GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es

"Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad"

[Red.es]

MONOGRÁFICO PROTECCIÓN ANTE VIRUS Y FRAUDES

MONOGRÁFICO ANTE VIRUS Y FRAUDES

1. Objetivo del monográfico

«Sensibilizar sobre los riesgos para los menores asociados a los virus y fraudes en Internet, así como ofrecer recomendaciones, pautas y herramientas para su prevención y respuesta en caso de ser víctima de ellos».

2. Conceptualización y descripción del riesgo

Los virus y el fraude en Internet suponen un riesgo para todos los que hacen uso de la red, adultos y menores, profesionales y neófitos, usuarios que utilizan los recursos de Internet para estudiar o trabajar, o que simplemente buscan información y se relacionan con otras personas a través del ciberespacio.

La palabra “virus” se utiliza comúnmente para referirse a los programas informáticos que buscan alterar el funcionamiento de los dispositivos (ordenadores, tabletas, teléfonos móviles, etc.) y en muchos casos, robar información del usuario. Existen muchos tipos de programas maliciosos (virus, gusanos, troyanos) con diferentes objetivos, todos ellos perjudiciales. Estos programas maliciosos han ido evolucionando, volviéndose más sofisticados, más peligrosos, y más difíciles de detectar y combatir.

Por otro lado, el fraude electrónico suele ser mucho más sofisticado, y se basa en una actividad delictiva, que suele estar orientada a obtener un beneficio económico ilícito, y en algunos casos al robo de información, haciendo uso de dispositivos electrónicos y de Internet, todo ello combinado con tácticas de engaño en las que se trata de embaucar al usuario para que visite páginas web en las que se robará su información (*Phishing*), o instalando aplicaciones que supondrán un coste para el usuario (por ejemplo, suscripciones no autorizadas para el envío de mensajes *SMSPremium* con coste económico).

Nuevo paradigma del cibercrimen

Los primeros virus solían centrar su actividad encausar molestias y pérdidas al usuario:

- Corromper archivos.
- Borrar información.
- Impedir el uso de determinados programas.

- Obstaculizar el arranque del ordenador.

Desgraciadamente, la mayor parte de los virus actuales tienen un objetivo común: obtener información de los usuarios infectados:

- Datos bancarios.
- Números de tarjetas de crédito.
- Información personal.
- Fotografías.
- Contraseñas de acceso a correo electrónico y redes sociales.
- Uso de la webcam del usuario sin que éste sea consciente de que está siendo grabado.

Actualmente existen muchos programas maliciosos que permiten tomar el control absoluto del ordenador y realizar cualquier tipo de acción sin conocimiento del usuario, como por ejemplo:

- Suplantación de identidad y envío de correos electrónicos en nombre de la víctima.
- Utilizar el ordenador de la víctima para realizar ataques a otros ordenadores.
- Infectar a otros ordenadores para obtener información de sus usuarios.
- Realizar estafas en las que figurará el ordenador de la víctima (y su IP) como origen del delito.
- Enviar publicidad.

El riesgo es aún mayor en los dispositivos móviles, ya que estos virus pueden:

- Escuchar y grabar llamadas realizadas y recibidas en los teléfonos móviles.
- Enviar mensajes SMSPremium que incrementarán el coste de la factura.
- Obtener información de la posición geográfica del dispositivo mediante GPS.
- Hacer grabaciones con la cámara y tomar fotos sin conocimiento del usuario.

Y también están a la orden del día otros complementos como las barras de navegación que se instalan por defecto al instalar un programa, y que sin ser virus, obtienen

información no autorizada del usuario sobre sus hábitos de navegación, con el objetivo de mostrar publicidad relacionada.

Métodos de infección

Mientras que los primeros virus requerían la acción humana para su propagación (por ejemplo, ejecutando un programa infectado con imágenes), hoy día existen virus que no requieren de esta intervención. En algunos casos, la infección puede llevarse a cabo sin que el usuario sea consciente de ello, simplemente conectándose a una página web infectada, introduciendo un pen-drive USB, o abriendo un correo electrónico que contiene una imagen (aparentemente inocua), pero que realmente contiene código que se ejecuta de forma automática en el momento en que se visualiza dicha imagen.

Los virus informáticos se propagan de ordenador a ordenador, en muchas ocasiones sin la ayuda de una persona, aprovechando una vulnerabilidad del sistema operativo o del navegador para propagarse. Actualmente, los ciberdelincuentes aprovechan fallos de seguridad en *plugins* y aplicaciones que los usuarios utilizan habitualmente (por ejemplo, Adobe Flash Player, Java, Acrobat Reader, etc.). Otra estrategia muy habitual consiste en redirigir al usuario a páginas maliciosas a través de enlaces de chats y redes sociales, “invitando a ver un vídeo gracioso” o “fotos de famosas”. Lo más peligroso de los virus informáticos es su capacidad para replicarse, por lo que el ordenador de la víctima podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador enorme. Un ejemplo sería el envío de una copia de sí mismo a cada uno de los contactos de la libreta de direcciones del programa de correo electrónico.

Uno de los ejemplos más claros fue el virus *I love you*, que parecía ser un correo electrónico de un admirador, y al abrir el correo se auto-enviaba a los contactos de la agenda.

Ingeniería social

En los últimos tiempos ha tomado gran relevancia la Ingeniería Social, es decir, embaucar con engaños y manipulaciones a los usuarios para conseguir información que posteriormente será utilizada para llevar a cabo la infección y la sustracción de información (claves de acceso, contraseñas, etc.).

Hoy día son muy comunes las estrategias de engaño en las que se “invita” a la futura víctima a pulsar sobre un enlace que le llevará a una web fraudulenta en la que se intentará infectar su dispositivo (ordenador, tableta o teléfono), o se le solicitarán datos de

acceso a sus cuentas bancarias a través de correo electrónico, o incluso se le pedirá que introduzca su clave de usuario y contraseña, alegando un falso mantenimiento del servicio.

¿Y no me protege el antivirus?

Ningún antivirus es efectivo al 100%. El antivirus siempre va por detrás del código malicioso. Cada día surgen cientos de nuevos virus en Internet, y el tiempo que transcurre desde que el virus está activo hasta que un antivirus incorpora la información de cada nuevo virus en sus bases de datos, es un tiempo de riesgo y exposición al que todos los usuarios están expuestos.

Los laboratorios de los fabricantes de antivirus analizan cada día miles de patrones de código presuntamente malicioso. La detección de nuevos virus puede ser cuestión de horas o de días, y en ese periodo de tiempo se pueden infectar miles de ordenadores, tabletas y teléfonos.

En este punto, es importante destacar que algunos de los nuevos virus se ejecutan en memoria, sin que el archivo ejecutable se haya descargado en el disco duro (que es donde la mayoría de antivirus realiza el análisis). Conclusión: este tipo de virus son inmunes a los antivirus porque se ejecutan antes de que el antivirus pueda actuar.

Afortunadamente, los fabricantes de antivirus son conscientes de este peligro potencial y están trabajando para mejorar la efectividad de detección de sus productos, pero una vez más, el antivirus va por detrás, por lo que la prevención y el sentido común siguen siendo fundamentales en la navegación por Internet.

Perfiles de riesgo

En la actualidad existen virus para todas las plataformas y dispositivos, por lo que cualquier ordenador conectado a Internet es susceptible de ser infectado por un virus, independientemente de la plataforma (*Windows, Apple, Linux*) o el dispositivo (ordenador, tableta, teléfono móvil).

Ningún usuario que utilice Internet está exento de ser infectado. Aun haciendo un buen uso del sentido común, y evitando navegar por páginas web de dudosa reputación, cualquier internauta puede verse involucrado en una infección de virus procedente de una fuente confiable o de una web legítima. A continuación se indican distintas formas de posibles infecciones de virus:

- Un enlace propuesto por un contacto en *Facebook.*
- Un enlace recomendado en *Twitter.*
- Un enlace de *WhatsApp.*
- Un archivo adjunto en el correo electrónico.
- Un mensaje de *Spam* aparentemente inofensivo, que ejecuta un código malicioso al mostrar una imagen.

A estos riesgos, hay que añadir que los menores poseen ciertas características tales como inocencia, curiosidad, inexperiencia o impaciencia, que los pueden hacer especialmente débiles al potenciar los riesgos de infección y fraude.

Tipos de fraude online

El ciclo de vida de los fraudes electrónicos puede ser muy variado. En algunos casos, se estudian los hábitos de la víctima (especialmente a través de la redes sociales), y se busca ganar su confianza para eliminar protecciones (por ejemplo, se suele aconsejar desactivar el antivirus para que el ordenador vaya más rápido). En otros casos, se recurre a incluir cláusulas y condiciones en un lenguaje ambiguo y rebuscado antes de instalar un juego o programa, confiando en que el usuario aceptará las condiciones de instalación sin leerlas, especialmente, si se trata de un menor.

El retorno para el defraudador suele consistir en obtener un beneficio económico, o en robar información que posteriormente también puede ser utilizada para realizar chantajes.

