TIPS DE SEGURIDAD INFORMÁTICA

Internet ha sido y es un avance contante que llego para cambiarnos la vida… pero así como tiene su infinidad de ventajas, también tiene una parte oscura y riesgosa la cual puede reducirse en mucho si seguimos las recomendaciones y consejos de nuestro amigo *Sebastián Bortnik* – Analista de Seguridad para ESET Latinoamérica en su "Decálogo de seguridad en el ciberespacio.»

1. **Evitar los enlaces sospechosos**: uno de los medios más utilizados para direccionar 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 capaces de infectar al usuario. Los enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social: la clave está en analizar si son ofrecidos en alguna situación sospechosa (una invitación a ver una foto en un idioma distinto al propio, por ejemplo), provienen de un remitente desconocido o remiten a un sitio web poco confiable.

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 descuentos en la compra de productos (o incluso ofrecimientos gratuitos), primicias o materiales exclusivos de noticias de actualidad, material multimedia, etc. Es recomendable para una navegación segura 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 sistema 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 y descargan el código malicioso al momento que el usuario lo instala en el sistema. Por eso, es recomendable que al momento de descargar aplicaciones lo haga siempre desde las páginas web oficiales.

5. **Utilizar tecnologías de seguridad**: las soluciones antivirus, firewall y antispam representan las aplicaciones más importantes para la protección del equipo ante la principales amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante amenazas.

6. **Evitar el ingreso de información personal 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 verificar 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 forma, se pueden prevenir ataques de phishing que intentan obtener información sensible a través de la simulación de una entidad de confianza.

7. **Tener precaución con los resultados arrojados por buscadores web**: a través de técnicas de Black Hat SEO , los atacantes suelen posicionar sus sitios web entre los

primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público, como temas de actualidad, noticias extravagantes o temáticas populares (como por ejemplo, el deporte y el sexo). Ante cualquiera de estas búsquedas, el usuario debe estar atento a los resultados y verificar a qué sitios web está siendo enlazado.

8. **Aceptar sólo contactos conocidos**: tanto en los clientes de mensajería instantánea como en redes sociales, es recomendable aceptar e interactuar sólo con contactos conocidos. De esta manera se evita acceder a los perfiles creados por los atacantes para comunicarse con las víctimas y exponerlas a diversas amenazas como malware, phishing, cyberbullying u otras.

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 conozca la seguridad del mismo y su procedencia sea confiable (tanto si proviene de un contacto en la mensajería instantánea, un correo electrónico o un sitio web). Cuando se descargan archivos de redes P2P, se sugiere analizarlos de modo previo a su ejecución con un una solución de seguridad.

10. **Utilizar 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 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.

    Como siempre, las buenas prácticas sirven para aumentar el nivel de protección y son el mejor acompañamiento para las tecnologías de seguridad. Mientras estas últimas se encargan de prevenir ante la probabilidad de algún tipo de incidente, la educación del usuario logrará que este se exponga menos a las amenazas existentes, algo que de seguro cualquier lector deseará en su uso cotidiano de Internet.

    Aprovechamos el día en cuestión para celebrar con todos ustedes la existencia de Internet, junto a todos los que desde su lugar intentan hacer del uso de las tecnologías una experiencia para bien… y segura.

Fuente:

https://www.infospyware.com/articulos/10-consejos-para-navegar-seguro-por-internet/