tan perjudicado por este sistema y aunque pensemos por analogía que podría suceder idéntico fenómeno para otro tipo de servicios como suscripciones a servicios de noticias, periódicos o proveedores de bases de datos como *Dialog* no sucede en la misma proporción.

Paraísos fiscales e Internet

Las finanzas virtuales han traído consigo toda una serie de ventajas para individuos y corporaciones deseosos de pagar menos al fisco o su evasión total. Los motivos que Permiten que todo este proceso goce de cierta impunidad son:

- La facilidad que proporciona un medio como Internet para la transmisión de capitales y flujos financieros. El hombre del maletín cruzando la frontera ha quedado en el recuerdo. Esta opción permite contratar asimismo despachos y asesores legales en cualquier parte del mundo expertos en atender esta cuestión.
- El anonimato de las comunicaciones implica una cierta indeterminación para las autoridades a la hora de asociar una actividad o sesión en línea con la realidad física de la evasión o elusión de impuestos.
- Las autoridades financieras y gubernamentales no han regularizado este sector con la misma eficacia que en el sector real. Se configura así un área virtual donde la indefinición legislativa ampara este tipo de actividades.
- La presencia de paraísos fiscales no son un delito, especialmente cuando se realizan actividades de elusión fiscal, es decir, exprimir al máximo los recursos legales disponibles para pagar al fisco la menor cuantía posible o conseguir aplazarla en el tiempo. La evasión fiscal sí que puede tipificarse como delito que consiste llanamente en no pagar impuestos.

No existe impedimento para que usted contrate en el exterior todo tipo de servicios financieros o asesores económicos. En Internet es relativamente fácil obtener

prestaciones de esta naturaleza. Puede visitar portales especializados como [Lowtaxt.Net](#) que facilita noticias, información y directorio de servicios de asesoría ubicadas en estos paraísos fiscales en las secciones de finanzas o abogados. Otra opción es interrogar a buscadores genéricos ([Google](#), [AlltheWeb](#), [Yahoo!](#)) con términos como “offshore taxes”, “offshore services”, u “taxes heaven”. Una vez localizado y contratado un abogado, asesor o empresa –residente y con actividad legal en el paraíso fiscal- ésta realizará todos los trámites en su nombre: constituirá la sociedad, la inscribirá y la activará. Normalmente la persona encargada de toda esta burocracia de constitución es la que figurará como gestor de la nueva empresa, incluso puede ofrecerle nombres de consejeros y accionistas de paja que le permitirán mantener un anonimato absoluto. A partir de ese momento usted puede comenzar a operar con su capital garantizado por el secreto de la composición accionarial y registral que ofrecen estas sociedades.

Ciberestafas

Web Spoofing

Consiste en un técnica de engaño mediante el cual se le hace creer al internauta que la página que está visitando es la auténtica y fidedigna cuando en realidad se trata de una réplica exacta de la misma sólo que va a estar controlada y monitorizada por alguien hostil que pretende extraerle información. La víctima puede realizar todas sus operaciones habituales como en las páginas auténticas: podrá consultar los contenidos, navegar a través de enlaces, cumplimentar formularios y teclear contraseñas, códigos, números de cuenta corriente, números de tarjeta de crédito, etcétera.

El *ciberestafador* tiene dos alternativas: limitarse tranquilamente a seguir, vigilar, leer y grabar todas las actividades que realice el usuario o bien, manipular alguno de los datos que parten desde el usuario hasta el servidor con el que cree estar operando. Por ejemplo, en el caso de una venta por comercio electrónico, el *ciberestafador* puede modificar los datos de un pedido: nombre y domicilio a su favor, pero mantener el servicio de pago a la víctima.

Llamadas telefónicas

Uno de los sistemas de conexión a Internet es a través del dialer o marcador telefónico que establece la comunicación por este medio entre el módem del ordenador y el proveedor de Internet. Este proceso se realiza habitualmente mediante un nodo local de modo que la tarifa telefónica a pagar se corresponde a una llamada local. El fraude con este dispositivo consiste en desviar inadvertidamente la llamada de un nodo local a otros prefijos de tipo comercial mucho más caros.

El engaño más común parte de empresas suministradoras de contenidos de sexo que engañan al internauta prometiéndole acceso gratuito a todos los contenidos si previamente se baja de la red y activa un programa específico. Esta aplicación una vez está activada corta la comunicación telefónica con el proveedor habitual del internauta afectado y realiza una nueva llamada dirigida a un prefijo de la modalidad 906 que son mucho más caros.

Subastas en línea.

Otro lugar frecuentado por los *ciberestafadores* son los portales de subastas, ha adquirido tal dimensión que se sitúa en el primer puesto de la lista de fraudes en Estados Unidos. Desde estas páginas se ofrece toda una panoplia de productos y servicios. En algunos casos, el supuesto vendedor se limita a cobrar por el producto y no entregarlo nunca u ofrece un producto de marca que es una falsificación. Las empresas de subastas eluden su responsabilidad aduciendo que la operación final de la transacción es totalmente privada entre el vendedor y el comprador. Si usted está

dispuesto a comprar en uno de estos centros lo mejor es que acuda a aquellos portales que ofrezcan las mejores garantías de control sobre vendedores y productos. Así [eBay](#) se sirve de la ayuda de un software específico (Fraud and Abuse Detection Engine –FADE-), para detectar este tipo de fraudes, así es capaz de detectar subasta de productos a precios inusualmente bajos como es la venta de un coche a 1 dólar.

Medicamentos

En países como España la legislación prohíbe expresamente la venta de medicamentos por Internet y sólo está permitida en farmacias y centros sanitarios autorizados. A pesar de esta norma han existido casos de venta fraudulenta de determinados compuestos farmacológicos que ni si quiera tienen la aprobación gubernamental de considerarse como medicamento. El último caso de mayor impacto en los medios de comunicación es el de [Bio-Bac](#) donde se vendía como un compuesto antitumoral y regenerativo aplicable a enfermedades como Sida, hepatitis, cáncer o artritis. Una prohibición difícil de sostener en la red de redes donde una página de venta de medicamentos puede ubicarse en países con una legislación más permisiva o simplemente inexistente donde no sólo se puede adquirir sin receta médica medicamentos perfectamente legales (caso de la [Viagra](#)) sino también las sustancias dopantes. En este último caso las circunstancias se agravan porque existe una asociación entre doping y deporte pero también son sustancias empleadas con otras finalidades que generan problemas de sanidad pública como el engorde ilícito de ganado.

València,
05 de Noviembre de 2002
Ricardo Fornas Carrasco
Webmaster de [Buscopio](#) y [Métodos de Busca](#)

¹ **Nota:**

Si tiene dificultades con el vocabulario técnico empleado en este artículo puede aclarar dudas en http://www.ati.es/novatica/glosario/buscador/buscador_gloint.html