***Rogues*: falsos antivirus**

Los *rogues* son un tipo de programa fraudulento que genera en el ordenador falsas alertas de virus a través de ventanas emergentes desde las que se advierte al usuario de que su sistema se encuentra infectado con un peligroso virus, ofreciéndole en la misma ventana la solución, que consiste en un enlace de descarga de un potente antivirus, capaz de eliminar el riesgo del virus que amenaza al usuario.

Una vez que se instala el falso antivirus, hace un primer chequeo del sistema en el que confirma la infección del peligroso virus, e incluso en ocasiones, recomienda la desinstalación del viejo antivirus.

La estafa consiste en invitar al usuario a descargar la versión completa del programa de protección, solicitando para ello el pago de cierta cantidad de dinero, especialmente, por medios poco seguros. Obviamente, no se trata de un antivirus real, y el resultado del análisis es totalmente falso[1].

Phishing

Es una actividad delictiva cuyo objetivo se basa en obtener de forma ilícita claves de acceso y contraseñas. Aunque su uso está muy extendido para obtener credenciales bancarias, el *phishing* también se utiliza para robar datos de acceso a correos electrónicos y redes sociales, servicios que utilizan habitualmente los menores.

Para ello, los cibercriminales copian una página web y mediante Ingeniería Social (normalmente, a través del correo electrónico), hacen creer a la víctima que está conectando a la web original, pero en realidad la conexión está siendo desviada a una web "copiada" exactamente igual a la original, en la que la víctima introducirá sus datos de acceso (que serán guardados por los ciberdelincuentes), y posteriormente (para no levantar sospechas) el usuario será redirigido de nuevo a la web original, con un mensaje indicando que el servicio no está disponible en ese momento.

[1] El Blog de Angelucho (2013) SEAMOS NUESTRO PROPIO CSI (II): Analizando un PHISHING
http://elblogdeangelucho.com/elblogdeangelucho/blog/2013/07/07/seamos-nuestro-propio-csi-ii-analizando-un-phishing/

Cuando el usuario vuelva a conectar a la web original podrá acceder sin problema y no sospechará, pero los datos de acceso ya estarán en manos ajenas que podrán acceder sin restricciones.

Un claro ejemplo son los ataques de *Phising* a través de Facebook, como el de "*sex sex sex and more sex*[2]" que consiste en mensajes que provienen de la red de contactos de la víctima, los cuales han sido infectados, y no saben que la invitación se realiza en su nombre. Estos mensajes contienen un enlace que redirige a una web maliciosa en la que se solicitan los datos de usuario y contraseña. Ejemplo de ello podemos encontrar en el caso de *phishing* "Vidas Infinitas" expuesto en el apartado "Casos reales".

Redes *Zombie*

Una red *zombie* es una red de ordenadores infectados que sin el conocimiento de sus propietarios legítimos están siendo controlados por un grupo de ciberdelincuentes de forma remota (desde cualquier parte del mundo con conexión a Internet), y que utilizan para realizar actividades fraudulentas: propagar virus, enviar correo basura (spam) y cometer otros tipos de delitos y fraudes. Los delincuentes consiguen comprometer esos ordenadores mediante la infección por virus, convirtiendo el dispositivo en un zombie que responde a sus órdenes. A su vez, los atacantes buscarán que la infección pase desapercibida durante el mayor tiempo posible para que el propietario del equipo no tome medidas al respecto. Entre los diferentes usos fraudulentos que éstas presentan podemos destacar los siguientes:

- Inicialmente, las redes *zombie* eran utilizadas para obtener ancho de banda de forma gratuita.
- Es habitual que una red *zombie* realice un ataque de miles de ordenadores intentando conectarse a la vez a una página web, que al no poder asumir el volumen masivo de peticiones de conexión, se viene abajo y deja sin servicio a los usuarios (denegación de servicio). Esta táctica se utiliza a veces entre empresas de la competencia en épocas de muchas ventas, para perjudicar al adversario (provocando la caída de su tienda en Internet) y así robarle clientes.

[2] Fuente: OS: (2009) Ataque de Phising a través de Facebook https://www.osi.es/es/actualidad/avisos/2009/08/ataque-de-phishing-trav%C3%A9s-de-facebook

- Envío masivo de *spam* (desde el correo electrónico de la víctima).

- Escribir comentarios en webs y blogs con mensajes publicitarios o enlaces a otras páginas para incrementar su presencia en *Google*. Es posible que en la firma de estos comentarios figure la dirección de correo electrónico de la víctima (lo cual, puede acarrear problemas legales).

- Existen redes *zombie* en dispositivos móviles que hacen valoraciones de las App en los *markets* con el objetivo de posicionar dichas App para aumentar el número de descargas.

- También existen redes *zombie* cuyo objetivo consiste en manipular encuestas, y robar información personal y credenciales (contraseñas de correo electrónico, claves de acceso a redes sociales, fotografías) para después comercializar con esta información en el mercado negro. Hay casos en los que se realizan intercambios de datos de tarjetas de crédito por ordenadores infectados pertenecientes a una *botnet (*red *zombie).*

Es habitual que estos robots estén alojados en ordenadores particulares, sin que sus dueños sean conscientes de ello, lo cual puede acarrear problemas legales, ya que en el ataque figura la dirección IP del ordenador infectado perteneciente a la red *zombie*, y el propietario es responsable de las actividades del ordenador. Será responsabilidad de éste demostrar que el ataque producido se ha realizado como consecuencia de una infección, lo cual puede conllevar un alto coste económico (abogados, peritos informáticos, etc.) y acciones penales.

SMSPremium

Existen aplicaciones fraudulentas para dispositivos móviles que envían mensajes *SMSPremium* desde el teléfono sin que la víctima se dé cuenta hasta recibir la propia factura. Además, existen otras aplicaciones con un nivel de sofisticación aún mayor, en las que se informa de que dicha instalación contempla el envío de mensajes *SMSPremium*. Esta información suele hallarse camuflada en el listado de condiciones que se debe aceptar antes de instalar una aplicación. Cuando se pulsa el botón y se acepta la instalación, se está dando consentimiento para que la aplicación envíe mensajes *SMSPremium* en nombre de la víctima, cuyo coste será cargado en su factura. Este tipo de fraudes se produce muy a menudo en la descarga de juegos, aprovechando la ingenuidad de los menores.

Se conocen casos en los que la futura víctima es etiquetada en un enlace de un video acompañado por un mensaje "¿Has visto qué bien sales en este vídeo?" Si el usuario pulsa el enlace, será redirigido a otra página web en la que debe introducir su número de teléfono. Si lo introduce, se estará suscribiendo a un servicio *SMS Premium*.

Fraudes asociados al mundo del videojuego

Tal como ya hemos podido comprobar, el fraude electrónico se basa en la ingenuidad y desconocimiento de los usuarios para llevar a cabo una estafa. En el caso de los menores, el riesgo es aún mayor, debido a su inocencia e ímpetu, y los cibercriminales se aprovechan de esta vulnerabilidad para llevar a cabo sus estafas poniendo el foco en puntos de atención del menor, como los videojuegos y las aplicaciones gratuitas.

Otro de los aspectos que aprovechan los ciberdelincuentes es el hecho de que muchos menores utilizan la misma clave de acceso y contraseña para distintos servicios (correo electrónico, redes sociales, etc.) lo que aumenta aún más el riesgo de robo de información personal cuando se es víctima de una estafa. [3]

Suscripciones ocultas y con coste

Incluir publicidad en los juegos gratuitos es una práctica habitual. Hay casos en los que al hacer clic en la publicidad de aplicaciones, el móvil envía el alta a servicios de pago sin que el usuario sea consciente de ello. De hecho, en algunos casos los *SMSPremium* no quedan registrados en el teléfono, pero sí que figuran en la factura.

Robo de datos del menor

La popularidad de los juegos (especialmente entre los menores) atrae a nuevos jugadores, y cómo no, también atrae a los ciberdelincuentes. Se han dado casos en los que se trataba de embaucar a los menores para que proporcionaran sus datos de acceso a *Facebook*, a cambio de "vidas infinitas".

[3] Fuente: Symantec (2014) Security 1:1 - Part 5 - Online gaming fraud, scam and phishing attempts. http://www.symantec.com/connect/articles/security-11-part-5-online-gaming-fraud-scam-and-phishing-attempts

Así, es fácil para los menores caer en la tentación de conseguir “trucos para pasar de pantalla” o “vidas infinitas” ofreciendo a cambio (y de forma ingenua) sus datos de acceso a redes sociales. Por eso, es aconsejable instruir correctamente a los menores para que no proporcionen ningún dato personal ni contraseña, a aplicaciones que estén fuera de la versión oficial del juego.

¿No te tienes que preocupar de los virus si tienes un Apple?

Existe desde hace tiempo una leyenda urbana que dice que los dispositivos Apple no se infectan con virus. Esto no es del todo cierto. Existe una gran cantidad de software malicioso y vulnerabilidades para los dispositivos Apple (Macintosh, iPhone, iPad y iPod).

