Malware

Obtenga información sobre cómo identificar, evitar y abordar el malware en diferentes tipos de dispositivos.

1. ¿Qué es el malware?

Malware significa “software malicioso” y es una especie de término general que cubre diferentes tipos de software que pueden infectar o alterar un dispositivo, u obtener acceso no autorizado a este.

El malware puede infectar computadoras, teléfonos y tabletas. Estas son algunas formas habituales de malware que puede haber escuchado antes:

- **Ransomware:** malware que puede encriptar archivos y bloquearle el acceso a alguien de su dispositivo.
- **Spyware:** malware que recopila información sobre el usuario.
- **Adware:** suele adoptar la forma de anuncios emergentes descontrolados.
- **Gusanos:** un tipo de virus que en realidad se copia a sí mismo y se envía a otros usuarios.
- **Virus:** una forma de malware que puede infectar dispositivos y dañar datos y software. Los virus se reproducen replicándose a sí mismos a través de códigos.

¿Cuáles son algunos tipos de virus?

- **Virus troyano:** un tipo de virus informático famoso que ingresa a un dispositivo camuflado como un programa legítimo. Se engaña a los usuarios para que instalen o descarguen algo que contiene un virus troyano.
- **Secuestrador de navegadores:** virus que pueden infectar un navegador y cambiar su configuración, o redirigir a los usuarios a sitios maliciosos.
- **Virus en macros:** virus que pueden infectar el macro en Microsoft Word.

- **Virus de sobrescritura:** un virus que puede infectar y propagarse entre archivos informáticos críticos.

2. ¿Cómo puede saber si tiene un malware?

Por desgracia, no siempre es sencillo detectar el malware. Sin embargo, hay algunas señales a las que puede prestar atención para determinar si tiene o no un malware en su dispositivo.

Una medida que puede tomar es instalar un software de seguridad que analizará su dispositivo en busca de malware. Sin embargo, investigue y asegúrese de descargar una herramienta legítima. Algunos malware en realidad simulan ser un software de seguridad y lo engañan para que los instale.

Tenga en cuenta que algunas versiones de software de seguridad pueden costarle dinero. No obstante, hay opciones de diferentes precios, y muchos dispositivos tienen un software de seguridad instalado, por lo que puede decidir cuál es la mejor opción para usted.

Estas son algunas formas de identificar un posible malware:

- Su dispositivo funciona de forma muy lenta o se bloquea constantemente.
- No puede apagar ni reiniciar su dispositivo.
- Faltan archivos.
- Recibe mensajes inesperados de error.
- Nota correos electrónicos masivos y extraños que se envían desde su cuenta.
- El navegador comienza a redirigirlo o se retrasa.
- Siguen apareciendo ventanas emergentes o anuncios excesivos o molestos.
- La batería se agota rápido.
- (Para las computadoras portátiles) El ventilador funciona de forma constante y hace ruido.
- Ve anuncios, pestañas abiertas y elementos que no abrió ni instaló en su dispositivo.

3. ¿Qué puede hacer si tiene un malware?

Si sospecha que descargó un malware o que su computadora está infectada con uno, controle para ver si hay un software malicioso presente y proceda a eliminarlo.

Es útil verificar y confirmar su sospecha primero, ya que algunas de las señales de malware pueden en realidad significar otros problemas. Por ejemplo, el agotamiento rápido de la batería podría solo significar que el dispositivo es antiguo.

Sin embargo, si descubre que tiene un problema más grande, debe hacer lo siguiente:

- Deje de hacer determinadas acciones, como comprar en línea o ingresar las contraseñas de sus cuentas, hasta no haber solucionado el problema. Cambie sus contraseñas después de haber solucionado el inconveniente.
- Si su dispositivo forma parte de una red, desconéctelo para evitar la propagación del malware.
- Reinicie el dispositivo en modo seguro para ejecutar mejor el software de seguridad y tratar la infección del malware.
    - **Windows:** oprima y mantenga presionada la tecla F8 en cuanto comience el reinicio, y luego elija la opción Safe Mode en el menú. Luego, ejecute el escaneo del software de seguridad.
    - **Mac:** mantenga presionada la tecla Mayús mientras el dispositivo se reinicia, y luego ejecute el escaneo del software de seguridad.
- Asegúrese de que el software de seguridad esté actualizado.
- Si no tiene un software de seguridad instalado, instale uno confiable para su dispositivo particular. Puede buscar recomendaciones y listas de fuentes legítimas, como sitios de reseñas tecnológicas y blogs, como *Wirecutter* de *The New York Times* (https://www.nytimes.com/wirecutter/).
- Cuando tenga instalado un software de seguridad, ejecute un escaneo en el dispositivo para ver si hay un malware presente.

- Use el software de seguridad para ayudar a eliminarlo.
- Para infecciones más graves, es posible que deba reinstalar su sistema operativo. Visite el sitio web oficial del fabricante de su dispositivo para obtener instrucciones sobre cómo hacerlo.
- Si aún necesita ayuda, comuníquese con el soporte técnico de su dispositivo (puede estar cubierto por la garantía).
- Cambie su contraseña y controle las cuentas para detectar fraudes después de una infección de malware.

4. ¿Cómo puede evitar el malware?

Estas son acciones que puede realizar para proteger sus dispositivos de malware:

- **Tenga cuidado al instalar software, aplicaciones y extensiones de navegadores.**
  El malware puede ocultarse en estos elementos, por lo que debe asegurarse de instalar software confiable y legítimo en su dispositivo.

- **Mantenga actualizada la configuración de seguridad en sus dispositivos y navegadores.**
  Instale las actualizaciones del sistema operativo, los parches y las actualizaciones de seguridad de forma oportuna.

- **Manténgase alerta.**
  Busque fraudes de suplantación de identidad, y evite hacer clic en enlaces o descargar archivos de fuentes sospechosas o desconocidas.

- **Preste atención a los sitios web que visita.**
  No ignore las advertencias del navegador sobre sitios inseguros.

- **Haga una copia de seguridad de sus datos con regularidad.**

Esto le ayudará a mantenerlos protegidos y a poder recuperarlos en caso de que acabe con un malware.

- **Instale un software de seguridad.**

Úselo para controlar su dispositivo y bloquear, detectar y eliminar malware.

5. Haga un plan

Use este espacio para escribir sus planes e ideas sobre acciones que puede hacer para evitar el malware: