Soluciones Digitales

- Sistemas empaquetados
- Software a Medida
- Soporte Corporativo
- Consultoría Informática

Pueyrredón 935 - (2630) Firmat
Tel.: 03465-420494 // Whatsapp: +54 9 3465 522230
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar
telegram: @aesantarelli skype: sdigitales

Decálogo de Seguridad en Internet

El 17 de mayo se celebra en todo el mundo el Día de Internet, una iniciativa que tiene como objetivo dar a conocer las nuevas tecnologías y las posibilidades que éstas ofrecen, desde un marco voluntario donde cualquier persona u organización puede realizar actividades o eventos relacionados con este día.

Con motivo de esta fecha, el equipo de Educación de ESET Latinoamérica ha preparado un decálogo de seguridad para usuarios de Internet, con los consejos más importantes para cuidarse al momento de utilizar la computadora en el ciber-espacio:

1. Evitar los enlaces sospechosos: uno de los medios más utilizados para enlazar a las víctimas a sitios maliciosos son los hipervínculos, o enlaces. Evitar hacer clic en éstos previene el acceso a páginas web que posean amenazas que pueden infectar el equipo del usuario. Los enlaces pueden estar disponibles tanto en un correo electrónico, como en una ventana de chat o en un mensaje en una red social.

2. No acceder a sitios web de dudosa reputación: a través de técnicas de Ingeniería Social, muchos sitios web suelen promocionarse con datos que pueden llamar la atención del usuario, como por ejemplo descuentos en la compra de productos (o incluso ofreciéndolos gratis), primicias o materiales exclusivos de noticias de actualidad, material multimedia, entre otros. Es recomendable que el usuario esté atento a estos mensajes y evite acceder a páginas web con estas características.

3. Actualizar el sistema operativo y aplicaciones: el usuario debe mantener actualizados con los últimos parches de seguridad no sólo el sistema operativo, sino también el software instalado en el equipo a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.

4. Descargar aplicaciones desde sitios web oficiales: muchos sitios simulan ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware que puede infectar el equipo al momento que el usuario lo instala, si es que no cuenta con una solución de seguridad efectiva. Si desea descargar aplicaciones, hágalo desde las páginas oficiales.

5. Utilizar tecnologías de seguridad: particularmente las soluciones de seguridad tales como antivirus, firewalls y antispams representan las aplicaciones más importantes para la protección ante las principales amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante estos peligros.

6. Evitar el ingreso de información en formularios dudosos: cuando el usuario se enfrente a un formulario web que contenga campos con información sensible (por ejemplo, usuario y contraseña), es recomendable que compruebe la legitimidad del sitio, tanto a través del dominio como verificando la utilización del protocolo HTTPS que garantiza la confidencialidad de la información. De esta forma, se protege de los ataques de phishing que intentan obtener información confidencial a través de la simulación de una entidad de confianza.

7. Tener precaución en los resultados en buscadores: A través de técnicas de BlackHat SEO, los atacantes suelen posicionar sus sitios web entre los primeros lugares de los resultados de los buscadores. Esto ocurre especialmente en búsquedas realizadas frecuentemente por el público, como temas de actualidad, noticias extravagantes o temáticas populares (como el deporte, el sexo o similares). Ante cualquiera de estas búsquedas, el usuario debe estar atento a los resultados de las mismas y verificar a qué sitios web está siendo enlazado.

8. Aceptar sólo contactos conocidos. Tanto en los clientes de mensajería instantánea como en las redes sociales, es recomendable aceptar e interactuar sólo con contactos conocidos, para así evitar los perfiles creados por los atacantes para contactarse con las víctimas y exponerlas a diversas amenazas como pueden ser el malware, el phishing, el cyberbulling u otras.

Pueyrredón 935 - (2630) Firmat
Tel.: 03465-420494 // Whatsapp: +54 9 3465 522230
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar
telegram: @aesantarelli skype: sdigitales

9. Evitar la ejecución de archivos sospechosos: la propagación de malware suele realizarse a través de archivos ejecutables. Es recomendable evitar la ejecución de archivos a menos que se sepa que el mismo es seguro, y que su procedencia sea confiable (tanto provenga de un contacto en la mensajería instantánea, un correo electrónico o un sitio web). Además, cuando se descargan archivos de redes P2P, es recomendable que antes de ejecutarlos, sean explorados con un software antivirus.

10. Utilice contraseñas fuertes: muchos servicios en Internet están protegidos con una clave de acceso, de forma de resguardar la privacidad de la información. Si esta contraseña fuera sencilla o común (muy utilizada entre los usuarios) un atacante podría adivinarla, y de esa manera acceder indebidamente en nombre del usuario. Por este motivo es que se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud de al menos 8 caracteres.

Estas buenas prácticas permitirán a los usuarios aumentar su protección contra las principales amenazas que circulan en la actualidad por Internet. Son por lo general sencillas de realizar y seguramente minimizarán el riesgo mientras se utilice la **"Red de redes".**