Boletín mensual de concientización en seguridad para ti

Cuatro sencillos pasos para mantenerse seguro

Resumen

Aprovechar al máximo la tecnología de forma segura puede parecer abrumador y confuso. Sin embargo, independientemente de la tecnología que estés utilizando o cómo la estés utilizando, aquí hay cuatro sencillos pasos que te ayudarán a mantenerte seguro.

1. Tú: Primero y ante todo, la tecnología por sí sola no puede protegerte completamente, tú eres la mejor defensa. Los atacantes han aprendido que la forma más fácil de obtener lo que quieren es dirigiéndose a ti, en lugar de tu computadora u otros dispositivos. Si quieren tu contraseña, tarjeta de crédito o control de tu computadora, intentarán engañarte de alguna manera para que se las proporciones, a menudo creando un sentido de urgencia. Por ejemplo, pueden llamarte fingiendo ser soporte técnico de Microsoft y afirmar que tu computadora está infectada, cuando en realidad son solo cibercriminales que quieren que les des acceso a tu computadora. O tal vez te enviarán un correo electrónico advirtiendo que tu paquete no podrá ser entregado, presionandote para hacer clic en un enlace y confirmar tu dirección postal, cuando en realidad te están engañando para visitar un sitio web malicioso que va a infectar tu computadora. En última instancia, la mayor defensa contra los atacantes eres tú. Mediante el uso de sentido común se puede detectar y evitar muchos ataques.

2. Frases de contraseña: La capacidad de procesamiento de los equipos de cómputo modernos han hecho que la antigua contraseña de 8 caracteres sea anticuada y vulnerable. Cuando un sitio te pida que generes una contraseña, es mejor utilizar una frase de contraseña segura y única. Esta es un tipo de contraseña que utiliza una serie de palabras que es fácil de recordar, como “granos de cafe miel de abeja”. Cuanto más larga sea tu frase de contraseña, más fuerte se vuelve. Una frase de contraseña única significa usar una diferente para cada dispositivo o cuenta en línea. De esta manera, si alguna se ve comprometida, todas las demás cuentas y dispositivos continúan siendo seguros. Ahora bien, ¿te resulta complicado recordar todas esas frases de contraseña? Utiliza un gestor de contraseñas, que es un programa especializado que te permite almacenarlas de forma segura en un formato cifrado (y un montón de otras grandes características también).

Por último, habilita la verificación en dos pasos (también denominada de doble factor o autenticación multifactor). Esta utiliza tu contraseña, pero además agrega un segundo paso, como un código enviado a tu

dispositivo móvil o una aplicación que genera un código. La verificación en dos pasos es probablemente el paso más importante que puedes tomar para proteger tus cuentas en línea y es mucho más fácil de lo que se podría pensar.

3. Actualizaciones: Asegúrate de que cada una de tus computadoras, dispositivos móviles, programas y aplicaciones están ejecutando la última versión. Los ciberatacantes constantemente buscan nuevas vulnerabilidades en el software que utilizan tus dispositivos. Cuando descubren vulnerabilidades, utilizan programas especiales para explotarlas y comprometer los dispositivos que estas utilizando. Mientras tanto, las empresas que crearon el software para estos dispositivos están trabajando para solucionarlas mediante la publicación de actualizaciones. Asegurate que tus equipos y dispositivos móviles cuentan con estas actualizaciones, así haces que sea mucho más difícil comprometerlos. Para mantenerlos al día, simplemente habilita las actualizaciones automáticas siempre que sea posible. Esta regla se aplica a casi cualquier tecnología conectada a Internet, incluidos televisores, monitores para bebés, cámaras de seguridad, ruteadores domésticos, consolas de juegos o incluso tu automóvil.

4. Respaldos y recuperación: A veces, no importa lo cuidadoso que seas, podrían hackearte. Si ese es el caso, a menudo la única manera de restaurar toda tu información personal es desde un respaldo. Asegúrate de realizar respaldos de manera periódica de cualquier información importante y comprueba que es posible restaurar tus datos. La mayoría de los sistemas operativos y dispositivos móviles permiten respaldos automáticamente, en unidades externas o en la nube.

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

Editor Invitado

***Steve Anson**, instructor certificado del Instituto SANS, imparte asesorías para mejorar la seguridad a equipos de seguridad de TI y gobiernos alrededor del mundo. Steve es autor del libro a publicarse próximamente "Applied Incident Response" y proporciona recursos gratuitos para los profesionales de la seguridad de TI en www.AppliedIncidentResponse.com.*

Recursos

Ingeniería Social:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_sp.pdf
Estafas personalizadas:	https://www.sans.org/sites/default/files/2019-02/201902-OUCH-February-Spanish.pdf
Creando contraseñas simples:	https://www.sans.org/u/W3V
¿Realizo respaldos?:	https://www.sans.org/sites/default/files/2019-08/201908-OUCH-August-Spanish.pdf