A pesar de ello, el número de infecciones en dispositivos Apple es menor que en plataformas más extendidas como Windows principalmente porque el número de usuarios de Apple también es menor y porque los controles de calidad de aprobación de *software* son muy exhaustivos. No obstante, el número de amenazas en estos dispositivos se incrementa de forma exponencial con el aumento de usuarios de esta conocida marca.

Además, es conveniente tener en cuenta que una gran parte de los usuarios que consumen estos productos poseen un alto poder adquisitivo, lo que resulta muy atrayente para los ciberdelincuentes, que ven en estos perfiles de usuarios oportunidades de “estafa” y “negocio” muy rentables.

El riesgo de los dispositivos móviles

Hoy día, los dispositivos móviles se han convertido en los juguetes preferidos de muchos menores, y esta tendencia va en aumento. En un teléfono móvil se almacenan contactos, fotos personales, contraseñas de acceso a múltiples aplicaciones, documentos, grabaciones, y todo tipo de información personal.

La situación actual en referencia a virus y fraude electrónico es preocupante. Cada día se suben cientos de aplicaciones maliciosas a Google Play[4] (el *market* de aplicaciones Android) y aunque la mayor parte se ubican en India y China, ningún país se queda al

[4] Fuente: Un Informático en el lado del mal. Blog sobre seguridad informática. (2014) Android: Apps maliciosas en Google Play http://www.elladodelmal.com/2015/03/android-apps-maliciosas-en-google-play.html

margen del riesgo que esto supone. La mayor parte de estas aplicaciones son juegos y aplicaciones de ocio, destinadas a infectar los dispositivos, a robar información, y en muchos otros casos, a enviar publicidad en nombre de terceros o a actuar como cebo para realizar estafas *online*.

Por otro lado, aplicaciones como *Facebook*, *Twitter*, *Whatsapp*, *Line* o *Snapchat* son utilizadas a diario por los menores en sus dispositivos móviles, y los ciberdelincuentes se aprovechan de estos entornos para conseguir que sus enlaces a webs fraudulentas, documentos infectados y otros fraudes, tengan una gran viralidad y lleguen al máximo de usuarios.

Los dispositivos móviles son altamente vulnerables a las amenazas de Internet, en algunos casos (como Android) mucho más que los ordenadores, ya que los usuarios de tabletas y teléfonos no están acostumbrados a instalar antivirus en sus dispositivos, y cada vez existen más aplicaciones fraudulentas destinadas a robar información (fotografías, contactos, contraseñas, etc.) y a realizar actividades delictivas, como por ejemplo, pasar a formar parte de redes *zombie* que ejecuten procesos de publicidad masiva, o visitas a páginas web "sospechosas" para aumentar el posicionamiento.

En este punto, es necesario destacar el alto riesgo que conlleva descargar aplicaciones de las páginas web no oficiales, pues no suelen contar con controles de calidad demasiado exhaustivos y son foco de infección de virus y programas maliciosos, que pueden robar información y realizar suscripciones a servicios SMS Premium.

Para una persona con determinados conocimientos informáticos es relativamente fácil conseguir acceder al control total de un ordenador y de toda la información que contiene, (utilizando distintas variantes de ingeniería social para conseguir claves de acceso a los servicios que los menores utilizan regularmente -redes sociales, chats-). No obstante, el riesgo es aún mayor en los dispositivos móviles actuales como tabletas y teléfonos.

Pero sin duda, uno de los aspectos más preocupantes son las cláusulas y condiciones ambiguas que los usuarios aceptan (sin leer los detalles) cuando acceden a comprar puntos o vidas infinitas a través de un juego o aplicación.

¿Por qué hay más aplicaciones fraudulentas en Android que en Apple?

Tal y como se indica a continuación, existen varias razones por las que unos *markets* son más seguros que otros.

Mientras que en Apple Store no se publica una aplicación (APP) hasta que ha pasado un control de calidad y se ha certificado que no contiene código malicioso, en Play Store se puede publicar y conseguir que esté disponible en pocos minutos desde cualquier parte del mundo. Google realiza verificaciones de *software* posteriormente, y debido al gran volumen de las mismas, una aplicación puede estar disponible durante semanas, e incluso meses, sin haber sido comprobada.

Otra de las razones se basa en las diferencias de coste que tiene publicar las aplicaciones en los *markets*.

- Coste para publicar una aplicación para Apple: 99€.
- Coste para publicar una aplicación para Android: 0€/año.
- Coste para publicar una aplicación para Windows Phone: 75€.

Afortunadamente, se está trabajando en la creación de mecanismos de seguridad para investigar y mitigar la puesta en circulación de aplicaciones fraudulentas. Prueba de ello es la empresa Eleven Paths (filial de Telefónica), que ha creado una aplicación que permite analizar y detectar posibles fallos de seguridad en las aplicaciones Android alojadas en Play Store.

3. Datos de situación y diagnóstico

Hábitos de seguridad en los hogares con menores

El «Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles» (Inteco, 2012), elaborado sobre una muestra de 869 hogares, analiza los hábitos de seguridad en los hogares con menores que utilizan Internet. Las medidas contempladas se agrupan en tres categorías en función del tipo:

Medidas coercitivas y de control

El estudio confirma un aumento continuado en la concienciación de los progenitores respecto a la supervisión del uso que sus hijos hacen de Internet. Prácticamente la totalidad de los encuestados no permite que el menor realice compras o proporcione datos bancarios (95,2%). También una amplia mayoría vigila y limita el tiempo en que su hijo utiliza Internet (85,1%), además de haber ubicado el ordenador con el que éste accede a la red en un lugar común a la vista de todos (82,9%).

El hábito menos seguido por los padres es el de crear una cuenta con permisos limitados para el menor (43,1%). Aun así, su uso aumentó ligeramente respecto a fechas pasadas.

Medidas de comunicación, diálogo y educación

También se observa un aumento continuado en la labor que realizan los padres para concienciar a los menores sobre un uso seguro de Internet. Se les preguntó a los progenitores por tres cuestiones: si los responsables del menor les advierten de los problemas de facilitar información propia o relativos a personas de su entorno familiar, si se le informa acerca de las amenazas de Internet, y si se le ha pedido al menor que les informe de cualquier contacto o conducta sospechosa.

Las tres prácticas analizadas son seguidas por nueve de cada diez padres siendo en todos los casos mayor que en fechas anteriores. En este sentido, la medida que mayor crecimiento experimentó es la de informar al menor sobre las amenazas que acechan en la red.

Medidas de implicación de los padres en la navegación del hijo

Cada vez son más los padres que se preocupan por las noticias relacionadas con la seguridad de los menores (89%). También se observó una gran preocupación en lo referente a los contactos en línea (77,7%) y en conocer el nick y el perfil que usa el menor en chats y redes sociales (70,9%).

Los datos anteriores contrastan con los que apuntan a que dos de cada tres padres confían en su hijo permitiendo que navegue sin su supervisión (65,9%). Por último, cabe destacar que sólo uno de cada cuatro padres consideraba posible que sus hijos accedieran a contenido inadecuado (pornografía, violencia, racismo, etc.).

Medidas de protección en los hogares

Por otro lado, según el “Estudio sobre la Ciberseguridad y Confianza en los hogares españoles” (Red.es 2015) el 82% de los equipos informáticos están protegidos con software antivirus. En el estudio queda reflejado que las medidas de seguridad con mayor presencia real en los equipos informáticos españoles son los programas antivirus o antimalware (82%) y los cortafuegos (79,4%).

El número de usuarios que hace uso de las contraseñas para proteger sus equipos es del 58,2%, así como la eliminación de archivos temporales y cookies (52,9%), o la realización de copias de seguridad de los archivos (40,4%).

El riesgo de ordenadores equipados con Windows XP es altísimo, ya que prácticamente se utiliza cuentas con permisos de administrador (que permiten realizar todo tipo de acciones en el equipo). En sistemas operativos posteriores, el uso de cuentas de administrador se reduce al 28,5% en Windows 7, 13,2% en Windows Vista y al 8% en el caso de Windows 8. Esto es así por la configuración que traen por defecto las distintas versiones. Estos problemas de seguridad irán remitiendo a medida que los usuarios vayan migrando a las nuevas versiones de sistemas operativos.

Solamente el 8,2% de los usuarios declara, hacer uso de software de cifrado en su terminal móvil, para proteger la información que contiene en caso de pérdida o robo.

Incidentes de seguridad en los hogares

El spam sigue siendo la incidencia más común que sufren los internautas (85%), mientras que las relacionadas con virus y malware son declaradas únicamente por un 31,7% de aquellos usuarios que han sufrido incidencias de seguridad.

No obstante, la situación real es más negativa, ya que se ha detectado alrededor de un 60% de ordenadores infectados por *malware.* Esta situación sigue una tendencia ascendente, que indica que los programas maliciosos son cada vez más sofisticados y consiguen esquivar con mayor facilidad a los programas antivirus.

Las principales incidencias relacionadas con los menores se basan en haber facilitado información personal (14,3%) a desconocidos, y el acceso a contenidos de carácter sexual (11,9%).

