



Consejos para navegar seguro por Internet

Edufuturo

En Internet hay mucha basura (spam), mensajes de publicidad, promociones, premios... una gran cantidad de anuncios que llaman la atención y te invitan a acceder a ellos. No caigas en la trampa, si haces clic sobre ellos puedes descargar un virus a tu computadora, como le sucedió a Adam, o podrías darle acceso a tu información privada a algún hacker, o también podrías ser víctima de un fraude u otras amenazas de la red.



10 consejos para navegar seguro por Internet.

El 17 de mayo de cada año se celebra el Día de Internet. Durante esta celebración se promueve el cuidado en la red y la navegación segura.

Internet se ha caracterizado por innovar constantemente. Internet es uno de los pilares fundamentales que ha hecho

posible la revolución tecnológica-informática de nuestros días. Se le reconoce como revolución porque ha cambiado nuestras vidas, modificando nuestras conductas. Un ejemplo claro es el celular. Hoy en día, muchísimas personas tienen un teléfono celular y no salen de su casa si no lo llevan consigo. Según la Superintendencia de Telecomunicaciones (SIT), para el 2012 había casi 21 millones (20,787,080) de teléfonos celulares activos en Guatemala, cuando la población del país, para el mismo año, se estimó que no alcanzaba los 15.5 millones de habitantes, según el Instituto nacional de Estadística (INE), (15,073,375 habitantes). O sea que había más celulares que habitantes en Guatemala, imagínate eso...

Con las nuevas tecnologías hacemos cosas que de pequeños no hacíamos y que nuestros abuelos tal vez ni se imaginaron: hablar por videoconferencia en tiempo real y sincosto, con alguien que está en el otro lado del mundo, a través de una computadora, una tableta, o un celular. Nuestros abuelos tal vez solo vieron esto en las películas de ciencia ficción. Estos cambios, así como tienen sus ventajas, también contienen riesgos, los cuales podemos minimizar si tomamos ciertas precauciones o seguimos

los consejos de algunos expertos, como el decálogo de Sebastián Bortnik, analista de seguridad para ESET Latinoamérica. Con este decálogo, Bortnik nos previene de muchos de los riesgos que podemos encontrarnos en el ciberespacio.

1. Evita los enlaces sospechosos: uno de los medios más utilizados para dirigir a las víctimas a sitios maliciosos son los hipervínculos o enlaces. No hagas clic en estos enlaces, de esta manera evitarás acceder a páginas web que contengan amenazas capaces de infectar tu tableta o computadora.



Estos enlaces se encuentran en casi cualquier sitio: pueden estar presentes en un correo electrónico, una ventana emergente de chat, un mensaje en una red social... Una clave para identificarlos es detectar si se presentan en alguna situación sospechosa, por ejemplo: si te invitan a ver una foto en un idioma distinto al propio, si te avisan que “ganaste un premio”, si provienen de un remitente desconocido o si te redireccionan a un sitio web poco confiable.

2. No accedas a sitios web de dudosa reputación: mediante técnicas de Ingeniería Social, muchos sitios web



Advertencia- Si visitas este sitio web, tu ordenador puede resultar dañado.

Sugerencias:

- [Vuelve a la página anterior](#) y elige otro resultado.
- Realiza otra búsqueda para encontrar lo que buscas.

Si lo deseas, puedes acceder a <https://bugs.php.net/bug.php?id=65957> bajo tu propia responsabilidad. Para obtener información más detallada sobre los problemas que detectamos, visita la [página de diagnóstico "Navegación segura"](#) de este sitio.

Para obtener más información acerca de software malintencionado en Internet y sobre cómo protegerlo de él, puedes visitar la página [Shutterstock.com](#).

Si eres el propietario de este sitio web, puedes solicitar una revisión del mismo a través de las [Herramientas para webmasters](#) de Google. Encontrarás más información sobre el proceso de revisión en el [Centro de ayuda para webmasters](#).

Ausencia de plagio por 

suelen promocionarse con datos que pueden llamar la atención del usuario –como descuentos en la compra de productos (o incluso ofreciéndotelos de forma gratuita), primicias o materiales exclusivos de noticias de actualidad, material multimedia, entre otros. Para una navegación segura es recomendable que estés atento a estos mensajes y evites acceder a páginas web de tales características.

3. Actualiza constantemente el sistema operativo y las aplicaciones: procura mantener tu tableta al día con las últimas actualizaciones de seguridad, en especial las del sistema operativo, las relativas al sistema de seguridad, y también cualquier software que hayas instalado. Con ello evitarás la propagación de amenazas a través de las debilidades que pueda tener el sistema.

4. Descarga aplicaciones desde sitios web oficiales: muchos sitios simulan ofrecer programas populares; pero estos son alterados, modificados o suplantados por otras versiones que



contienen algún tipo de malware (software malicioso). Cuando descargas el archivo, al momento de la instalación, el código malicioso también se graba en el sistema de tu computadora, pudiendo afectar gravemente tu equipo y tus datos. Por eso es recomendable que utilices los sitios oficiales para realizar las descargas de cualquier aplicación. En otras palabras: evita descargar cualquier aplicación o programa desde sitios “chafas” (quenosean oficiales).

