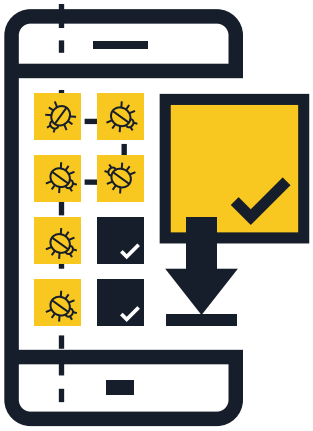
MOBILE MALWARE

TIPS & ADVICE TO PROTECT YOURSELF

1 Install apps from trusted sources only



- **Shop at reputable app stores** — Before downloading an app, research both the app and its publishers. Be cautious of links you receive in email and text messages that might trick you into installing apps from third party or unknown sources.
- **Check other users' ratings and reviews** if available.
- **Read the app's permissions** — Check which types of data the app can access, and if it might share your information with external parties. If you are suspicious or uncomfortable with the terms, don't download the app.

2 Don't click on links or attachments in unsolicited emails or text messages

- **Don't trust links in unsolicited emails or text messages** (SMS and MMS) — Delete them as soon as you receive them.
- **Double-check shortened URLs and QR codes** — They could lead to harmful websites or directly download malware to your device. Before clicking, use a URL preview site to confirm that the web address is legitimate. Before scanning a QR code, choose a QR reader that previews the embedded web address and use mobile security software that warns you of risky links.

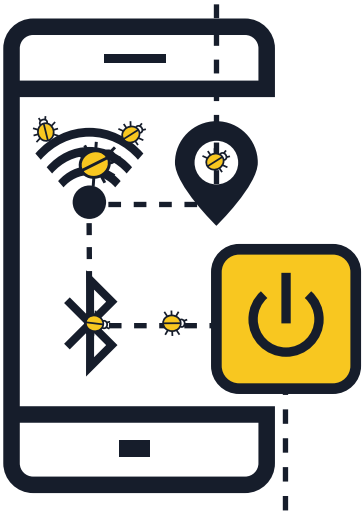
3 Log out of sites after you have made a payment

- **Never save usernames and passwords in your mobile browser or apps** — If your phone or tablet is lost or stolen, anybody could log in to your accounts. Once the transaction is completed, log out of the site instead of just closing the browser.
- **Don't bank or shop online using public Wi-Fi connections** — Only do online banking and transactions from networks you know and trust.
- **Double-check the site URL** — Ensure that the web address is correct before logging in or sending sensitive information. Consider downloading your bank's official app to ensure you are always connecting to the real site.

4 Keep your operating system and apps updated

- **Download software updates for your mobile device's operating system as soon as you are prompted** — Having the latest updates will ensure that your device is not only more secure, but it also performs better.

5 Turn off Wi-Fi, location services and Bluetooth when not in use



- **Turn off Wi-Fi if you are not using it** — Cybercriminals can access your information if the connection is not secure. If possible, use a 3G or 4G data connection instead of hotspots. You can also opt for a virtual private network (VPN) service to keep your data encrypted in transit.
- **Don't allow apps to use your location services unless they need to** — This information may be shared or leaked and used to push ads based on your whereabouts.
- **Turn off Bluetooth when you don't need it** — Ensure it is turned off completely and not just in invisible mode. The default settings are often pre-set to allow others to connect to your device without your knowledge. Malicious users could potentially copy your files, access other devices attached or even gain remote access to your phone to make calls and send text messages, resulting in expensive bills.

6 Avoid giving out personal information

- **Never respond with personal information** to text messages or emails claiming to be from your bank or another legitimate business. Instead, contact the business directly to confirm their request.
- **Regularly review your mobile statements to check for any suspicious charges** — If you identify expenses that you have not made, contact your service provider immediately.

7 Don't jailbreak your device

- Jailbreaking is the process of removing the security limitations imposed by the operating system vendor, gaining full access to the operating system and features — **Jailbreaking your own device can significantly weaken its security**, opening security holes that may not have been readily apparent.

8 Back up your data

- **Many smartphones and tablets have the capability to back up data wirelessly** — Consult the options depending on your device's operating system. By creating a backup for your smartphone or tablet, you can easily restore your personal data if the device is ever lost, stolen or damaged.

9 Install a mobile security app

- All operating systems are at risk of infection. If available, use a **mobile security solution** that detects and prevents malware, spyware and malicious apps, alongside other privacy and anti-theft features.

EUROPOL EC3 European Cybercrime Centre | NCA National Crime Agency | Lookout | #MobileMalware