GUIAS DE SEGURIDAD UJA

Uso seguro de la web

1. Introducción

En la actualidad la navegación web es, con diferencia, una de las actividades a las que más tiempo dedicamos en nuestro uso habitual de Internet.

Pero ¿es segura la navegación web? De entrada, navegar por Internet no es una actividad anónima, por lo que la privacidad y la seguridad son dos temas a los que debemos prestar máxima importancia, máxime cuando accedamos a sitios web especialmente sensibles por donde circulan nuestros datos personales, como pueden ser las webs de comercio electrónico o de banca on-line.

En este documento se ofrecen algunos consejos básicos a tener en cuenta para que nuestra navegación diaria por la web sea más segura.

2. Peligros más frecuentes asociados a la navegación web

Entre las diferentes amenazas a los que nos podemos ver expuestos hoy en día cuando navegamos por Internet, se encuentran las siguientes:

- La posible instalación de **software malicioso de tipo adware (software comercial) y spyware (software espía)** que genera la apertura constante de ventanas emergentes y que hace un seguimiento de nuestros hábitos de navegación, con finalidades diversas.

- Ataques llevados a cabo explotando **vulnerabilidades en los sistemas operativos y aplicaciones** instaladas, con objeto de capturar contraseñas y otro tipo de información sensible.

- **Secuestradores de navegador (browser hijackers)**: se trata de un intento de terceros para tomar el control de nuestro navegador web y utilizarlo con fines maliciosos. Asociados a los secuestradores de navegador, en muchos casos también se instalan **keyloggers (capturadores de pulsaciones de teclado)** que registran todo lo que tecleamos, incluyendo contraseñas.

- Una de las modalidades de secuestro cada vez más habituales es el denominado **Ransomware, o instalación de falsas aplicaciones (rogue)**. Los casos más famosos de ransomware son el "virus de la Policía" y el "virus de la SGAE".

- Especialmente peligrosa es la **infección web denominada "drive-by-download"**, que permite infectar masivamente a los usuarios simplemente accediendo a un determinado sitio web. **Hace tiempo estos ataques eran casi exclusivos de sitios de dudoso contenido (software ilegal, hacking, pornografía…), pero en la actualidad, la tendencia es encontrarlos en todo tipo de sitios web, ya sea directamente o bien, a través de terceros en forma de banners publicitarios, por lo que no debemos bajar la guardia.**
  Ante esto, es fundamental tener el sistema operativo y las aplicaciones correctamente actualizadas, además de tener instalado y actualizado un buen antivirus o suite de seguridad.

- **Envío y uso de información personal a través de sitios web.** El mejor consejo es evitar proporcionar en Internet cualquier tipo de información que nunca ofreceríamos en el mundo real.

2.1. Falsas aplicaciones (rogue) y barras de utilidades (toolbars)

Las **aplicaciones de tipo "rogue"** son falsos programas que simulan ser antivirus y suites de seguridad (las interfaces de usuario son muy similares a las de otras aplicaciones antivirus reales existentes en el mercado), pero que en realidad esconden malware destinado a hacer un mal uso de nuestro ordenador y la información contenida en él. **Son especialmente peligrosas porque pueden ser el origen de un secuestro de navegador o del robo de nuestras contraseñas. Además, actualmente es uno de los métodos más difundidos y efectivos por lo que hay que tener un especial cuidado.**

Algunos consejos para detectar aplicaciones "rogue":

1. La falsa aplicación por lo general **se descarga sin autorización del usuario** o solicita su descarga de forma muy insistente, justo después de acceder a algún sitio donde se realiza un falso análisis on-line de nuestro equipo.

2. Al querer realizar la limpieza de las amenazas **el programa nos "invitará" a comprar la licencia del producto** a través de un sitio donde poder realizar el pago con tarjeta de crédito. **Es muy importante que bajo ninguna circunstancia se indiquen dichos datos.**

3. La aplicación "rogue", una vez instalada, **tiende a realizar ciertas modificaciones a nuestro sistema operativo para insistir en el riego que tenemos** y así apresurarnos a realizar la compra del producto.

