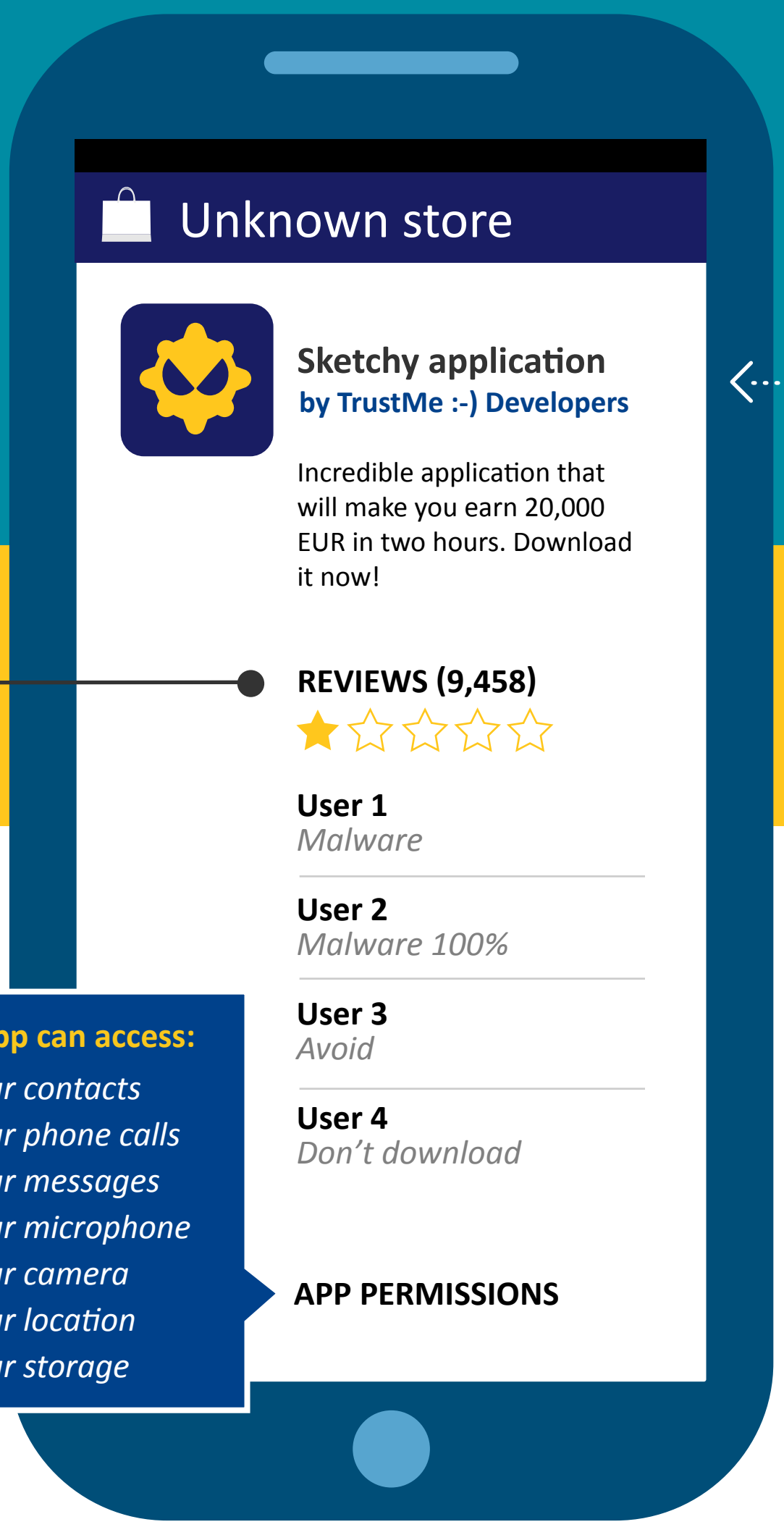
APPS

JUST A GAME?

Only install apps from official app stores

Before downloading an app, research 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' REVIEWS AND RATINGS

READ THE APP'S PERMISSIONS

Check which types of data the app can access, and if it might share your information with external parties. Does it need all these permissions? If not, don't download it.

INSTALL A MOBILE SECURITY APP

It will examine all the apps on your device and each new one you install later, alerting you if malicious software is found.

EUROPOL EC3 European Cybercrime Centre

NCA National Crime Agency

Lookout

#MobileMalware

MOBILE BANKING MALWARE

MALWARE CAN COST YOU MONEY

Mobile banking malware is designed to steal the financial information stored on your mobile device.