A pesar del número de usuarios que potencialmente tiene su red inalámbrica expuesta, un porcentaje mínimo (solo el 1,7%) sospecha haber sufrido una intrusión en su red.

Sólo el 1,7% de los usuarios sospecha haber sufrido una intrusión en su red wifi, a pesar del alto número de usuarios que tiene expuesta su red inalámbrica (16%).

En referencia a las consecuencias de los incidentes de seguridad, es necesario destacar que el 48% de los usuarios ha sufrido alguna vez un intento de fraude electrónico. La relación de estos fraudes con el comercio electrónico o loterías, casinos y juegos online ronda el 27% de las ocasiones. En general, estos tipos de fraude se rigen por manejar pequeñas cantidades de dinero, con el objetivo de evitar la consideración de delito según el código penal. De este modo, el 65,5% de los fraudes online y el 79,5% de los telefónicos no superaron los 100 euros.

Confianza en el ámbito digital de los hogares españoles

El grado de confianza de los usuarios en el uso de Internet es elevado: un 45,3% confía en gran medida en la red, mientras que solo un 1,4% desconfía totalmente. De este modo, un 46% de los encuestados considera Internet como una red más segura cada día, y un 72,3% estima que sus dispositivos están razonablemente protegidos.

La gestión que menos confianza genera entre los entrevistados es el pago a través de Internet utilizando la tarjeta de crédito/débito (sólo un 33,4% de los usuarios). Existe un alto porcentaje de usuarios (44%) que tiene poca o ninguna confianza a la hora de facilitar sus datos personales mediante un e-mail o un servicio de mensajería instantánea. La mayor tasa de confianza se presenta al facilitar datos en un organismo público de forma presencial (46,4%), o bien a través de portales de organismos públicos (41,2%).

4. Ejemplos de casos reales

En este apartado se mostrarán a modo de ejemplo algunos casos reales, con el objetivo de acercar al lector a una realidad que para muchos aún es desconocida, y que supone un riesgo potencial para adultos y menores en relación con la infección de los virus actuales y la exposición de menores a las distintas estrategias de fraude electrónico.

La linterna molona

La estafa comienza con un anuncio a través de Facebook, en el que se publica un post sobre una aplicación para Android, que supuestamente ofrece una linterna molona[5] para el móvil que "...hace brillar el led más que ninguna otra aplicación de linternas y totalmente gratuita...".

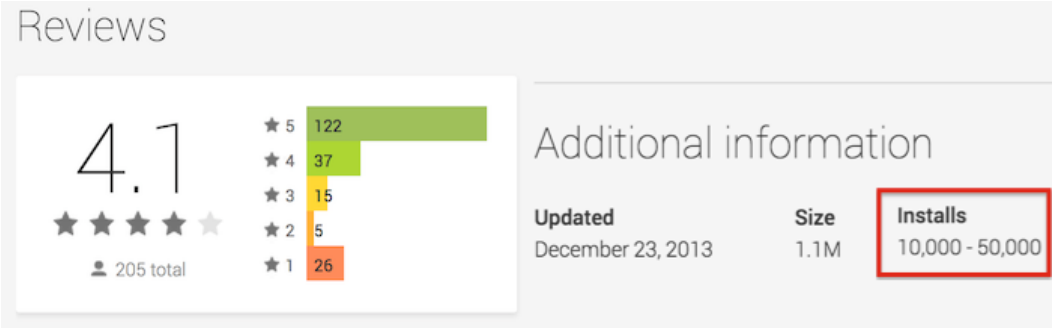
Para descargarse la aplicación supuestamente no existe ningún servicio que pueda acarrear coste alguno. Sin embargo, nada más ejecutarse, esta aplicación lee el número de teléfono de la víctima, se conecta a Internet, y lo da de alta en una página de servicios ofrecidos vía mensajes SMS. Una vez que queda confirmada la suscripción (el operador de telefonía supone que ha sido el usuario, y no una aplicación maliciosa en el terminal

[5] Fuente OSI (2015) Linterna HD. Más luz en tu Smartphone, menos en tu monedero https://www.osi.es/es/actualidad/avisos/2015/02/linterna-hd-mas-luz-en-tu-smartphone-menos-en-tu-monedero

móvil por su cuenta) se ha autorizado al proveedor de servicios a enviar mensajes SMS con coste, que serán cargados en la factura de la víctima.

Y aún hay más: para conseguir la "viralización" del negocio, si está instalada la aplicación de Facebook en el terminal Android, la "linterna molona" publica en el nombre de la víctima un post contando las virtudes de la famosa linterna para que los amigos también la prueben.

La aplicación fue retirada de Play Store, en los foros tenía quejas de usuarios, pero después de superar más de 10.000 descargas. Aún está disponible en algunas páginas en la caché de Google (y con muy buena valoración de la misma)



Fuente: www.elladodelmal.com

Find&Call

Esta aplicación[6] para iPhone robaba toda la agenda de contactos desde el terminal (además de la información GPS) sin notificar nada a los usuarios, y usaba los datos de la agenda para hacer campañas de *spam* por SMS. La aplicación no solo estaba publicada en Apple Store, sino que también era posible detectarla en Play Store en su versión para Android, y tanto Google como Apple ya han decidido eliminarla de la lista de aplicaciones disponibles.

[6] Fuente: Seguridad Apple (2012) Malware en la App Store: Find and Call. http://www.seguridadapple.com/2012/07/malware-en-la-app-store-find-and-call.html

Vidas infinitas

Hace unos meses se descubrió un fraude orientado a robar datos personales de los usuarios de un famoso juego, llamado *Top Eleven Be a Football Manager*[7], que tiene más de 10 millones de seguidores en *Facebook*. Fue su popularidad lo que hizo que los ciberdelincuentes lo utilizaran para robar datos personales de sus usuarios.

El *malware* (o programa malicioso), actuaba disfrazado de aplicación, ofreciendo ganar puntos para el juego con los que comprar jugadores. Evidentemente, esta era estrategia para conseguir los datos de acceso de la cuenta de correo electrónico o de Facebook de la víctima.

La estafa para conseguir puntos gratis para el *Top Eleven* se realizaba del siguiente modo:

- El usuario descarga la *App* desde diferentes foros sobre juegos.
- Para conseguir el número de *tokens* seleccionados, se debe insertar una cuenta de correo electrónico o de Facebook y la contraseña de acceso.
- Esos datos son enviados a los ciberdelincuentes, que los utilizan para hacerse con el control de la cuenta, impidiendo al usuario el acceso a la misma.

Invitaciones desde Facebook

Esta estrategia también está muy extendida:

[7] Fuente: Panda Security (2014) Se descubre un estafa para el juego 'Top Eleven Be a Football Manager'. http://www.pandasecurity.com/spain/mediacenter/noticias/estafa-para-top-eleven-football-manager/

1. El estafador crea una cuenta falsa en Facebook[8], envía solicitudes de amistad a personas que encajen en el perfil de sus víctimas, y realiza publicaciones atractivas e interesantes para sus nuevos e ingenuos amigos.

2. El usuario víctima pulsa sobre el enlace de la publicación que le llevará a una web en la que podrá descargar juegos, programas gratis, ver fotos de famosas o comprar artículos con descuentos increíbles.

3. Cuando el usuario accede a la web maliciosa, automáticamente se hace un chequeo de la versión de navegador que utiliza, de los *plugins* instalados y sus posibles vulnerabilidades.

4. A partir de aquí, las infecciones pueden ser de todo tipo:

    a. Instalación de programas maliciosos (virus, troyanos, etc.).

    b. Instalación de *Adware* (barras de herramientas, molestas ventanas Emergentes, etc.).

    c. Robo de agenda de contactos.

    d. Robo de direcciones de correo electrónico para incluir en listas de correo, que posteriormente serán vendidas a empresas generadoras de *Spam.*

[8] OSI (2012) : Conoce los fraudes utilizados en Internet II: los SMS Premium. https://www.osi.es/es/actualidad/blog/2012/07/05/conoce-los-fraudes-utilizados-en-internet-ii-los-sms-premium

Webcam controlada desde otro ordenador

Cuando un virus toma el control de un ordenador[9], puede llevar a cabo todo tipo de acciones sin que el usuario sea consciente de ello, y una de esas acciones consiste en que el atacante grabe al usuario con su propia *webcam* (sin que el usuario se dé cuenta) y posteriormente, publique las imágenes íntimas, o peor aún, que trafique con ellas en la *Deep Web* (una red paralela y oculta de Internet, que sirve de refugio para la delincuencia, debido al contenido ilícito que se encuentra en ella, y en la que se trafica con todo tipo de información).

Una aplicación para espiar conversaciones de *Whatsapp*

En junio de 2013 fue detenido un joven de 23 años, responsable de haber creado la aplicación *WhatsappSpy*, a través de la cual, las víctimas eran suscritas a un servicio de mensajes *SMS Premium*, lo que permitió al estafador ganar más de 40.000€.

