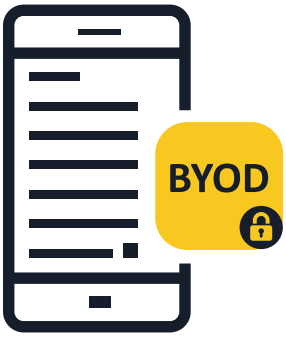
# MOBILE MALWARE

## TIPS AND ADVICE FOR BUSINESSES

### 1 Inform your staff about mobile risks

- Mobile working blurs the lines between corporate and personal usage. Enterprises can be severely impacted by an attack initially directed at an individual's mobile device. A mobile device is a computer and should be protected like one.




### 2 Implement a corporate bring-your-own-device (BYOD) policy

- Employees using their own mobile devices to access enterprise data and systems (even if just email, calendar or contact database) should follow company policies. Carefully choose which technologies will be used to manage and secure mobile devices and encourage your staff to exercise caution.

### 3 Include mobile security policies as part of your overall security framework

- If a device does not comply with security policies, it should not be allowed to connect to the corporate network and access corporate data. Companies should deploy their own Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solutions.
- To complement this, it is critical to install a Mobile Threat Defence solution. This will provide enhanced visibility and contextual awareness of apps, network and operating system level threats.

### 4 Be wary of using public Wi-Fi networks to access company data

- In general, public Wi-Fi networks are not secure. If an employee is accessing corporate data using a free Wi-Fi connection at an airport or coffee shop, the data may be exposed to malicious users. It is advised that companies develop effective use policies in this regard.

## 5 Keep device operating systems and apps updated

- Advise your staff to download software updates for their mobile device's operating system as soon as they are prompted. Especially for Android, research mobile providers and handset manufacturers to know their updates policy. Having the latest updates will ensure that the device is not only more secure, but also performs better.

## 6 Install apps from trusted sources only

- Companies should only permit the installation of apps from official sources on those mobile devices that connect to the enterprise network. As an option, consider building an enterprise application store through which end users can access, download and install corporate-approved apps. Consult your security vendor for set up advice, or build your own in-house.

## 7 Prevent jailbreaking

- 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 a device can significantly weaken its security, opening security holes that may not have been readily apparent. Root-enabled devices should not be allowed in the company environment.

## 8 Consider cloud storage alternatives

- Mobile users often want to access important documents not only via their work PCs but also from their private phones or tablets outside of the office. Companies should assess building a secure cloud-based storage and file-syncing services to accommodate such needs in a secure manner.

## 9 Encourage your staff to install a mobile security app

- All operating systems are at risk of infection. If available, make sure they 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

ERSTE Bank

#MobileMalware