Sea ciberinteligente: Poner los "escudos"

Pasos sencillos para la seguridad en línea

Las estafas cibernéticas no son nada nuevo. Cada día, los hackers y otros ciberdelincuentes buscan el objetivo más fácil en internet. ¿Crees que no mereces ser el objetivo de los depredadores de internet? ¡Piénsalo de nuevo!

Ya sea su identidad, la información de su cuenta bancaria o simplemente lo que hay en su correo electrónico, su información es valiosa y los ciberdelincuentes harán todo lo posible para acceder a ella. Cuentan con que usted piense que no es un objetivo. Es hora de que se ponga los ***escudos*** y tome medidas para evitar ser víctima de un ciberdelito.

Empecemos por lo más básico de la ciberhigiene: formas fáciles y de sentido común de protegerse en internet. Estas son las cuatro cosas más sencillas que puede hacer hoy para mantenerse ciberseguro:

- **Utilice más de un tipo de autenticación en todas sus cuentas.** Una contraseña no es suficiente para mantenerlo seguro en internet. Al implementar una segunda capa de identificación, como un mensaje de texto de confirmación, un código de una aplicación de autenticación, la verificación facial o de la huella dactilar, o una clave de seguridad, le está dando a su banco, proveedor de correo electrónico o cualquier otro sitio web en el que se conecte una capa extra de seguridad. La autenticación multifactorial puede reducir hasta en un 99% las probabilidades de que le pirateen o roben su información.

- **Actualice su software.** Los piratas informáticos tratarán de aprovechar los fallos y vulnerabilidades del software. Actualice el software del sistema en todos sus dispositivos, como teléfonos móviles, tabletas y ordenadores portátiles. Asegúrese también de comprobar si hay actualizaciones de sus aplicaciones con regularidad -especialmente los navegadores web- en todos sus dispositivos. Facilite la tarea simplemente activando las actualizaciones automáticas para todos los dispositivos, aplicaciones y sistemas operativos.

- **Piense antes de hacer clic.** Más del 90% de los ciberataques que tienen éxito comienzan cuando se hace clic en un enlace desconocido en un correo electrónico de *phishing*. Un esquema de *phishing* es cuando un enlace o página web parece legítimo, pero es un truco diseñado para que revele sus contraseñas, números de tarjetas de crédito u otra información confidencial. Además, los correos electrónicos de *phishing* pueden ser intentos de hacer que ejecute software malicioso, también conocido como *malware.* Si es un enlace que no reconoce, confíe en sus instintos y piense antes de hacer clic.

- **Utilice contraseñas seguras.** Una contraseña segura debe tener ocho o más caracteres y utilizar una combinación de letras, números y caracteres especiales. Evite utilizar la misma contraseña en diferentes cuentas. Lo ideal es utilizar también un administrador de contraseñas para generar y almacenar contraseñas únicas.

Nuestro mundo es cada vez más digital y cada vez más interconectado, y todos tenemos la responsabilidad de proteger realmente las redes informáticas de las que todos dependemos. Conviértase en un defensor de la ciberseguridad y comparta estos consejos con sus amigos, familiares y vecinos.

Para obtener más información, visite CISA's Shields Up webpage