El timador comenzó a hacer publicidad en las redes sociales sobre una supuesta alternativa para leer las conversaciones de otros contactos. Los incautos usuarios introducían en la aplicación su número de teléfono para descargar la aplicación, y se les cobraba entre 1,5 y 7€, dependiendo del operador.

[9] Fuente: El diario (2013): ¿Me pueden espiar desde la webcam?. http://www.eldiario.es/turing/webcam_hackers-RAT_0_111989089.html

Al ser un importe pequeño, las autoridades reconocen que apenas ha habido denuncias, pero lo cierto es que puede haber más de 11.000 afectados. El joven timador también se aprovechó de sus víctimas robando los datos de acceso a sus cuentas sociales para ser utilizados después con el fin de hacer publicidad de la aplicación[10].

Virus de la Policía

El virus de la policía es uno de los r*ansomwares* más extendidos en los últimos años. Este virus, que está activo desde 2011, "secuestra" todos los archivos del ordenador, argumentando que el usuario ha estado navegando por páginas web pornográficas con contenido infantil, y pide "como multa" 100 € para liberar la información. Es un virus muy sofisticado que actúa en varios países, y en cada país muestra imágenes de los cuerpos de seguridad nacionales, con objeto de dar más veracidad al mensaje. A día de hoy sigue estando activo, e infecta miles de dispositivos diarios[11] en todo el mundo.

Las últimas versiones del "virus de la policía" muestran a la víctima, en la pantalla de su ordenador, una fotografía tomada minutos antes con su propia *webcam*.


ABC.es | ESPAÑA

ACTUALIDAD DEPORTES CULTURA VIAJAR GENTE&ESTILO TV VIDEO SALUD BLOGS HEMEROTECA SERVICIOS TE

España Internacional Economía Sociedad Toros Madrid Local Ciencia Familia Defensa Opinión HoyCinema GuíaTv ABCfoto Casa Real Buscar

TOROS Sigue en directo la reaparición de El Soro en la Feria de Fallas

ESPAÑA

Atención al virus informático de moda: «Policía Nacional, páguenos 100 euros»

ABC.ES / MADRID | Día 03/05/2013 - 09.52h

Publicidad

Fuente: Periódico ABC (2013)

[10] Fuente: OSI (2013) ¡Las llamadas "gratuitas" de Whatsapp pueden salirte muy caras! https://www.osi.es/es/actualidad/avisos/2015/03/las-llamadas-gratuitas-de-whatsapp-pueden-salirte-muy-caras

[11] Fuente:Infospyware (2014) El ransomwareKovter, el virus de la policía infecta 44.000 dispositivos por día http://www.forospyware.com/t492003.html

5. Estrategias, pautas y recomendaciones para su prevención

Mantener software actualizado

Cada día surgen nuevas vulnerabilidades, por lo que es fundamental mantener actualizado[12] todo el software instalado, el sistema operativo, el navegador de Internet y el antivirus[13] en todos los dispositivos (ordenadores, tabletas y teléfonos móviles).

Los fabricantes y desarrolladores de software trabajan cada día por mejorar las aplicaciones y por solucionar vulnerabilidades que permitirían a un atacante realizar acciones peligrosas en el equipo. El objetivo principal de las actualizaciones consiste en mejorar sus funcionalidades y proteger su seguridad.

Cualquier software es susceptible de contener fallos de seguridad, en función de sus propios componentes, o de componentes de terceros que a menudo se instalan de forma complementaria en forma de extensiones (*plugins*), y que son necesarios para su funcionamiento (por ejemplo, Java para visualizar gráficos y utilizar juegos, extensiones de Adobe Flash Player para visualizar videos, Adobe Acrobat Reader para ver archivos en formato PDF, etc.).

Por ello, es recomendable establecer el modo de actualización automática en todos aquellos programas que lo permitan (por ejemplo, el sistema operativo Windows), de forma que las actualizaciones se instalen en el mismo momento en que el sistema detecte que están disponibles. De este modo, se evita que el usuario tenga que estar pendiente de instalar las actualizaciones, y el sistema estará menos tiempo en situación de riesgo.

Así mismo, existen herramientas como PSI (Personal Software Inspector), que recopila el software que está instalado en el sistema y alerta de las aplicaciones que no están actualizadas. De este modo se cubren aquellas aplicaciones que no poseen un sistema de actualizaciones automático.

[12] Fuente OSI (2015) Actualizaciones de seguridad. https://www.osi.es/es/actualizaciones-de-seguridad
[13] Fuente OSI (2015) Recursos gratuitos. http://www.osi.es/es/herramientas-gratuitas%20?herramienta_selec%5b%5d=22

Precauciones

Hay sitios de Internet que ofrecen la instalación de actualizaciones falsas, y al aceptarlas, el equipo quedará infectado, por lo que no se debe instalar ninguna actualización que no provenga de los canales oficiales que proporcionan los fabricantes de los dispositivos o desarrolladores de software.

Otra situación que se debe tener en cuenta es la instalación o actualización de una aplicación que necesita ciertos privilegios para funcionar correctamente (esto es especialmente delicado en dispositivos móviles). Es recomendable revisar los privilegios que se concederán, antes de realizar la instalación, para evitar que programas maliciosos puedan tomar el control del dispositivo.

Por lo tanto, sólo deben instalarse aplicaciones provenientes de fuentes de confianza, y revisar los privilegios por si fuesen excesivos o innecesarios para el propósito al que están destinados.

Recomendaciones técnicas

Todas las precauciones son pocas para evitar infecciones de virus y para no ser víctima de un fraude electrónico. A continuación se describen algunas recomendaciones técnicas a modo de prevención:

- **Mantener actualizado todo el *software* instalado, el sistema operativo, el navegador de Internet y antivirus:** es fundamental contar con un antivirus actualizado en todos los dispositivos (ordenadores, tabletas y teléfonos móviles).

  La Oficina de Seguridad del Internauta (OSI) dispone de un repositorio de herramientas gratuitas desde donde descargar antivirus: https://www.osi.es/es/herramientas-gratuitas

  Para más información sobre actualizaciones de software consultar: https://www.osi.es/es/actualizaciones-de-seguridad

- **Contar con cuentas de usuario limitadas** para cada una de las personas que utilizan el equipo compartido con contraseñas personales para regular el acceso a éste. De esta forma, cada usuario podrá tener su propio escritorio -con aquellos archivos y carpetas a los que pueda acceder- de forma que tan solo el usuario administrador, con permiso para poder administrar las diferentes cuentas, pueda instalar aplicaciones o modificar aspectos importantes de la configuración. Así, se

minimiza el riesgo de infección por virus y, por tanto, del robo de contraseñas de los servicios.

Para obtener más información sobre cuentas de usuario y su configuración, consultar: www.osi.es/es/cuentas-de-usuario

- **Realizar copias de seguridad[14]:** las copias de seguridad permiten recuperar la información en caso de que un virus infecte un dispositivo, y deben realizarse en dispositivos externos (unidades de almacenamiento, discos duros, etc.). Los sistemas operativos actuales permiten establecer puntos de restauración y recuperación de la información, tanto en ordenadores como en dispositivos móviles.

  Para obtener más información sobre copias de seguridad, consultar: http://www.osi.es/es/copias-de-seguridad-cifrado

- **Gestión de contraseñas**: las contraseñas deben ser secretas, robustas y no repetidas.

  - **Secretas**. La fecha de nacimiento no es una contraseña secreta para las personas que del entorno (familiares, amigos, compañeros de clase). Es muy importante transmitir esta recomendación a los menores, acostumbrados a compartir las claves con amigos. Si se produce una enemistad, la otra persona tendrá acceso a toda su información.

  - **Robustas**. "1234" o "qwerty" no son contraseñas robustas. Es conveniente utilizar combinaciones de mayúsculas, minúsculas, números y símbolos de puntuación, con una longitud mínima de 8 caracteres, y evitar palabras conocidas y nombres propios.

  - **No repetidas**. Utilizar la misma contraseña para el correo electrónico, para acceder a las cuentas bancarias, y para acceder a las redes sociales, significa estar poniendo en riesgo toda la información en caso de que alguien descubra (o robe) la contraseña.

[14] Fuente OSI (2015) Copias de seguridad y cifrado. http://www.osi.es/es/copias-de-seguridad-cifrado

Uno de los problemas de utilizar claves demasiado simples, es que existen programas diseñados para probar millones de contraseñas por minuto.

La OSI ofrece varias técnicas para crear contraseñas robustas y seguras: https://www.osi.es/es/contrasenas

- **Claves WIFI:** las contraseñas de las claves WIFI de los *router* deben configurarse para ser cambiadas periódicamente para evitar que otros usuarios puedan hacer uso de ellas sin autorización. En internet hay programas que permiten descifrar algunas claves WIFI en cuestión de minutos, y no son difíciles de utilizar, por lo que si no configuramos adecuadamente el *router* cualquier vecino (con unos mínimos conocimientos de informática) puede descifrar una clave WIFI en cuestión de minutos.

