Consejos para la protección de la computadora

Hoy en día, utilizamos computadoras para todo. PERO… ¿qué pasa cuando hackean su computadora? A continuación, se indican algunos pasos sencillos pero muy importantes que puede seguir para evitar que los hackers accedan a su computadora e información personal.

Utilice contraseñas fuertes.

- **Haz un respaldo de su información con frecuencia.** Usted puede copiar sus datos a un CD, DVD, dispositivo USB o a un disco duro externo. De esta forma, si su computadora se cuelga o es hackeada, no perderá toda su información.
- **Nunca le dé a alguien acceso remoto a su computadora**. Si usted recibe una llamada de alguien reclamando ser de Microsoft o cualquier otra empresa diciendo que tiene un virus o que pueden arreglar otros problemas con su computadora, cuelgue inmediatamente. Los estafadores intentarán convencerle de pagar servicios no necesarios y conseguir acceso a su computadora para obtener información personal o instalar software malicioso.
- **Actualice su sistema operativo regularmente.** Los sistemas operativos de las computadoras se actualizan periódicamente para mantenerse al día con los requisitos tecnológicos y para arreglar los puntos débiles que pueden ser atacados por los hackers. Asegúrese de instalar las actualizaciones para estar seguro de que su computadora tiene la última versión. A menudo hay configuraciones en su sistema operativo para hacer estas actualizaciones automáticas.
- **Utilice contraseñas fuertes y cámbielas con frecuencia**. No utilice la misma contraseña para cuentas múltiples. Utilice contraseñas que contengan letras minúsculas y mayúsculas, números, y símbolos. Cambie su contraseña cada tres meses y no reúse las contraseñas. Esto es especialmente cierto para las contraseñas que se utilizan para acceder a su correo electrónico y cuentas bancarias.
- **Use un doble factor de autenticación**. Un doble factor de autenticación es una herramienta de seguridad agregada que combina cosas que usted posee, ya sea desde un token físico, como una tarjeta o un código, hasta algo que usted sabe de memoria, como una contraseña o un PIN.
- **No haga clic en ventanas emergentes**. Las ventanas emergentes en internet son herramientas de publicidad rápida, pero ten cuidado con las ofertas "demasiado buenas para ser verdad". Estas ventanas emergentes no solo pueden reducir la velocidad de su computadora e internet, sino que al hacer clic en estos puede accidentalmente registrarse para servicios no autorizados. Establezca la barra de información en su navegador para no permitir ventanas emergentes.
- **Tenga cuidado con lo que descarga.** Unos de los virus más destructivos se han ocultado en programas del internet y aplicaciones o archivos adjuntos de correos electrónicos. Esté seguro de solo descargar de una fuente confiable. En cuanto a los correos electrónicos, nunca haga clic en

enlaces o archivos adjuntos si no reconoce al remitente. Incluso si conoce el remitente, ¡cuidado! Es posible que su computadora fue hackeada y está enviando correos electrónicos infectados. Esos correos electrónicos también podrían ser muy bien disfrazados para parecerse a reconocidas instituciones financieras o sitios web minoristas, enviados para conseguir su información personal.

- **No envíe información confidencial o personal a través del correo electrónico**. El correo electrónico no suele ser cifrado, o en otras palabras no en un "código secreto," y puede ser interceptado y leído por hackers.
- **Utilice software antivirus y configúrelo para actualizarse a diario.** Hay muchos productos comerciales que pueden ayudarle a proteger su computadora de los virus maliciosos. La mayoría de la protección de software tiene una característica que escaneará archivos descargados automáticamente y algunos incluso escanearán correos electrónicos entrantes por defecto.
- **Evite instalar software innecesario, desconocido o no probado.** Esto incluye juegos, barras de herramientas o salvapantallas que podrían dejar su computadora vulnerable a ataques. A menudo se instalan spyware y los virus al descargar programas desconocidos. Compruebe para asegurarse que cuando usted instale el software que quiere, el programa no está incluyendo otras barras de herramientas o software en la instalación. Busque casillas automáticamente marcadas en la página del acuerdo dando su permiso para instalar estos otros artículos.
- **Utilice un cortafuego personal.** Un cortafuego actúa como una barrera entre usted y el internet. Ayuda a mantener los hackers fuera y ayuda a prevenir que el software malicioso envíe su información personal a criminales. Hay versiones minoristas y gratuitas disponibles y los cortafuegos pueden venir en la forma de software y hardware.

- **Tenga cuidado con las redes inalámbricas.** Para su red doméstica, asegúrese de que su enrutador esté protegido por contraseña. Para acceso a redes públicos (tales como en restaurantes, bibliotecas o cafés), preste atención si la red no es segura. Los criminales cibernéticos aprovechan estas redes inseguras para hackear su computadora y acceder a sus datos personales.
- **Apague su computadora cuando no esté en uso.** Dejando su computadora prendida y sin uso podría dejarla expuesta a un ataque por hackers. Proteja su computadora, y ahorre energía apagando su computadora cuando no la está usando.
- **Deseche su computadora de manera segura.** Asegúrese de que todos los datos personales se eliminen mediante el borrado o destrucción físico del disco duro de su computadora.

Si su computadora ha sido hackeada y usted siente que su seguridad está en peligro, o piensa que el hacker es alguien que usted conoce, debe llamar a la policía local.

Póngase en contacto con un profesional de la informática local confiable para remover cualquier software malicioso que pudiera haber sido instalado.

La tecnología continúa cambiando y evolucionando. Es posible que no pueda evitar todo el hacking, pero puede ayudar a equiparse con las herramientas y el conocimiento para proteger su computadora de los delincuentes cibernéticos.

También usted puede encontrar más consejos útiles en nuestra publicación "Redes Sociales."

Para obtener más información o para presentar una queja contáctese con:

Department of Agriculture, Trade and Consumer Protection

Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Correo electrónico: DATCPHotline@wi.gov
Sitio web: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftComputerProtection907 (rev 4/23)