OUCH! | Febrero, 2021

El Boletín Mensual de Concientización en Seguridad para ti

Fui hackeado. ¿Y ahora qué hago?

¿Me han hackeado?

No importa qué tan seguro estés, tarde o temprano puedes tener un accidente y ser hackeado. A continuación, te compartimos algunas pistas que podrían indicarte que fuiste hackeado y, de ser así, qué podrías hacer.

Tus cuentas en línea

- Tu familia y amigos te dicen que recibieron mensajes inusuales o invitaciones tuyas que sabes que jamás enviaste.
- La contraseñas de una de tus cuentas no funciona, a pesar de que sabes que es correcta.
- Recibes notificaciones de sitios web que alguien ha ingresado cuando sabes que no has entrado. No des clic en ningún enlace de dichas notificaciones para verificar tu cuenta; en su lugar, escribe la dirección del sitio web en el navegador, utiliza el marcador previamente guardado o accede desde una aplicación móvil.

Tu computadora o dispositivo móvil

- Tu programa antivirus genera una alerta de que tu sistema está infectado. Asegúrate de que tu software antivirus sea el que genere la alerta y no una ventana emergente aleatoria de un sitio web que intente engañarte para que llames a un número o instales otra cosa. ¿No estás seguro? Abre y verifica el programa antivirus para confirmar si tu computadora está realmente infectada.
- Te aparece una ventana emergente diciendo que tu computadora ha sido cifrada y tendrás que pagar un rescate para recuperarlos.
- Las aplicaciones parecen haberse pasmado aleatoriamente o se cargan muy lento.
- Mientras navegas por la web, frecuentemente eres redirigido o emergen nuevas ventanas de páginas que no deseabas visitar.

Finanzas

- Te aparecen cargos sospechosos o desconocidos a tu tarjeta de crédito o cuentas bancarias que tú no hiciste.

¿Y ahora qué hago? - Cómo recuperar el control

Si sospechas que te han hackeado, guarda la calma; superarás esto. Si la intrusión está relacionada con el trabajo, no intentes solucionar el problema tú mismo; informarlo de inmediato. Si comprometieron un sistema o cuenta personal, aquí hay algunos pasos que puedes seguir:

- **Recuperando tus cuentas en línea:** Si aún tienes acceso a la cuenta, ingresa desde una computadora confiable que estés seguro que no está infectada y restablece tu contraseña. Una vez que ingreses, asegúrate de configurar una contraseña nueva, única y fuerte; mientras más larga mejor. Recuerda que, cada una de tus cuentas debería tener una contraseña diferente. Si no puedes dar seguimiento a todas, te recomendamos utilizar un gestor de contraseñas. También, si es opción, habilita el factor de autenticación múltiple (por sus siglas en inglés MFA) para tus cuentas, ayudando a garantizar que los ciberatacantes no puedan volver a entrar. Si ya no tienes acceso a tu cuenta, comunícate con el sitio web e infórmales que tu cuenta ha sido comprometida.
- **Recuperando tu computadora personal o dispositivos:** Si tu programa antivirus no puede reparar una computadora infectada o si deseas estar más seguro de que tu sistema es seguro, considera reinstalar el sistema operativo y cambiar componentes de la computadora. Esto suele requerir borrar o reemplazar el disco duro y luego reinstalar y actualizar el sistema operativo. No reinstales el sistema operativo desde respaldos. Los respaldos deberían ser utilizados únicamente para recuperar archivos personales. Si te sientes incómodo reemplazando componentes, considera utilizar un servicio profesional. Si tu computadora o dispositivo es viejo, puede ser el momento de comprar uno nuevo.
- **Recuperando tus cuentas financieras:** Sobre cualquier problema con tu tarjeta de crédito o cualquier cuenta financiera, llama a tu banco o compañía de tarjeta de crédito de inmediato. Comunícate utilizando un número de teléfono de confianza, como el que se encuentra al reverso de tu tarjeta bancaria, el impreso en tus estados financieros o visita su sitio web. Revisa tus estados de cuenta y reportes de crédito frecuentemente. Adicionalmente, considera el congelamiento o bloqueo de seguridad para restringir el acceso a tu informe crediticio.

Si has sufrido daños financieros o te sientes amenazado de alguna manera, reporta el incidente a la policía local.

Editor invitado

Maxim Deweerdt (Twitter @alfasec) es instructor certificado del Instituto SANS, imparte principalmente cursos de ciberdefensa. También es consultor en NVISO, donde se enfoca a la detección proactiva de amenazas (en inglés Threat Hunting), respuesta a incidentes y proyectos de madurez de SOC.

Recursos

El Poder de actualizar: https://www.sans.org/security-awareness-training/resources/power-updating
¿Hacer respaldos?: https://www.sans.org/security-awareness-training/resources/got-backups
Creando contraseñas simples: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Ransomware: https://www.sans.org/security-awareness-training/resources/ransomware
Reporta el robo de identidad: https://www.identitytheft.gov
Congelamiento de crédito: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

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