HOW DOES IT SPREAD?

- Visiting malicious websites
- Downloading malicious apps
- Phishing

WHAT ARE THE RISKS?

- Capture of your personal authentication information
- Unauthorised withdrawals

WHAT CAN YOU DO?

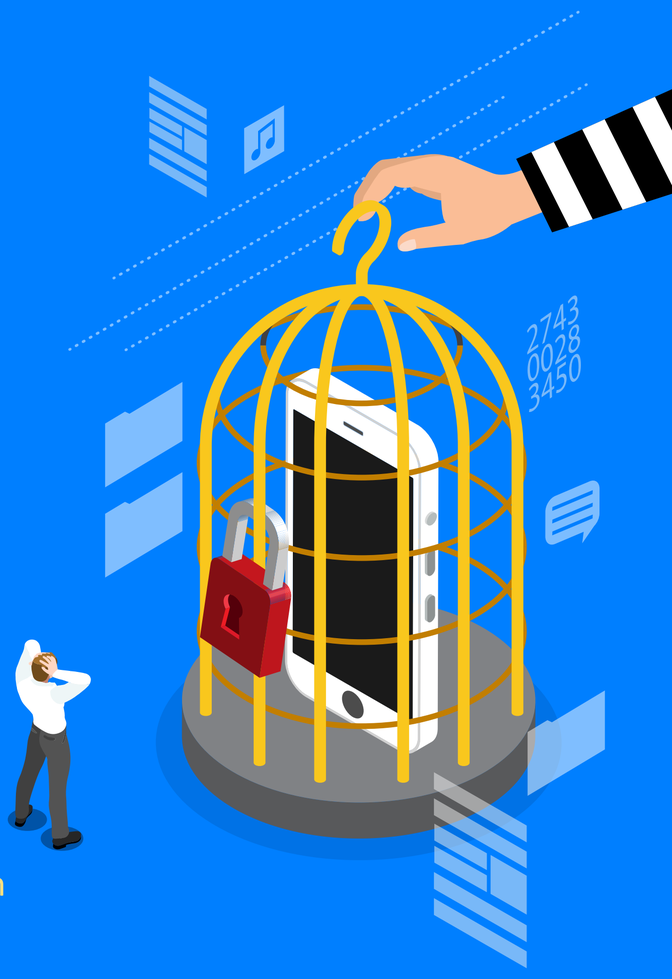
- Download your bank's official mobile app and make sure you are visiting the real bank website every time. (https://)
- If you lose your mobile phone, or change your number, contact your bank so they can update your information.
- Avoid having your online banking site or app to log you in automatically.
- Don't share any information about your account via text message or email.
- Don't share or disclose your bank card number or password to anyone.
- Always use a secure Wi-Fi network when connecting to your bank's mobile site or app. Never do it from an open Wi-Fi!
- If available, install a mobile security app which will alert you of any suspicious activity.
- Frequently check your financial statements.

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

#MobileMalware

MOBILE
RANSOMWARE

SAY GOODBYE TO YOUR PERSONAL FILES



Ransomware holds your mobile device and data hostage for a price. This type of malware locks your device's screen or prevents you from accessing some of the files and features.

HOW DOES IT SPREAD?

Visiting compromised websites.

Downloading fake versions of legitimate apps.

Clicking on malicious links and attachments embedded in phishing emails.

WHAT ARE THE RISKS?

You may have to factory reset the device, losing all your data.

An attacker may have full access to your device and can share your data with third parties.

WHAT CAN YOU DO?

Back up your data frequently and keep all your apps and operating system up to date.

Avoid shopping in third party app stores.

If available, install a mobile security app which will alert you if your device has been compromised.

Be wary of emails and websites that look suspicious or sound too good to be true.

Don't grant device administrator rights to anybody.