  La OSI ofrece una serie de pautas para asegurar la conexión WIFI de casa. https://www.osi.es/es/actualidad/blog/2015/03/09/aprende-asegurar-tu-wifi-en-7-pasos?origen=boletin

- Es importante educar a los menores para que tomen precauciones al utilizar **ordenadores públicos y al conectarse a redes WiFi públicas**. Por eso nunca se debe utilizar redes WiFi no confiables para acceder a servicios donde se intercambie información sensible o un componente importante de privacidad.

Guía de Buenas Prácticas

Además de lo anterior, resulta interesante que conozcamos la siguiente guía general de buenas prácticas preventivas ante virus y fraudes:

- **Precaución con los enlaces cortos antes de acceder a ellos**: los enlaces cortos, empleados especialmente en pantallas móviles para ahorrar en caracteres, se configuran como un caldo de cultivo perfecto para ataques de *phishing*, ya que el usuario no sabe hacia dónde apunta el enlace. Es conveniente desconfiar de los enlaces cortos cuando en páginas de dudosa credibilidad, o en comentarios de noticias y foros.

- **Descargar los programas solo de las páginas oficiales.** Para evitar la instalación de programas manipulados maliciosamente se recomienda descargarlos únicamente de sus páginas oficiales.

- **Ten cuidado con las preguntas de seguridad:** Algunos servicios ofrecen la opción de utilizar preguntas de seguridad para que, en caso de olvido, sea posible recuperar la contraseña. No obstante, algunas respuestas a estas preguntas pueden ser conocidas por personas del entorno. Por ejemplo: ¿Cómo se llama tu mascota? Por esta razón, no es recomendable utilizar preguntas de seguridad con respuestas obvias. Es conveniente establecer respuestas complejas que no puedan ser averiguadas por personas cercanas[15].

- **Evitar la navegación por páginas web sospechosas** (programas gratis, juegos gratis, fotos de famosas, etc.).

- **Configurar adecuadamente la privacidad en las redes sociales.** Para ampliar información, consultar el monográfico “Gestión de la privacidad e identidad digital”.

- **Evitar introducir en los equipos medios de almacenamiento extraíbles de dudosa procedencia.** Estos dispositivos se conectan vía USB y pueden ser una puerta de entrada para los virus.

Prevención en el hogar

Las herramientas de Control Parental pueden suponer una gran ayuda para los padres a la hora de evitar que los menores puedan verse involucrados en fraudes electrónicos e infecciones de virus.

Configurar adecuadamente estas herramientas ayudará a prevenir la instalación de aplicaciones infectadas, ya que estableciendo las restricciones adecuadas, se impide que el menor pueda realizar acciones que puedan poner en riesgo la información del dispositivo. Por otro lado, también se podrá evitar el uso no autorizado de la cámara de fotos, el envío de mensajes, o la realización de llamadas.

Estas herramientas también ayudan a controlar y a filtrar la navegación por Internet de los menores, tanto en ordenadores como en tabletas, ya que se pueden establecer

[15] Oficina de Seguridad del Internauta (OSI) (2014) https://www.osi.es/es/contrasenas

restricciones para que no se pueda navegar por sitios web potencialmente peligrosos que pueden contener virus y otros programas maliciosos[16].

Consejos sobre la instalación de aplicaciones en dispositivos móviles

- Descargar aplicaciones sólo desde fuentes confiables.
    - Play Store para Android.
    - Apple Store para IOS.
    - Marketplace para Windows Phone.
- Sospechar ante un número bajo de descargas.
- Desconfiar si los comentarios son excesivamente halagadores, pues pueden estar escritos por el propio desarrollador o personas de su entorno.
- Comprobar los permisos de acceso al teléfono que se solicitan antes de iniciar la instalación. Por ejemplo, una aplicación de linterna no tiene sentido que requiera permisos para acceder al registro de llamadas.
- Desactivar en los dispositivos móviles la opción Permitir Orígenes Desconocidos ubicada en Ajustes -> Seguridad -> Orígenes desconocidos.
- Instalar un antivirus para dispositivos móviles.
- No utilizar navegadores extraños, ya que pueden contener vulnerabilidades que permitan “a los malos” robar las contraseñas.

Desgraciadamente, existen cientos de aplicaciones fraudulentas para dispositivos móviles. Los principales *markets* de aplicaciones disponen de procedimientos de control de calidad y políticas de seguridad que no son efectivos en todos los casos, y que varían en función de la plataforma (Android, IOS, Windows Phone).

[16] Software para Protección de menores (2014) www.controldeinternet.com

En la plataforma Play Store de aplicaciones para dispositivos Android existen aplicaciones fraudulentas como "*Exprime tu Whatsapp*" o "La linterna molona", que suscriben a sus víctimas a servicios de pago con solo leer los *SMS* y hacer el registro vía web. Play Store analiza periódicamente las aplicaciones subidas al *market* por los desarrolladores, y retira aquellas que hacen un uso fraudulento o que incorporan código inseguro. A pesar de ello, la gran cantidad de aplicaciones que se suben al *market* a diario complican enormemente las tareas de análisis, lo cual repercute en la seguridad de los usuarios que descargan las aplicaciones.

Por su parte, los controles de calidad en Apple Store son muy estrictos. Los terminales iPhone o iPad con sistema operativo IOS cuentan con muchas protecciones contra aplicaciones no deseadas en la Apple Store. No obstante, se cuelan de vez en cuando aplicaciones maliciosas o simplemente estafas. A continuación se muestra un listado de aplicaciones falsas que simulan funcionalidades similares a Whatsapp[17]:

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
</table>

[17] Redeszone (2014). Las web falsas para hackear WhatsApp aumentan exponencialmente http://www.redeszone.net/2014/08/11/las-web-falsas-para-hackear-whatsapp-aumentan-exponencialmente/

Prevención en centros de enseñanza

Los centros de enseñanza deben contar con mecanismos que faciliten la monitorización del uso que hacen los menores en Internet, y con la posibilidad de establecer restricciones de acceso a las web que puedan resultar potencialmente peligrosas por el riesgo a infección de virus (por ejemplo, descarga de juegos, descarga de programas pirata, visualización de vídeos violentos, descarga de fotos de famosos/as).

Los métodos más apropiados son los sistemas de listas blancas. Un sistema de lista blanca sólo permite que los menores se conecten a determinadas páginas web a las que se ha concedido permiso de conexión, y el resto de páginas web serán inaccesibles.

Por ejemplo, en las aulas de Informática de un centro de enseñanza se puede permitir el acceso a páginas web relacionadas con la educación: www.wikipedia.org, www.mundoprimaria.com, www.matematicas.net. Cualquier página web que no figure en la lista blanca no estará disponible.

En la actualidad existen sistemas de restricción y monitorización de Internet para controlar el uso de menores en Internet, pero algunos sistemas están obsoletos o no son lo suficientemente seguros.

Los jóvenes de hoy en día tienen una gran capacidad para encontrar trucos que les permitan saltarse estas restricciones (por ejemplo, cambiar el rango de IP o “crackear” la WIFI del colegio), por lo que resulta recomendable contar con el asesoramiento de personal especializado en Seguridad Informática, que se encargue de establecer mecanismos seguros de uso y acceso a Internet.

Este tipo de restricciones de acceso ayuda a los educadores a afianzar la protección de los menores en el uso y aprendizaje de las nuevas tecnologías. No obstante, durante las actividades que requieran el uso de Internet en clase, es conveniente establecer mecanismos de monitorización que permitan la supervisión de la actividad en Internet de los estudiantes[18].

También señalar que los centros educativos tienen la posibilidad de participar en el **Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos**[19], que pretende potenciar actuaciones preventivas en relación con los riesgos a los que se ven sometidos los menores y los jóvenes, en temas tan importantes como el uso de Internet y las nuevas tecnologías, entre otros. En el marco de este Plan los miembros de las Fuerzas y Cuerpos de Seguridad realizan charlas, visitas y actividades en centros escolares, dirigidas tanto al alumnado como al resto de la comunidad educativa (directivos, personal docente y Asociaciones de Madres y Padres de Alumnos). Como medidas adicionales, se contemplan acciones de sensibilización y formación dirigidas a concienciar sobre el "uso responsable de las nuevas tecnologías y los riesgos que las mismas pueden implicar, promoviendo, a su vez, la comunicación a su entorno familiar, educativo o a las Fuerzas de Seguridad de los hechos de los que pueden ser víctimas o testigos.

6. Mecanismos de respuesta y soporte ante un incidente

Cómo reaccionar ante una infección de virus

La prevención es la mayor garantía de seguridad informática que existe. No obstante, ningún dispositivo conectado a Internet está exento del riesgo de infección.

En los siguientes apartados se indica el modo de actuar ante la sospecha o la evidencia de una infección por virus, o por cualquier otro tipo de código malicioso.

[18] Software para Protección de menores (2014) www.controldeinternet.com

[19] Ministerio del Interior. Instrucción nº 7/2013 de la Secretaría de Seguridad, sobre el "Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos". Recuperado de: http://www.interior.gob.es/documents/642012/1568685/Instruccion_7_2013.pdf/cef1a61c-8fe4-458d-ae0d-ca1f3d336ace

¿Cómo saber si un dispositivo está infectado?

