

3.3 Pautas y recomendaciones

PAUTAS Y RECOMENDACIONES PARA FAMILIAS Y EDUCADORES

Virus en Android: ¿cómo detectar si mi dispositivo está infectado?

Como bien sabemos, en Internet circulan infinidad de virus y malware que pueden poner nuestros equipos informáticos en riesgo, y precisamente en el caso de Android, en los últimos años han comenzado a proliferar notablemente este tipo de amenazas.

- Se abren anuncios y publicidad extraña
- El dispositivo funciona más lento de lo normal, deja de responder o se bloquea con frecuencia.
- Comportamiento extraño del dispositivo (se apaga solo aun teniendo batería).
- Las aplicaciones no funcionan correctamente.
- El antivirus se desactiva solo.
- Los programas se inician de forma espontánea.
- Creación de accesos directos a páginas no deseadas, es decir a servidores DNS falso.
- Aumento en el uso de datos

¿Qué podemos hacer si nuestro dispositivo está infectado?

Ante la sospecha de que nuestro ordenador o teléfono ha sido infectado por un virus, debemos reaccionar rápidamente y llevar a cabo las siguientes medidas siguiendo el consejo de especialistas como la que se encuentra en la revista Computer:

1º Controla los permisos de las aplicaciones

| Permisos | Concede | Niega | | --- | --- | --- | | Acceso a los ajustes | Sólo las apps de Google deberían pedirte este permiso, para asegurarse de que el dispositivo puede ejecutar todos los procesos que cada aplicación requiere. | Sólo las aplicaciones primarias de Google necesitan utilizar este permiso, así que si cualquier aplicación que requiera este permiso, desinstálala enseguida. | | Modificación | La mayoría de las apps basadas en medios sociales usa esta función para guardar archivos en la tarjeta SD. Y sobre todo es muy común en las apps que usan vídeo. | Cualquier app con acceso a los contenidos de la tarjeta SD puede instalar un virus en ella. También pueden robar archivos o borrarlos de la tarjeta. | | Uso de la ubicación | Sólo suele ser importante

para las apps de navegación tipo Google Maps. Otras aplicaciones quieren acceder a estos permisos para mostrar sitios de interés cercanos. | Las apps maliciosas pueden reunir información sobre tu ubicación y los lugares a los que vas, para enviarte anuncios basados en tu localización. | ID del dispositivo e información de las llamadas | El principal uso de este permiso es leer el ID del teléfono y su estado, esto está bien cuando se accede a diferentes redes sociales o cuentas de correo electrónico. | Este permiso da acceso a tu número de teléfono, que podría ser utilizado por una aplicación maliciosa para enviarte spam constantemente. | | Hacer llamadas | Se trata de un permiso muy común para aplicaciones que permitan realizar llamadas de voz dentro de ellas, y que son independientes de la app Teléfono del dispositivo. | Hay aplicaciones que usan este permiso para marcar números de tarificación especial. Estas pueden ser de hasta 2 €/minuto. Así que cuidado. |

2. Tipo de infección. La mayoría de las infecciones en smartphones vendrán en forma de pop-ups, o un simple malware. Aunque no son muy perjudiciales para tu dispositivo, pueden ralentizar el rendimiento del teléfono o la tableta. Acude al cajón de aplicaciones para intentar encontrar cuál es la aplicación problemática.

3. Análisis antivirus. Incluso cuando creas que ya has identificado la aplicación problemática, haz un análisis antivirus completo del dispositivo. Descarga la aplicación Avast y selecciona la opción “Ejecutar análisis” disponible en la pantalla principal de la aplicación. Puedes escanear el dispositivo con un antivirus online. Aquí se muestran algunos:

- <http://www.pandasecurity.com/spain/>
- <http://www.bitdefender.es/scanner/online/free.html>
- <http://www.zonavirus.com/antivirus-on-line/>
- **Escanear el dispositivo con herramientas Anti Malware y AntiSpyWare.**
- **Desinstala aplicaciones problemáticas.**

Existen métodos avanzados de desinfección de virus que pueden realizarse sin llevar el dispositivo a un servicio técnico, pero requieren conocimientos avanzados de Informática, y pueden suponer un riesgo de pérdida de información si no se tiene claro lo que se está haciendo.

En la Oficina de Seguridad del Internauta se ofrecen instrucciones detalladas para llevar a cabo la desinfección, siempre bajo la responsabilidad del usuario.

<http://www.osi.es/es/desinfecta-tu-ordenador>

Revision #1

Created 1 February 2022 12:07:30 by Equipo CATEDU

Updated 1 February 2022 12:07:30 by Equipo CATEDU