OUCH! Febrero, 2023

El Boletín Mensual de Concientización en Seguridad para ti

¿Necesito software para protegerme?

Resumen

Cuando compraste una computadora nueva hace años, probablemente tuviste que instalar software de seguridad adicional en tu computadora para asegurarte que estuviera protegida contra los ciberatacantes. Sin embargo, la mayoría de las computadoras y dispositivos de hoy en día tienen varias funciones de seguridad ya integradas, como actualizaciones automáticas, firewalls, cifrado de disco y protección de archivos. Además, Microsoft proporciona en las computadoras con Windows una funcionalidad de seguridad llamada Microsoft Defender, que incluye características adicionales como antivirus. En muchos sentidos, los sistemas actuales son mucho más seguros de forma predeterminada. De hecho, lo más probable es que ahora TÚ seas la mayor debilidad. Esta es la razón por la cual los ciberatacantes continuamente se dirigen a las personas, intentando engañarlas para que hagan cosas que no deberían hacer, como: dar sus contraseñas, hacer clic en enlaces o abrir archivos adjuntos de correo electrónico que instalan malware en sus computadoras o comparten la información de sus tarjetas de crédito.

¿Qué herramientas debería considerar?

Si deseas tomar medidas adicionales para proteger tus sistemas, existen algunos programas de seguridad adicionales que debes tener en cuenta.

Gestores de contraseñas: Las contraseñas pueden ser complejas y abrumadoras, especialmente si tienes que recordar cientos de contraseñas diferentes. Un gestor de contraseñas es una bóveda segura que protege y almacena todas las credenciales de tus cuentas para que solo tengas que recordar una contraseña maestra. Además, pueden iniciar sesión en sitios web, generar contraseñas para ti y ayudarte a validar ciertos sitios web.

Red privada virtual (VPN): las VPN se enfocan principalmente en proteger tu privacidad cifrando tu conexión a Internet y ocultando tu ubicación de origen.

Soluciones de seguridad: Estas son colecciones de software que brindan una serie de características de seguridad adicionales que van más allá de lo que ya ofrece tu sistema operativo. Por ejemplo, filtrado de sitios web peligrosos, controles parentales y, frecuentemente, una VPN. Cada solución tiene características diferentes, así que busca la que consideres mejor si la necesitas.

Eligiendo a un proveedor de seguridad

Si necesitas comprar herramientas de seguridad o software adicional, hay muchos proveedores diferentes para elegir. ¿Cuál deberías elegir? Frecuentemente, las funcionalidades que los diferentes proveedores ofrecen suelen ser muy similares. La clave es utilizar una solución de un proveedor de confianza. No quieres comprar e instalar accidentalmente algo distribuido por ciberdelincuentes que esté infectado con malware.

Compra herramientas solo de proveedores conocidos de los que hayas escuchado hablar y en los que confíes. Nunca compres una herramienta de una empresa de la que no sabes nada, que sea nueva, que no tenga comentarios o que tenga muchos comentarios negativos. Tienes que asegurarte que la solución que estás comprando es legítima, constantemente la actualizan y le dan mantenimiento. Incluso podrías considerar en qué país se encuentra el proveedor. Existen varios sitios en línea que tienen reseñas de proveedores confiables que muestran las diferencias en características y costos de sus soluciones de seguridad.

Ten cuidado con las herramientas gratuitas. Si bien existen excelentes herramientas de seguridad gratuitas, pueden haber algunas preocupaciones. Estas herramientas podrían tener características limitadas, ser difíciles de usar o no actualizarse con frecuencia. En algunos casos, los ciberatacantes pueden haber desarrollado herramientas gratuitas y luego haberlas infectado con malware.

Recuerda, si bien estas herramientas de seguridad son útiles, comienza primero con las funciones de seguridad integradas de tu computadora, lo cual incluye la activación de las actualizaciones automáticas. Los sistemas operativos actuales suelen ser muy seguros de forma predeterminada. Finalmente, tú eres tu mejor defensa. Ten cuidado con cualquier llamada telefónica, correo electrónico o mensaje de texto extraño o sospechoso. Ningún software de seguridad en el mundo puede protegerte de alguien que intenta engañarte para que hagas algo que no deberías hacer.

Editor invitado

Nico "Dutch_OsintGuy" Dekens es instructor certificado de SANS y exanalista de inteligencia gubernamental especializado en inteligencia de fuentes abiertas (OSINT).
Más información sobre Nico aquí:
https://www.sans.org/profiles/nico-dekens/ y aquíhttps://www.dutchosintguy.com.

Recursos

Gestores de contraseñas: https://www.sans.org/newsletters/ouch/password-managers/
El poder de actualizar: https://www.sans.org/security-awareness-training/resources/power-updating
Redes privadas virtuales: https://www.privacyguides.org/vpn/
Ingeniería social: https://www.youtube.com/watch?v=lc7scxvKQOo
Reseñas de soluciones de seguridad:
https://www.pcmag.com/picks/the-best-security-suites

Traducido para la comunidad por: Célica Martínez Aponte and Iván Galindo, UNAM-CERT