5. Utiliza tecnologías seguras: para proteger tu equipo antelas principales amenazas que se difunden por Internet, las mejores solucionesonteneractivoslosantivirus, el firewall y anti spam.



6. Evita ingresar información personal en formularios dudosos: cuando tengas que completar un formulario electrónico que contenga campos con información sensible, por ejemplo: tu usuario

y contraseña; primero verifica la legitimidad del sitio. Una buena estrategia es corroborar el dominio y la utilización del protocolo HTTPS para garantizar la confidencialidad de la información. De esta manera podrás prevenir ataques de phishing de quienes intenten

obtener información sensible a través de la simulación de una entidad de confianza. En definitiva, ten cuidado con las imitaciones.



7. Ten precaución con los resultados que arrojan los buscadores web: a través de técnicas de Black Hat SEO, los atacantes posicionan sus sitios

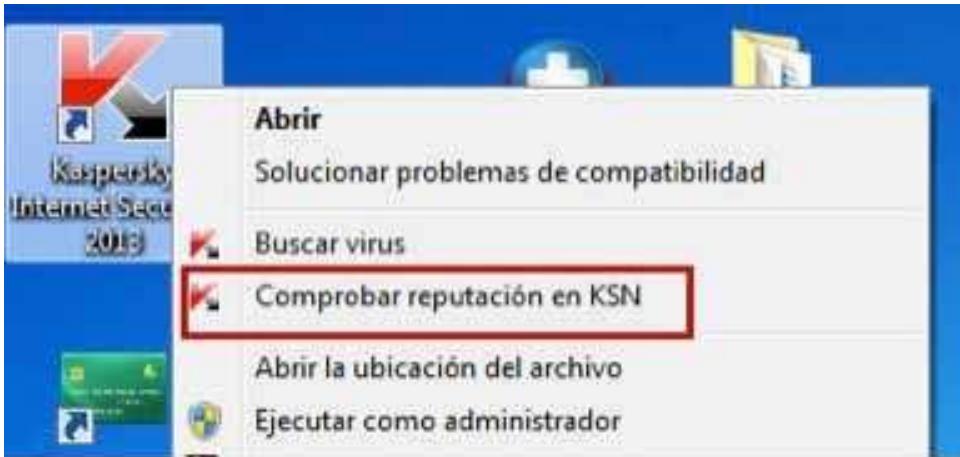
web entre los primeros lugares en los resultados de los buscadores. En especial cuando las búsquedas emplean palabras clave muy utilizadas por el público: temas actuales, noticias extravagantes o temáticas populares (como el deporte y el sexo). Ante cualquier búsqueda debes estar atento a los resultados y verificar a qué sitios web estás siendo enlazado. Si al leer la información te das cuenta que esta no corresponde a lo que buscabas, no le des más vueltas, cierra la ventana rápidamente.

8. Acepta las invitaciones solo de contactos conocidos:

tanto en las cuentas de mensajería instantánea como en las redes sociales, tipo facebook o twitter. Acepta e interactúa únicamente con contactos conocidos. De esta manera evitas acceder a los perfiles creados por los atacantes que buscan comunicarse con las víctimas y exponerlas a diversas amenazas como malware, phishing, cyberbullying u otras.



9. Evita la ejecución de archivos sospechosos: la propagación de malware suele realizarse a través de archivos ejecutables. Evita ejecutar archivos a menos que conozcas la seguridad del mismo y que su procedencia sea confiable (tanto si proviene de un contacto en la mensajería instantánea, un correo electrónico o un sitio web). Cuando descargas archivos de redes P2P, es preferible que la analices con tu antivirus o una aplicación de seguridad antes de ejecutarlos.



10. **Utiliza contraseñas fuertes:** muchos servicios en Internet están protegidos con una clave de acceso, para resguardar la privacidad de la información. Si esta contraseña fuera sencilla o común, un atacante podría adivinarla y por lo tanto acceder indebidamente como si fuera el usuario verdadero. Por este motivo se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud de al menos 8 caracteres.



Las buenas prácticas sirven para aumentar el nivel de protección y son el mejor aliado para las tecnologías de seguridad. Mientras tu antivirus, firewall, antispam y antimalware se encargan de prevenir algún tipo de incidente, la aplicación de estas buenas prácticas logrará que estés menos expuesto a las amenazas existentes.

Por: Luigi Santos
Palabras: 1648
Imágenes: Shutterstock
Referencias:

10 consejos para navegar seguro por Internet. Por InfoSpyware.
17/05/2010. <http://www.infospware.com/articulos/10-consejos-para-navegar-seguro-por-Internet/> Consultado el 20/09/2013

