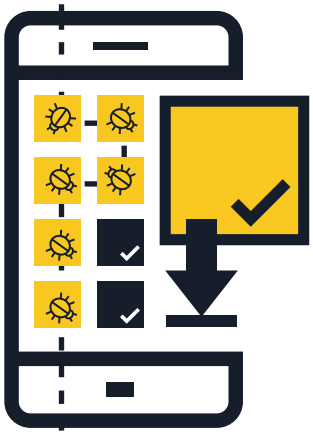
EUROPOL EC3 European Cybercrime Centre

SOFTWARE MALICIOSO EN DISPOSITIVOS MÓVILES

PAUTAS Y CONSEJOS PARA ESTAR PROTEGIDO

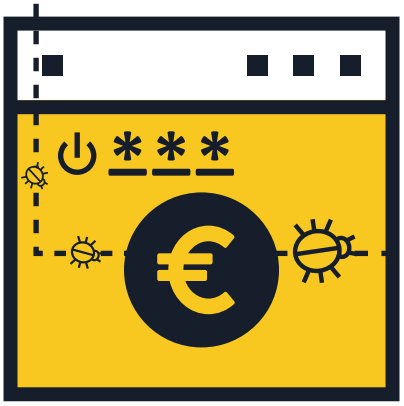
1 Instala aplicaciones solo de fuentes fiables



- **Compra en tiendas de apps con buena reputación** — Antes de descargar una app, realiza una búsqueda sobre ella y sobre sus autores. Ten cuidado con los enlaces que recibas por correo electrónico o a través de mensajes de texto. Es posible que sean un engaño para que instales apps desconocidas.
- **Comprueba las opiniones y calificaciones de otros usuarios.**
- **Lee los permisos de la app** — Comprueba los datos a los que puede acceder y si comparte información con terceros. Si las condiciones te hacen dudar o sospechar, no la descargues.

2 No pinches en los enlaces ni descargues los adjuntos de correos electrónicos o mensajes de texto no solicitados

- **No te fíes de los enlaces que aparezcan en correos electrónicos o mensajes de texto** (SMS y MMS) **no solicitados** — Bórralos nada más recibirlos.
- **Ten mucho cuidado con las URL abreviadas y los códigos QR** — Podrían llevarte a webs peligrosas o descargar directamente software malicioso en tu dispositivo. Antes de pinchar, utiliza un sitio de vista previa de URL para confirmar que la dirección web es legítima. Antes de escanear un código QR, utiliza un lector que ofrezca la vista previa de la dirección web que contiene y utiliza software de seguridad móvil que te avise de los enlaces peligrosos.



3 Sal de los sitios después de efectuar un pago

- **Nunca guardes nombres de usuario ni contraseñas en tu navegador o apps móviles** — Si te roban el teléfono o la tablet o se extravían, cualquiera podrá entrar en tus cuentas. Una vez completada la operación, sal de los sitios en vez de simplemente cerrar el navegador.
- **No compres ni realices operaciones bancarias por internet utilizando redes wifi públicas** — Hazlo solo desde redes que conozcas y en las que confíes.
- **Comprueba dos veces la URL del sitio** — Asegúrate de que la dirección es correcta antes de iniciar sesión o enviar información sensible. Piensa en la opción de descargarte la app oficial de tu banco para estar seguro de que siempre te conectas a su verdadero sitio.

4 Mantén actualizados tu sistema operativo y apps

- **Descarga las actualizaciones para el sistema operativo de tu dispositivo móvil en cuanto se publiquen** — Las últimas actualizaciones no solo harán que tu dispositivo sea más seguro, también que funcione mejor.

5 Apaga los servicios de wifi, ubicación y Bluetooth cuando no los uses

■ **Apaga la wifi cuando no la utilices** — Los ciberdelincuentes pueden acceder a tu información si la conexión no es segura. Si es posible, utiliza una conexión de datos 3G o 4G en vez de puntos de acceso. También existe la opción de una red privada virtual (VPN) para que el tránsito de datos sea cifrado.

■ **No dejes que las apps accedan a tu ubicación salvo que sea necesario** — Esta información podría compartirse o filtrarse y usarse para mostrar anuncios según los sitios en los que estés.

■ **Apaga el Bluetooth cuando no lo necesites** — Asegúrate de que está apagado del todo y no solo en modo invisible. La configuración predeterminada suele permitir que otros se conecten a tu dispositivo sin que lo sepas. Un usuario con malas intenciones podría copiar tus archivos, acceder a otros dispositivos anexos y hasta acceder en remoto a tu teléfono para llamar y enviar mensajes de texto, haciendo subir la factura.

6 Evita dar información personal

■ **Nuca respondas con información personal** a correos o mensajes que dicen ser de tu banco u otras empresas conocidas. Habla directamente con ellos para confirmar la solicitud.

■ **Repasa con frecuencia tus facturas de móvil para ver si hay algún cobro sospechoso** — Si ves gastos que no has hecho, habla con tu operadora inmediatamente.

7 No hagas jailbreak en tu dispositivo

■ Hacer jailbreak consiste en eliminar las limitaciones de seguridad impuestas por el proveedor del sistema operativo, accediendo así a todas las características y funciones del sistema operativo — **Hacer jailbreak en tu dispositivo puede provocar que sea mucho más inseguro y** crear fallos de seguridad que en un principio no estaban patentes.

8 Haz copias de seguridad

■ **Muchos smartphones y tablets son capaces de crear copias de seguridad de forma inalámbrica** — Consulta las opciones del sistema operativo de tu dispositivo. Al crear una copia de seguridad de los datos en tu smartphone o tablet, puedes recuperarlos fácilmente si alguna vez se extravía, te lo roban o se rompe.

9 Instala una app de seguridad móvil

■ Todos los sistemas operativos corren el riesgo de ser infectados. Si dispones de ella, **utiliza una solución de seguridad móvil** que detecte y evite malware, spyware y apps maliciosas, además de ofrecer otras funciones para proteger la privacidad y antirrobo.