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.

#MobileMalware