Consejos para prevenir el ingreso de malware a dispositivos Android

Para proteger un **dispositivo Android** de la posible descarga de virus, aunque sea de forma accidental, la presencia de un **antivirus** entre las aplicaciones es más que necesario. Sobre todo cuando se han presentado casos en los que incluso **Play Store**, con su función de **Play Protect**, no es suficiente para evitar que malware se infiltre en la descarga de aplicaciones.

Sin embargo, dejar la **protección** del dispositivo únicamente a sistemas informáticos que pueden ser hackeados o infiltrados, abre la posibilidad que las personas hagan un uso irresponsable o imprudente de los dispositivos. La primera línea de defensa es el **comportamiento de los usuarios**.

Es por eso que se presentan algunos consejos que pueden seguir los usuarios de **Android** para evitar ser víctimas de **malware**.

La presencia de un antivirus en los dispositivos Android es necesaria para evitar que malware se infiltre en la descarga de aplicaciones. (20Minutos)

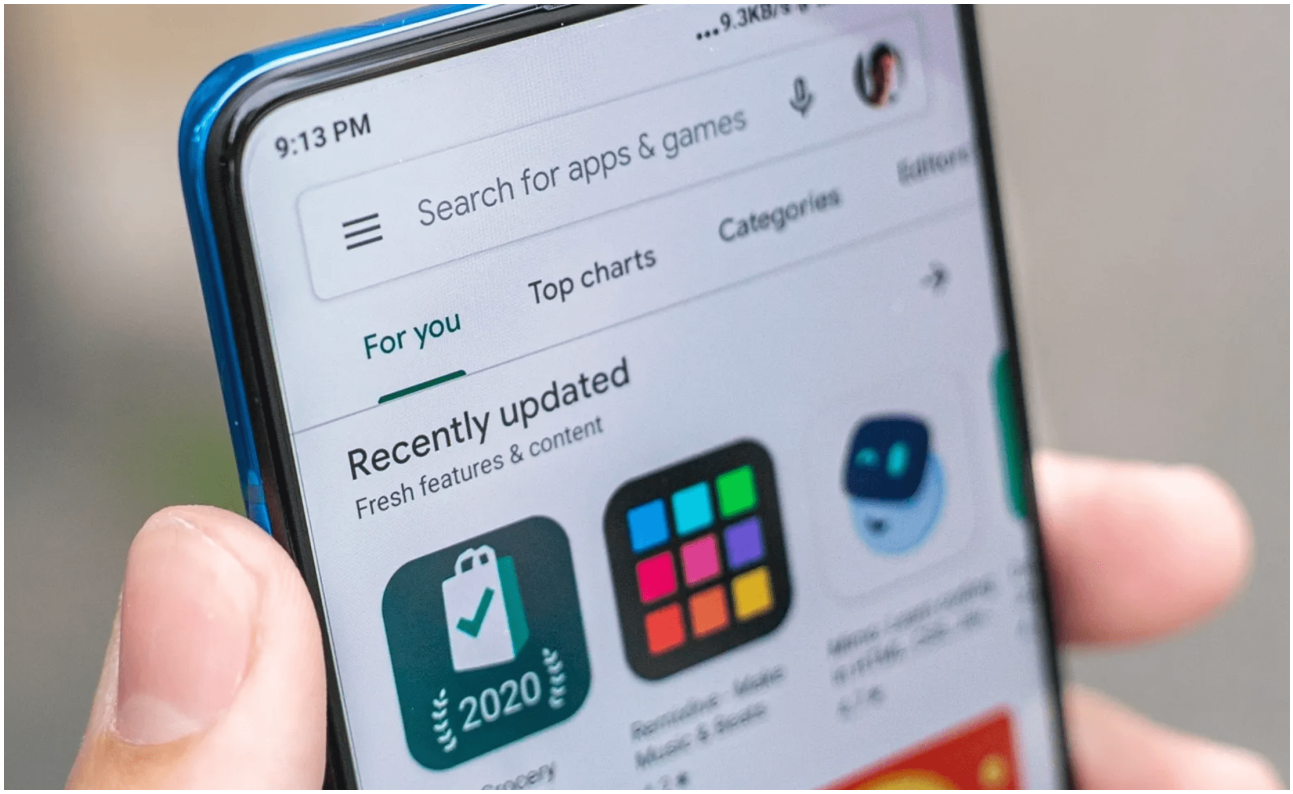
Verificar las actualizaciones de aplicaciones y software

