CITRA

الهيئة العامة للاتصالات و تقنية المعلومات
COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

Tips to Avoid Mobile Attacks

Personal data on your mobile is targeted and it is the responsibility of the data owners to apply security measure to protect their personal data from being stolen.

WiFi

- Don’t allow your device to auto-join public networks.
- Always turn off WiFi when not needed.
- Only send sensitive information over a trusted WiFi network.

Apps

- Only install apps from your device’s official store - NEVER download from a browser.
- always check the reviews before installing an app specially if the app developer is unknown
- Always keep your apps updated to ensure the security protection.
- If the app is no longer supported by your store, just delete!
- Don't grant excessive privileges to apps.
- Download an antivirus app to check regularly on security status of your device.

Vishing (voice phishing)

- Do not disclose personal and financial information to unknown phone calls.
- Try to verify the identity of the caller.
- When you are suspicious, report the call to the concerned helpdesk.

Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn off when not needed.

Browser

- Be careful from some ads. as they might lead to phishing sites that are legitimate.
- Examine the URLs. Look for the https and check the spelling of the domains.
- Never save your login information when you’re using a web browser.

Smishing (phishing via SMS)

- Do not disclose your personal information when requested from an unknown source.
- Be cautious about similar messages in social media apps, such as What’s App, Instagram, Facebook Messenger, Snapchat etc.
- Always think before you click! When dealing with unknown SMS source.

@CitraKuwait

@CitraKuwait

www.citra.gov.kw

ncsc@citra.gov.kw