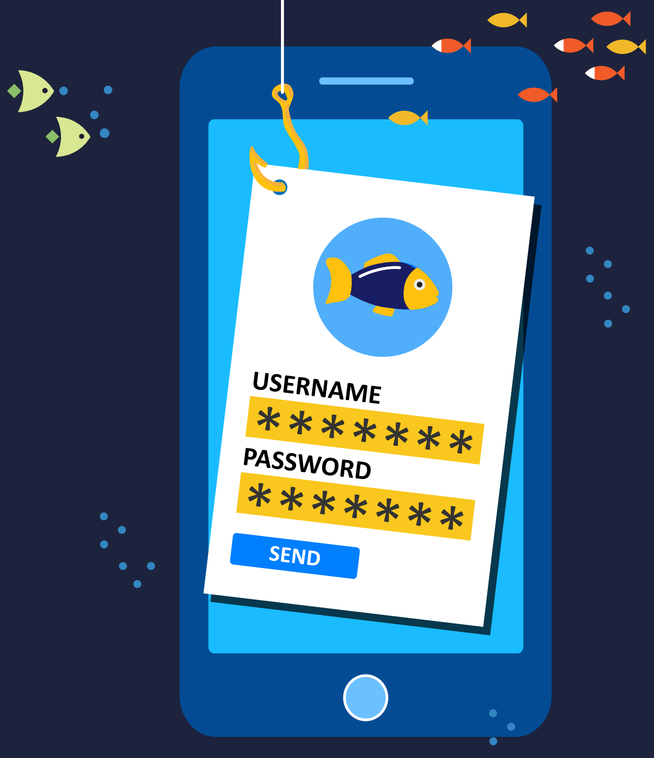
Don't pay the ransom. You will be financing criminals and encouraging them to continue their illegal activities.

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

WEB-BASED THREATS

LOOK TWICE BEFORE YOU CLICK

You could lose your money, your personal information and even your stored data, if the device stops functioning. Don't get hooked!



HOW COULD IT HAPPEN?

PHISHING ATTACKS: They trick users into giving up personal information by posing as a trustworthy entity. They spread through email, text message or social media platforms.

WEBSITE BROWSING: Your mobile device might get infected simply by visiting an unsafe website.

FILE DOWNLOAD: Malicious links and attachments can be directly embedded within an email.

WHY IS IT EFFECTIVE?

Mobile devices are **CONSTANTLY CONNECTED** to the internet.

The **REDUCED SIZE OF THE DEVICE'S SCREEN** is a general constraint. Mobile browsers display URLs on limited screen space, making it difficult to see if the domain is legitimate.

IMPLICIT USER TRUST in the personal nature of a mobile device.

WHAT CAN YOU DO?

Be suspicious if you receive an SMS or a phone call from a company asking for personal information. You can verify that the message/call is legitimate by directly calling the company on their official number.

https://

When browsing the web on your mobile device, make sure your connection is secured through HTTPS. You can always check it out at the beginning of the URL.

Never click on a link/attachment in an unsolicited email or SMS. Delete it immediately.

^BE:%}
W@RY
*)Z#$=

Be wary if you land on a site that contains poor grammar, misspellings or a low-resolution.

If available, install a mobile security app which will alert you of any suspicious activity.

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

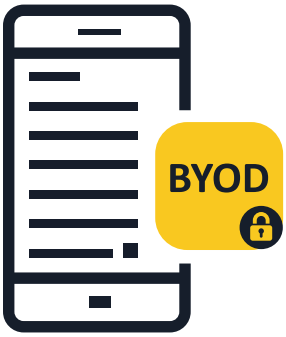
#MobileMalware

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

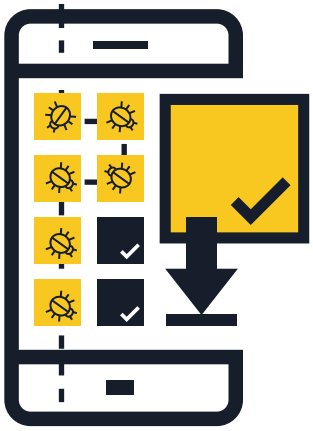
- All operating systems are at risk of infection. If available, make sure they use a mobile security solution that detects and prevents malware, spyware and malicious apps, alongside other privacy and anti-theft features.

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

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.

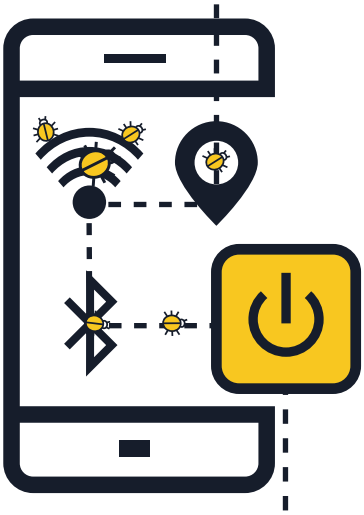
3 Log out of sites after you have made a payment

- **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