Navegación en Internet.

Al momento de usar Internet mediante algún **navegador** podríamos estar expuestos a varias **amenazas cibernéticas** las cuales podrían causar algún tipo de daño al sistema operativo, que van desde las que parecieran insignificantes hasta las potencialmente peligrosas para la Confidencialidad, Integridad y Disponibilidad de la información. Por ejemplo: al navegador (cambio de la página de inicio), la excesiva publicidad o lentitud al momento de navegar por internet, robo de información mediante técnicas de ingeniería social como **phishing, troyanos, PUA**[1] (Aplicación potencialmente no deseada), etc.

Algunas de las amenazas a las que podemos estar expuestos al navegar en Internet son:

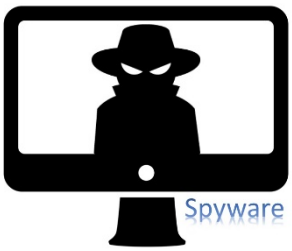
Tipos de Amenazas.

a) Troyanos.

El nombre de esta clase de malware proviene de la leyenda del caballo de Troya. De acuerdo a esa historia, estos **malware se presentan como un beneficio o aparentan el no representar ningún riesgo** como juegos o aplicaciones gratuitas, ofertas o publicidad para que el usuario sienta curiosidad y decida a instalar o ejecutar los programas. Una vez dentro del sistema, los troyanos pueden realizar varias acciones maliciosas como robo de información y contraseñas, envío de spam, registro de todo lo que se teclea, entre otras acciones.

[1] PUA: http://soporte.eset-la.com/kb2629/?locale=es_ES

b) Spyware.



Es software que puede **almacenar y/o robar información** sobre el usuario sin saberlo, estos datos pueden ser usados para fines publicitarios por lo cual son capaces de registrar la URL, las palabras introducidas en motores de búsqueda, compras en línea, etc.

Este tipo de software puede ser descargado aun sin el consentimiento del usuario al instalar otro software ya que muchas veces se incluye en los términos y condiciones, al abrir un correo electrónico o dar clic en un link en páginas poco recomendadas.

Puede causar que se modifique el navegador, como el motor de búsqueda preferido, la página de inicio, pueden aparecer otros accesos directos o software que el usuario no instalo, aparecen ventanas emergentes (pop-ups) casi en cualquier página.

c) Correo Spam.

Correo electrónico basura no solicitado también llamado *junk mail* generalmente enviado en forma masiva y conteniendo publicidad o ataques de robo de identidad (phishing). Por lo general provienen de una dirección de correo desconocida. Este tipo de amenaza es común por vía correo electrónico, sin embargo, también se puede difundir a teléfonos celulares mediante mensajes SMS o aplicaciones de mensajería instantánea.

¿Cómo consiguen nuestra dirección de email? Se puede hacer mediante ingeniería social, usando troyanos o gusanos que sean capaces de examinar la lista de direcciones (contactos), cuando se proporcionan nuestros datos para ingresar a ciertos foros, chats, wikis, comunidades virtuales, redes sociales, etc.

En muchos casos para la descarga de software “gratis” se pide un registro incluyendo nuestra dirección de email. Se debe tener cuidado donde proporcionamos nuestros datos personales.

d) Adware.

Adware es la unión de las palabras *"Advertising"* (Publicidad) del idioma inglés y "*Ware*" de Software (Programa). **Es un software que regularmente va ligado a barras de herramientas, plug-ins en los navegadores, o algún otro tipo de malware** que de modo automático presenta al usuario anuncios de publicidad.

Este software puede entrar al sistema operativo al descargar otro programa de software, navegar en páginas que contienen algún archivo infectado. Estos programas se basan en nuestras búsquedas para mostrar la publicidad relacionada o en relación a los sitios que visitamos.

¿Cómo puede proteger su Navegación?

A continuación, se describen brevemente las acciones y buenas prácticas que se pueden llevar a cabo al navegar por Internet, la cuales **ayudaran a reducir** de manera significativa el riesgo de fraude electrónico.

1) Descargar los navegadores y demás software de los sitios oficiales y de preferencia la última versión.
2) Navegar en medida de lo posible en sitios seguros y usar el sentido común para no aceptar ofertas o descargas "gratis".
3) Borrar regularmente los archivos temporales, cookies, historial de navegación y cambiar en los sitios más usados las contraseñas de forma regular
4) Tener y mantener actualizado el software antivirus.
5) Administrar sus contraseñas de forma segura y cambiarlas regularmente.

Si desea mayor información para mantenerse seguro, visítenos aquí: http://www.dsi.ipn.mx/

Referencias:

- http://definicion.de/adware/
- http://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/spyware/
- http://www.pcworld.com.mx/Articulos/11735.htm
- https://www.google.com/transparencyreport/safebrowsing/?hl=es-419
- http://news.netcraft.com/archives/2005/05/18/online_vigilantes_fight_back_against_phishing_fraudsters.html
- http://enavas.blogspot.mx/2015/10/acceso-httpsrayuelaeducarexes-esta.html
- https://www.unocero.com/2013/02/05/como-tener-una-navegacion-segura-por-internet/
- https://www.mywot.com/
- http://toolbar.netcraft.com/
- https://www.google.com.mx/chrome/browser/desktop/
- https://www.mozilla.org/es-MX/firefox/new/