Tashundre Gilmore
F24 CNT4524.0M1: MOBILE SECURITY

Mobile Security

Unsecure Wifi Networks

A wireless networks that lack proper security measures, allowing anyone in range to connect to the network without needing a password or encryption key.

Jailbreaking/Rooting

Processes that allow users to gain elevated privileges or full control over their mobile devices, which are typically restricted by the device’s operating system.

The goal is to bypass manufacturer or carrier limitations, enabling the user to install apps, customize the device, or access system files that are otherwise restricted.

App Permissions

Settings that allow apps to access certain features, functions, or data on your device. When you install an app, it often requests permission to use resources such as your camera, microphone, location, contacts, or storage.

Bluetooth Attacks

Cybersecurity threats that exploit vulnerabilities in Bluetooth technology to intercept, manipulate, or compromise data and devices. Since Bluetooth is commonly used for wireless connections between devices like smartphones, headphones, and IoT devices, attackers can exploit this communication to gain unauthorized access or control over the devices.

Why are these common mobile security threats?

These security threats—unsecure Wi-Fi, Bluetooth attacks, jailbreaking/rooting, and app permissions—are common for mobile devices due to their widespread use, constant connectivity, and the tendency of users to prioritize convenience over security.

Key Tips for Protecting Your Device

Unsecure Wifi Networks

Use a VPN: Protect your data and privacy by using a VPN on public or unsecured Wi-Fi

Avoid Sensitive Transactions**:** Don't use unsecured Wi-Fi for banking or personal accounts.

Disable Automatic Connections**:** Stop your device from connecting to unknown or unsecured Wi-Fi automatically.

Jailbreaking/Rooting

Avoid Jailbreaking/Rooting: It weakens built-in security and increases vulnerability to attacks.

Use Device Management Tools: For rooted/jailbroken devices, use MDM tools to manage security.

Regular Updates: Keep your OS and apps updated to reduce security risks, even on rooted devices.

App Permissions

Review Permissions: Regularly check app permissions and only allow necessary ones.

Limit Access: Be cautious of apps asking for excessive permissions.

Update Apps: Keep apps updated for security patches and improvements.

Bluetooth Attacks

- ***Turn Off Bluetooth:*** Disable when not in use to prevent unauthorized connections.
- ***Use "Non-Discoverable" Mode:*** Make your device invisible to others when not pairing.
- ***Verify Pairing Requests:*** Pair only with trusted devices and confirm requests.
- ***Update Bluetooth Software:*** Keep firmware and software updated to fix vulnerabilities**.**

Stay One Step Ahead, Secure Your Devices!