4. Si se intentamos desinstalar la herramienta desde la opción "Agregar o quitar programas" del panel de control, al reiniciar el equipo **la aplicación rogue puede volver a instalarse de forma automática**.

En cuanto a las **barras de utilidades (toolbars)** son barras de botones y complementos que se añaden a nuestro navegador, generalmente durante la instalación de cualquier otro software gratuito. Aunque algunas de ellas son totalmente legítimas e inofensivas, hay muchas otras que esconden malware que puede afectar a nuestro equipo o espiar nuestros hábitos de navegación sin que seamos conscientes de ello.

Como norma general, se recomienda **NO instalar ninguna de estas barras, a menos que la conozcamos y realmente la necesitemos.** Igualmente, es aconsejable revisar desde el Panel de Control de Windows, en la lista de aplicaciones instaladas si hay alguna de estas barras (alguna aplicación que contenga la palabra "toolbar" y desinstalarla. Nos evitaremos sorpresas y problemas en el futuro.

3. Consejos para un uso seguro de la web

3.1. Consejos generales

- En primer lugar, la protección comienza por el sistema. El equipo debe contar con un **antivirus** correctamente instalado y actualizado, un **firewall** y algún **software antimalware específico**.

- Aplica las actualizaciones disponibles del sistema operativo.

- Utiliza "conexiones seguras" siempre que sea posible. Asegúrate que, al transmitir datos sensibles, la dirección web comienza por HTTPS, y en la parte inferior del navegador aparece algún tipo de candado cerrado que indica que hemos establecido una conexión segura.

- Nunca hagas clic en enlaces sospechosos**.**

- **No accedas a sitios web de dudosa reputación,** tales como páginas de software ilegal (warez), generadores de números de serie (keygens), etc. Estos ficheros son muy propensos a contener malware y pueden poner en serie peligro nuestro equipo de forma instantánea. Hay que tener cuidado especialmente en evitar la instalación de aplicaciones "rogue", como se ha indicado anteriormente.

- **Ten precaución con los resultados que ofrecen los buscadores web**. A través de técnicas denominadas "Black Hat SEO", los atacantes suelen posicionar sus sitios web maliciosos entre los primeros lugares en los resultados de los buscadores. Ante cualquiera de estas búsquedas, debes estar atento a los resultados y verificar a qué sitios web está siendo enlazado.

- **Usa plugins o extensiones en el navegador para eliminar las molestas ventanas emergentes** (pop-up) que aparecen durante la navegación, o configura tu navegador para evitar estas ventanas. En muchas ocasiones, estas ventanas son la vía de acceso a virus, troyanos y otros tipos de malware.

- Se debe **evitar entrar desde lugares públicos en sitios web que requieran un nivel alto de seguridad** (ej: páginas de entidades bancarias y financieras).

- Si algún sitio web ofrece la descarga de aplicaciones que no se solicitaron, no deben ser aceptadas sin antes verificar la integridad del mismo con un antivirus o aplicación de seguridad.

- Ten especial precaución con la **instalación de complementos extras para el navegador, tales como barras de utilidades (toolbars).** Conviene revisar periódicamente las aplicaciones instaladas en nuestro PC y

eliminar cualquier aplicación de tipo ToolBar (barra de herramientas) que nos resulte sospechosa o que no recordemos haber instalado.

3.2. Proteger nuestra privacidad

- **Nunca facilites datos personales** si no existe una completa seguridad sobre quién los va a recibir.
- No incluyas en ninguna web **información personal sobre tus gustos, aficiones o preferencias**, si no quieres verte bombardeado de información comercial y publicidad relacionada con los datos registrados.
- Ten especial **cuidado con la información que compartes en Internet y con quién la compartes.** Esto es especialmente importante en las redes sociales.

3.3. Uso de contraseñas

- Ten **precaución con las contraseñas que guardes en el navegador**, y utiliza siempre una contraseña maestra para que nadie más pueda acceder a ellas.
- Cambia tus contraseñas periódicamente y utiliza contraseñas robustas. No dejes las contraseñas guardadas en claro en tu disco duro ni las anotes en un papel.

3.4. Descarga de software y aplicaciones

- Extrema la precaución en los archivos que recibes en sesiones de chat o desde cualquier otra página web o aplicación que se ejecute desde el navegador web.
- En general, ten mucha precaución con los ficheros que descargues desde redes de tipo P2P, descarga directa o enlaces de tipo Torrent. Es muy fácil que incluyan algún tipo de malware. Antes de abrirlos o ejecutarlos, analízalos con un buen software antivirus / antimalware actualizado.

3.5. Protegerse del clickjacking

- Ten mucha precaución con las páginas que visita y los enlaces que pulsaa. Usa el sentido común.
- Sospecha si alguna página web de las que frecuentas se comporta de forma extraña.
- Ten tu navegador web siempre actualizado.
- Instala y ten actualizadas herramientas como antivirus, antimalware, analizadores de enlaces, etc.
- Si usas Mozilla Firefox puedes instalar el complemento **NoScript** que incluye una funcionalidad llamada "ClearClick" que lanza una ventana al usuario avisándole si ha hecho clic sobre un elemento de la web que se encuentra escondido y que podría ser malicioso.

4. Seguridad en redes sociales

En la actualidad, las redes sociales constituyen uno de los usos más populares de la navegación web, lo que hace que se conviertan en objetivos específicos para la rápida propagación de malware. Por este motivo, hay que tener muy en cuenta una serie de medidas específicas:

- Evitar publicar ningún tipo de información sensible y confidencialque pueda ser usada por terceros con fines

maliciosos. También es muy recomendable evitar la publicación de imágenes propias y de familiares.

- Es muy importante aplicar los consejos para mantener la privacidad del perfil, configurándolo para que no sea público.
- En general, se recomienda no responder a las solicitudes de desconocidos, ya que pueden contener códigos maliciosos o pueden formar parte de actividades delictivas.
- Ignorar o denunciar los mensajes que ofrecen material pornográfico, pues suelen ser canales habituales para la propagación de malware.
- Como norma, también se recomienda cambiar periódicamente las contraseñas en nuestros perfiles de redes sociales, para evitar que sean capturada fácilmente.
- Denuncia cualquier uso abusivo que detectes en las redes sociales. Ante hechos graves, recurre a la Policía o la Guardia Civil, a través de sus unidades especializadas en delitos telemáticos.

El Instituto Nacional de Ciberseguridad (INCIBE) dispone de una sección en su sitio web donde ofrece guías de seguridad y videotutoriales específicos para diferentes redes sociales y sitios web 2.0:

https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet

4.1. Referencias en Internet

- Navegación Segura
  http://www.navegacionsegura.es/

- Guías de seguridad en el uso de las redes sociales (INCIBE)
  https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet

- ESET – Guía de buenas prácticas de seguridad informática
  http://www.eset-la.com/pdf/prensa/informe/buenas_practicas_seguridad_informatica.pdf

- Seguridad y privacidad en Mozilla Firefox:
  http://support.mozilla.org/es/products/firefox/privacy-and-security

- Oficina de Seguridad del Internauta (OSI)
  http://www.osi.es/es/actualidad/blog/2012/04/04/navega-mas-seguro-con-los-analizadores-de-enlaces-url

- Guardia Civil - Grupo de Delitos Telemáticos:
  https://www.gdt.guardiacivil.es

- Policía Nacional – Brigada de Investigación Tecnológica
  http://www.policia.es/org_central/judicial/udef/bit_alertas.html