- Se abren páginas web que no se han solicitado.
- El dispositivo funciona más lento de lo normal, deja de responder o se bloquea con frecuencia.
- El dispositivo se apaga solo (aun teniendo batería).
- El dispositivo se reinicia cada pocos minutos.
- El dispositivo no se puede iniciar.
- Las aplicaciones no funcionan correctamente.
- No se puede obtener acceso a los discos o a las unidades de disco.
- Aparecen mensajes de error poco usuales.
- Los menús y los cuadros de diálogo aparecen distorsionados.
- La factura refleja llamadas que no se han realizado, mensajes *SMS* que no se han enviado.
- Alguien responde a un correo electrónico que no se ha enviado.
- Aparecen mensajes de publicidad constantemente.
- Se muestran mensajes o imágenes inesperados.
- Se reproducen sonidos o música inusuales de forma aleatoria.
- El lector de CD-ROM se abre y se cierra de forma misteriosa.
- El antivirus se desactiva solo.
- Los programas se inician de forma espontánea.
- El cortafuegos informa de que algunas aplicaciones intentan conectarse a Internet, sin que el usuario las haya puesto en marcha.
- Los archivos y carpetas han sido borrados o su contenido ha cambiado.
- El disco duro muestra más actividad de lo normal, aun cuando no hay programas funcionando, (por ejemplo, si la luz en su unidad principal parpadea de forma rápida).

¿Qué hacer si se tiene la sospecha de que un dispositivo está infectado?

Ante la sospecha de que un ordenador o teléfono ha sido infectado por un virus, se debe reaccionar rápidamente y llevar a cabo las siguientes medidas siguiendo el orden recomendado:

1. Dejar de utilizar el dispositivo.
2. No realizar ninguna actividad que pueda suponer riesgo de pérdida de información, por ejemplo:
    a. No realizar compras por Internet con el dispositivo infectado.
    b. No acceder al correo electrónico, ni a redes sociales, ni a ningún otro servicio que requiera introducir datos de usuario y contraseña.
3. Eliminar de los navegadores los certificados digitales instalados (por ejemplo, el certificado digital de la Fábrica Nacional de Moneda y Timbre que se utiliza para la declaración de la renta, y que identifica al usuario con la misma validez que el DNI).
4. Antes de emprender cualquier acción, hacer una copia de seguridad de todos los datos críticos a una unidad externa (un disco flexible, un CD, *flash memory,* etc.)
5. Escanear el dispositivo con un antivirus online. Algunos ejemplos son:
    a. http://www.pandasecurity.com/spain/homeusers/solutions/activescan/
    b. http://www.bitdefender.es/scanner/online/free.html
    c. http://www.eset-la.com/online-scanner
    d. http://www.zonavirus.com/antivirus-on-line/
6. Escanear el dispositivo con herramientas *Anti Malware y Anti Spyware*

    En caso de duda, es recomendable llevar el ordenador o dispositivo a un servicio técnico para que un experto haga una revisión general, y garantice que el dispositivo está limpio y que se puede utilizar con tranquilidad, sin poner en riesgo la información que contiene.

¿Qué hacer si se tiene la certeza de que un dispositivo está infectado?

Ante la evidencia de que un ordenador o teléfono ha sido infectado por un virus, se debe reaccionar rápidamente y llevar a cabo las siguientes medidas siguiendo el orden recomendado:

1. Dejar de utilizar el dispositivo.
2. No realizar ninguna actividad que pueda suponer riesgo de pérdida de información, por ejemplo:
    a. No realizar compras por Internet con el dispositivo infectado.
    b. No acceder al correo electrónico, ni a redes sociales, ni a ningún otro servicio que requiera introducir datos de usuario y contraseña.
3. Desconectar el dispositivo de Internet, quitando el cable del *router* y desactivando la conexión WIFI.
4. Deshabilitar el envío de datos en tabletas y teléfonos.
5. Eliminar de los navegadores los certificados digitales instalados (por ejemplo, el certificado digital de la Fábrica Nacional de Moneda y Timbre que se utiliza para la declaración de la renta, y que identifica al usuario con la misma validez que el DNI).
6. Apagar el dispositivo. Si no es posible apagarlo (por ejemplo, porque es un teléfono y es necesario realizar llamadas) hay que asegurarse de que está desconectado de la red WIFI y del *router.*
7. Hacer una copia de seguridad de la información importante (fotos, documentos, archivos de trabajo, etc.) Se recomienda hacer la copia de seguridad con el dispositivo apagado, accediendo desde otro dispositivo, siempre que sea posible.
8. Verificar que los datos de la copia de seguridad no están infectados. Existe el riesgo de que al conectar una unidad externa (disco externo, *pen drive*) para guardar los datos de la copia, ésta también sea infectada.
9. En algunos casos existe la posibilidad de restaurar el dispositivo a los valores de fábrica. Esta opción borrará todos los datos personales y configuraciones, por lo que es altamente recomendable realizar previamente una copia de seguridad.

10. En caso de no poder restaurar el dispositivo a los valores de fábrica, llevarlo a un servicio técnico para que un experto haga una limpieza general, y si es necesario, formatear las unidades de almacenamiento (disco duro, tarjeta SD, etc.) y reinstalar el sistema operativo.

Existen métodos avanzados de desinfección de virus que pueden realizarse sin llevar el dispositivo a un servicio técnico, pero requieren conocimientos avanzados de Informática, y pueden suponer un riesgo de pérdida de información si no se tiene claro lo que se está haciendo.

En la OSI y en otros foros especializados se ofrecen instrucciones detalladas para llevar a cabo la desinfección, siempre bajo la responsabilidad del usuario.

- http://www.osi.es/es/desinfecta-tu-ordenador
- http://www.viruslist.com/sp/viruses/encyclopedia?chapter=153280800
- http://www.microsoft.com/es-es/security/pc-security/antivirus.aspx

Cómo reaccionar ante un fraude online

Si se sospecha que se está siendo víctima de un fraude electrónico, lo primero que hay que hacer es notificarlo a la autoridad competente.

En este sentido, INCIBE[20] ha puesto en marcha a través de la Oficina de Seguridad del Internauta (OSI) un formulario de alta de incidentes (https://www.osi.es/es/reporte-de-fraude/formulario-de-alta-de-incidentes-generales), desde donde se puede indicar la información disponible sobre el caso de fraude o estafa online, o a través del teléfono 901110121.

Del mismo modo, la Guardia Civil cuenta con el Grupo de Delitos Telemáticos (GDT) de la Unidad Central Operativa (UCO), con el que se puede contactar a través de la sección colabora de su página web https://www.gdt.guardiacivil.es/webgdt/pinformar.php, o incluso utilizar el formulario de denuncia que, una vez rellenado, generará un documento denuncia en formato PDF, que se puede presentar en un centro policial para interponer la denuncia.

[20] INTECO (Instituto Nacional de Tecnologías de la Comunicación) (2014). www.incibe.es

Por su parte, el Cuerpo Nacional de Policía, dispone de la Brigada de Investigación Tecnológica (BIT) para combatir la delincuencia que utiliza los medios que proporcionan las nuevas tecnologías de la información, y se puede contactar con ella a través del correo electrónico delitos.tecnologicos@policia.es

Qué medios de prueba se deben aportar en caso de ser víctima de un fraude online[21]

- Comprobar y acreditar documentalmente a través de la entidad financiera todos los movimientos económicos relativos a la operación fraudulenta.
- Correos electrónicos relacionados con el fraude.
- Dirección web fraudulenta.
- IP asociada.
- Entidad afectada.
- Mensajes privados relacionados con la estafa:
    - Invitaciones a través de *Facebook.*
    - Mensajes privados por *Whatsapp.*

7. Marco legislativo aplicable a nivel nacional y europeo

El fraude online es un fenómeno ampliamente extendido a nivel internacional y con una tendencia creciente y continuada.

Los fraudes que se llevan a cabo a través de Internet cuentan con determinados aspectos que dificultan la determinación de la competencia judicial, especialmente en los delitos que se cometen a distancia, en los que los elementos constitutivos del delito (la idea, la puesta en marcha, la realización, y la culminación) pueden llevarse a cabo en puntos geográficos muy lejanos y distantes. Por esta razón, el objetivo principal se basa en localizar el vínculo adecuado para determinar qué órgano jurisdiccional está más cerca

[21] Sanchís, C. (2013). Fraude electrónico. Navarra. España. Aranzadi

del punto de conexión con la conducta delictiva, lo cual en ocasiones suele ser una tarea ciertamente compleja y con notables consecuencias.

En este punto, y al hilo de lo comentado anteriormente, es importante destacar que el avance de las nuevas tecnologías supera al avance en materia legislativa. El resultado es un vacío legal que afecta y perjudica a todos las disposiciones del derecho. Tanto la protección de la información de la actividad de los ciudadanos como la regulación de las relaciones comerciales, y especialmente los derechos de propiedad intelectual, deben estar garantizados por los gobiernos. Es preciso que las normas se adapten al escenario actual para evitar que determinados actos delictivos cometidos en la distancia queden impunes, y que estos espacios desprotegidos puedan ser aprovechados por aquellos que quieren obtener beneficios de forma ilícita.