Google, como desarrollador del sistema operativo de **Android**, al igual que los creadores de las aplicaciones que los usuarios tienen descargadas en sus dispositivos; suelen ofrecer **actualizaciones**que, además de añadir características visuales y nuevas funciones, agrega **parches de seguridad** para proteger a los dispositivos.

Los usuarios deben estar atentos y revisar cada cierto tiempo si Play Store tiene disponibles algunas actualizaciones de las aplicaciones del dispositivo. En caso sí pueda realizarse la descarga, es necesario hacerlo tan pronto como sea posible.

Atención con las descargas

Es importante mantener la guardia alta y desconfiar de cada archivo o aplicación que se descargue, así sea desde la **tienda de Google**. El usuario debe asegurarse de que el antivirus que tenga disponible realice un diagnóstico del dispositivo cada vez que se haga una descarga para detectar amenazas.



Archived APK para Android. (foto: Google)

En caso de que se quiera descargar una aplicación como **APK**, pues no está disponible en Play Store, lo recomendable es hacerlo desde un **sitio web confiable** para evitar la descarga simultanea de malware.

Control de los permisos de las ‘apps’

Luego de ser descargadas, las aplicaciones suelen **solicitar permisos** a los usuarios

para acceder a determinados espacios dentro del sistema del dispositivo. Sin embargo, es importante prestar atención a tres que son la puerta de ingreso de malware: accesibilidad, **SMS y notificaciones**.

Tanto el acceso a los mensajes de texto como a las notificaciones es usado por **aplicaciones maliciosas** para poder usar códigos de verificación relacionados a cuentas de banco u otras aplicaciones que contienen información sensible.

Las aplicaciones maliciosas buscan que el usuario otorgue permisos que les den acceso a mensajes de texto y notificaciones, pues se usan para emitir códigos de verificación de cuentas bancarias. (Business Insider España)

La cámara, el micrófono y la localización también son funciones a las que intentan acceder los **cibercriminales**. Dentro de lo posible, no se debe otorgar ningún permiso a las aplicaciones a no ser que sea absolutamente necesario.

Evitar la conexión a redes públicas

Las redes públicas o sin contraseña son puertas abiertas para que cibercriminales accedan a la información que el usuario consulte durante la conexión. Cuentas de banco, url de sitios web, **credenciales de acceso** a perfiles, entre otros datos relevantes y que amenazan la seguridad.

En caso de que sea necesario establecer una conexión a estas redes, usar una **VPN**es lo más adecuado para proteger la privacidad durante la navegación.

VPN. (foto: Redes Zone)

No ingresar en sitios web maliciosos

Ligeramente relacionado con la recomendación acerca de la **descarga de APKs,** el no ingreso a sitios web maliciosos es importante para evitar el acceso de malware, ya sea en dispositivos móviles como en computadoras de escritorio.

En el caso de algunos navegadores, estos tienen integrados filtros de navegación que protegen a los usuarios de acceder a estos sitios y, aunque en ocasiones también se

filtran **páginas seguras**, esta configuración da la posibilidad de que se acceda a estos sitios de todas formas.

La recomendación aplica también para links de sitios web que se envían por SMS o **mensajes de WhatsApp**. De ser posible, se tiene que preguntar a quien envió el link si realmente quiso hacerlo, para descartar virus, o a qué página web dirige.