Boletín mensual de concientización en seguridad para ti

¿He sido hackeado?

Sinopsis

No importa qué tan seguro te encuentres, al igual que al conducir un automóvil, tarde o temprano puedes tener un accidente. A continuación, se encuentran algunas pistas para ayudarte a identificar si has sido hackeado y en ese caso, qué hacer. Entre más pronto identifiques que algo malo ha sucedido, es más probable que puedas solucionar el problema.

Pistas que indican que has sido hackeado

- **Tu programa antivirus genera una alerta diciendo que tu sistema ha sido infectado. Asegúrate que es tu programa antivirus el que generó la alerta, y no una ventana emergente de una página web tratando de engañarte para que llames a algún número o instales algo más. ¿No estás seguro?, abre tu programa antivirus.**
- **Te aparece una ventana emergente diciendo que tu computadora ha sido cifrada y que tienes que pagar un rescate para recuperar tus archivos.**
- **Tu navegador te lleva a todo tipo de páginas web a las que no quieres acceder.**
- **Tu computadora o aplicaciones fallan constantemente, hay íconos de aplicaciones que no conoces o extrañas ventanas apareciendo.**
- **Tu contraseña ya no funciona, incluso aunque sabes que es correcta.**
- **Tus amigos te preguntan por qué les envías muchos correos que tú no sabes que has enviado.**
- **Hay cargos a tu tarjeta de crédito o retiros de tu cuenta bancaria que nunca hiciste.**

Cómo responder

Si sospechas que has sido hackeado, entre más pronto actúes, mejor. Si el hackeo está relacionado con el trabajo, no intentes resolver el problema tú solo, mejor repórtalo inmediatamente. Si se trata de un sistema o cuenta personal la que ha sido hackeada, aquí hay algunos pasos que puedes seguir:

- **Cambia tus contraseñas.** Esto incluye cambiar también las contraseñas de tus cuentas en línea y no únicamente las de tu computadora y dispositivos móviles. No utilices la computadora hackeada para cambiar tus contraseñas, usa un sistema diferente que sepas que es seguro. Si tienes múltiples cuentas, inicia con las más importantes. Si no puedes mantener un seguimiento de todas tus contraseñas, utiliza un gestor de contraseñas.

Financiero. Para situaciones que involucren tu tarjeta de crédito o cuentas bancarias, llama a tu banco o compañía de crédito inmediatamente. Utiliza un número confiable para marcarles, como el que se encuentra al reverso de tu tarjeta bancaria, en tus estados de cuenta o visita su sitio web desde una computadora confiable. Adicionalmente considera realizar un bloqueo o congelamiento de crédito.

Antivirus. Si tu programa antivirus te informa de un archivo infectado, sigue las acciones que te recomienda. La mayoría de los programas antivirus tienen enlaces que puedes seguir para aprender más sobre esa infección en específico.

Reinstalar. Si no puedes reparar una computadora infectada o quieres estar más seguro que tu sistema está protegido, reinstala el sistema operativo. No reinstales desde respaldos, estos únicamente deberían ser usados para recuperar los archivos personales. Si no te sientes cómodo haciéndolo tú mismo, contrata a un profesional para que te ayude. Si tu computadora o dispositivo es viejo, puede ser más fácil comprar uno nuevo. Finalmente, una vez que hayas reinstalado o comprado un dispositivo nuevo, asegúrate que esté actualizado y habilita las actualizaciones automáticas siempre que sea posible.

Respaldos. Un paso clave para protegerte es prepararse con anticipación con respaldos periódicamente. Varias soluciones pueden respaldar automáticamente tus archivos cada día o incluso cada hora. Sin importar cual solución utilices, revisa regularmente que eres capaz de restaurar dichos archivos. Muchas veces, la única forma de recuperar tus datos después de haber sido hackeado es a través de tus respaldos.

Cumplimiento de la ley. Si te sientes amenazado de cualquier forma, reporta el incidente a la policía local. Si eres víctima de robo de identidad y vives en México, consulta esta guía para prevenir el robo de identidad, así como las autoridades ante las que puedes reportar.

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

El Dr. Johannes Ullrich *(@johullrich) es decano de investigación del SANS Technology Institute, director del SANS Internet Storm Center y miembro de SANS. Él creó la red de sensores colaborativos DShield y participa en el podcast del Internet Storm Center sobre noticias de seguridad de la red.*

Recursos

Respaldos:	https://www.sans.org/u/JGP
Frases de contraseña:	https://www.sans.org/u/JGU
Gestores de contraseñas:	https://www.sans.org/u/JGZ
Qué es malware:	https://www.sans.org/u/JH4