Todo ello sin olvidar la complejidad del escenario global, pues los límites geográficos son imprecisos debido a la inmensidad del tráfico internacional de información, y consecuentemente, a la interacción de sujetos y acciones sometidas a distintas jurisdicciones con distintos marcos legislativos, lo que da lugar a espacios de impunidad con poco o ningún control normativo.

El marco legislativo en este aspecto es muy complejo, ya que gran parte de los fraudes se producen con origen en países en los que la jurisdicción de las autoridades a veces no está permitida, o se encuentra restringida. Muchos cibercriminales son conscientes de estos vacíos legales y realizan sus ataques a través de servidores alojados en lugares en los que resulta muy difícil (y a veces, imposible) realizar un seguimiento de la actividad fraudulenta así como obtener evidencias que demuestren la actividad delictiva.

En este punto, es importante destacar que el alcance de la jurisdicción española en materia penal sólo es competente para los delitos cometidos en territorio español, incluidas naves y aeronaves españolas. Por lo tanto, para el caso de un fraude informático cometido fuera de las fronteras españolas, normalmente sólo se podrá considerar la competencia de la jurisdicción española para supuestos en los que el autor fuera español en el momento de cometer el delito, o nacionalizado después de cometerlo[22].

[22] Sanchís, C. (2013). Fraude electrónico. Navarra. España. Aranzadi

La persecución de la ciberdelicuencia y las actividades delictivas cometidas a través de Internet, presenta ciertas características que hacen indispensable la cooperación policial y judicial internacional, así como la asistencia técnica entre los países, la comunidad internacional y el sector privado.

Desde el punto de vista internacional, determinar el lugar de comisión del delito es un elemento esencial para perseguir y condenara los autores, así como para aplicar la ley penal, ya que determinar de forma correcta la jurisdicción de los países en materia penal puede tener consecuencias transcendentales, tanto en el plano penal como en el plano procesal, pues ambas leyes (procesal y penal) van firmemente unidas a la territorialidad del órgano juzgador, lo que hace que los tribunales penales españoles sólo puedan aplicar la legislación penal procesal española. Este hecho pone de manifiesto que la incertidumbre sobre el modo de decretar la jurisdicción competente, puede provocar una situación de ineficiencia legal, que permita a los ciberdelincuentes delinquir en aquellos países cuya legislación sea poco exigente, o incluso con determinadas conductas que en el país de origen no estén tipificadas como delito, y que permitan a los ciberdelincuentes actuar desde estos países con total impunidad.

Ahí radica la importancia de los tratados internacionales, como por ejemplo, el Convenio europeo sobre transmisión de procedimientos en materia penal, que permite solicitar a otro país que encause un hecho que es delito tanto en el país que se comete el delito, como en el país desde el que se realiza la acción delictiva.

A día de hoy se sigue trabajando con gran esfuerzo en los aspectos legislativos que han de dar solución a esta problemática, pero resulta imprescindible la colaboración internacional para frenar la tendencia delictiva que se está llevando a cabo en Internet, y con el firme objetivo de no dejar impunes los actos delictivos cometidos en países con un marco legislativo menos exigente.[23]

[23] Fuente: Sanchís, C. (2013) Fraude electrónico. Navarra. España. Aranzadi

8. Organismos, entidades y foros de referencia

ORGANISMO / DETALLE

Grupo de Delitos Telemáticos Guardia Civil (www.gdt.guardiacivil.es/webgdt/pinformar.php)

El Grupo de Delitos Telemáticos fue creado en 1996 para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet.

Brigada de Investigación Tecnológica Policía Nacional (delitos.tecnologicos@policia.es)

La Brigada de Investigación Tecnológica es la Unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia: pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería, etc.

Oficina de Seguridad del Internauta (www.osi.es)

La Oficina de Seguridad del Internauta (OSI) de INCIBE es un portal de información general sobre la seguridad en Internet, que proporciona información y soporte para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.

Instituto Nacional de Ciberseguridad (www.incibe.es)

El Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas.

Pantallas Amigas (www.pantallasamigas.net)

Iniciativa que tiene como misión la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia. Algunas de sus actividades principales son la creación de recursos didácticos, sesiones y jornadas formativas y estudios, con especial énfasis en la prevención del *ciberbullying*, el *grooming*, el *sexting*, la sextorsión y la protección de la privacidad en las redes sociales. Dispone de una línea de ayuda para niños y adolescentes ante situaciones de peligro en Internet.

Asociación de Internautas (www.internautas.org/)

La Asociación de Internautas (A.I.) es una asociación de ámbito nacional sin ánimo de lucro fundada en 1998. Orientada a defender los intereses de los ciudadanos frente a las grandes compañías de telecomunicaciones, proveedores, empresas informáticas y, por supuesto, ante cualquier organismo competente en esta materia.

9. Más información

Presentamos a continuación una relación de documentos y recursos para ampliar información sobre virus y fraudes:

RECURSO / DETALLE

Blog de Seguridad en Internet y Protección de menores (www.elblogdeangelucho.com)

Blog que pretende convencer de las infinitas bondades que las nuevas tecnologías e Internet ofrecen a los internautas, ofreciendo consejos sobre los peligros que acechan en la red, y enseñando a identificarlos y a disfrutar con mayor seguridad de la red de redes.

Blog de seguridad de productos Apple (www.seguridadapple.com)

Blog destinado a explorar de forma diaria todo tipo de contenido relacionado con la seguridad de los productos Apple.

Explicación sobre cómo funciona un antivirus (https://www.youtube.com/watch?v=xZECq69Um2A#t=249)

Video explicativo sobre cómo funciona un antivirus explicado por un experto de la empresa ESET distribuidora de productos antivirus.

Eleven Paths (http://blog.elevenpaths.com)

Empresa filial de Telefónica que cuenta con herramientas que permiten analizar el comportamiento de Apps maliciosas en las distintas tiendas de aplicaciones de dispositivos móviles orientadas al mundo del fraude online

Blog con información sobre las estafas relacionadas con envío de mensajes SMS Premium (www.afectadosporlossmspremium.com/)

Plataforma que trata de denunciar el uso indebido por parte de muchas empresas, con la complicidad de las operadoras de telefonía móvil de estos servicios.

10. Bibliografía

ADSL Zone (2013). *Detenido el creador de WhatsAppSpy, una aplicación falsa para espiar conversaciones*. http://www.adslzone.net/article12102-detenido-el-creador-de-whatsapp-spy-una-aplicacion-falsa-para-espiar-conversaciones.html

De los Santos, S. (2012). *El sentido común contra el Malware*. Accesible en www.unaaldia@hispasec.com

El Blog de Angelucho (2013). *Seamos nuestro propio CSI (II): Analizando un Phishing.* http://elblogdeangelucho.com/elblogdeangelucho/blog/2013/07/07/seamos-nuestro-propio-csi-ii-analizando-un-phishing/

Infospyware (2014). *El ransomware Kovter, el virus de la policía infecta 44.000 dispositivos por día.* http://www.forospyware.com/t492003.html

INTECO (2010). *Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles.* http://www.osimga.org/export/sites/osimga/gl/documentos/d/estudio_sobre_seguridad_y_privacidad_en_el_uso_de_los_servicios_moviles_por_los_menores_espanoles-1.pdf

INTECO (2012). *Estudio sobre el fraude a través de Internet.* *https://www.incibe.es/file/xk6K9xU46WM_Q1i88xyWtA*

INTECO (2014). *Estudio sobre la Ciberseguridad y confianza en los hogares españoles.* http://www.ontsi.red.es/ontsi/sites/default/files/ciberseguridad_y_confianza_en_los_hogares.pdf

Lorenzana, C. (2011). *Seguridad y Ciudadanía.* Revista del Ministerio del Interior Nº5. http://www.interior.gob.es/documents/642317/1203831/Seguridad+y+ciudadan%C3%ADa.+N.+5+%282011%29.pdf/860c1cdf-cfa3-4953-a79e-16a9af72f1be

Oficina de Seguridad del Internauta (OSI) (2014) https://www.osi.es/es/contrasenas

Redeszone (2014). Las web falsas para hackearWhatsApp aumentan exponencialmente http://www.redeszone.net/2014/08/11/las-web-falsas-para-hackear-whatsapp-aumentan-exponencialmente/

Sanchís, C. (2013). *Fraude electrónico*. Navarra. España. Ed. Aranzadi

Software para Protección de menores (2014) www.controldeinternet.com

Software para Protección de menores (2014) www.controldeinternet.com

Symantec (2014). *Security 1:1 - Part 5 - Online gaming fraud, scam and phishing attempts.* http://www.symantec.com/connect/articles/security-11-part-5-online-gaming-fraud-scam-and-phishing-attempts

Un Informático en el lado del mal. Blog sobre seguridad informática. (2014) *Android: Apps maliciosas en Google Pl*ay. http://www.elladodelmal.com/2015/03/android-apps-maliciosas-en-google-play.html