MOBILE DEVICE SECURITY

Mobile Device Security is the protection of sensitive information transmitted by your smartphones, tablets, laptops, and other mobile devices.

Mobile device security aims to:

- ✓ **Protect sensitive data** stored on portable devices
- ✓ **Prevent unauthorized users** from using mobile devices to access the enterprise network.

Here are some helpful tips to keep your devices and personal information safe.

WHY DOES IT MATTER?

60.5% **of government agencies reported they had experienced a security incident involving a mobile device.**

– Lookout, Inc.

Think about how often you use a smart device and the information that shared apps, emails and notes. **Our devices hold plenty of personal and workplace data valuable to cybercriminals.**

Mobile **technology continues to become more complex** – leading to wider opportunities for unauthorized access to, change of, or destruction of government/personal functions.

- HuffPost

As government and personal services become increasingly dependent on mobile technology**, new threats emerge, and new approaches are needed** to secure the unique capabilities and functions of mobile devices.

- DHS

NETWORK THREATS

Unsecure Wi-fi

No one wants to burn through their cellular data when wireless hot spots are available—but free Wi-Fi networks are usually unsecured.

- ✓ Only use free Wi-fi sparingly and never use it to access confidential or personal services, (i.e. banking, credit card).

Fake Networks, AKA: Network Spoofing

Cybercriminals give Wi-Fi access points common names to encourage users to connect. In some cases, attackers require users to create an "account" to login. Once logged in, the hacker may compromise the user's email, e-commerce, and other secure information.

- ✓ Beware of fake access points (Wi-Fi) that look like networks but are traps in high-traffic public locations (i.e. coffee shops, libraries and airports). Confirm the Wi-Fi you are connecting to is legitimate prior to accessing.
- ✓ Use caution when connecting to any free Wi-Fi and never provide personal information. If asked to login always create a unique password, just in case.

Bluetooth Vulnerability

A group of researchers exposed a severe vulnerability called *Key Negotiation Of Bluetooth* (KNOB). The vulnerability allows the attacker to intercept, monitor, or manipulate encrypted Bluetooth traffic between two paired devices, without being detected.

- Security Boulevard

- ✓ Prevent tracking by disabling and enabling Bluetooth service when needed. This action will reset the address as well as the message content, which prevents further tracking. You may also choose to disable the default (always-on) option.

- Futurity

DEVICE/APP THREATS

Data Privacy

Install the patches and security updates as soon as you receive them. These updates not only improve your device's performance, they improve security and can prevent known threats/vulnerabilities.

- ✓ Don't ignore necessary software updates designed to improve your device's security by fixing bugs and potential vulnerabilities.

Cybercriminals can access your phone through the unused apps.

- ✓ Remove outdated and unused apps to reduce your device's susceptibility.

Hackers and cybercriminals can use your location services (e.g., Cloud services) to hack your phone.

- ✓ Use cloud services, such as Android Device Manager and Find My iPhone to your advantage. Remotely track (and wipe) a lost/stolen device.

Phishing Attacks

Mobile devices are always powered-on and often the first to receive legitimate-seeming emails. Don't take the bait!

- ✓ Never click on unfamiliar links and hover over to verify the link source. When in doubt, enter URLs manually to be as safe as possible.

Data Leakage

Mobile apps are often the cause of unintentional data leakage. Free apps may perform as advertised, but also send data to a remote server, where it is mined by advertisers and even cybercriminals.

- ✓ To avoid data leakage, only give apps the permissions they absolutely insist on, and forgo any program that asks for more than necessary.

Additional Resource:

DHS – Study of Mobile Device Security

https://www.dhs.gov/publication/st-mobile-device-security-study