Cyber Directorate
U.S. Army Criminal Investigation Division

Cybercrime Prevention Flyer

CPF 00023-22-CID361-9H **26 July 2022**

Mobile Device Protection

The computing power, reliability, internet accessibility, and ease of use of today's mobile devices, phones, tablets, e-readers, smartwatches, small portable computers, etc. has revolutionized communication, financial transactions, and the modern work environment. It goes without saying, these same devices have also impacted, for good and unfortunately sometimes bad, the daily lives of the billions of people relying on them for personal use.

With such a target rich environment, one would be naïve to think cybercriminals are not taking advantage of mobile device vulnerabilities or those made available by the device users. Having a little knowledge about mobile device threats and vulnerabilities, the average user will have the information necessary to continue to rely on and use mobile devices safely.

Common mobile device threats and vulnerabilities include:

Adware and Spyware

Adware and spyware, both considered malicious software, more broadly known as malware, are programs used by cybercriminals to compromise mobile device end-user safety and privacy. Adware, while not wholly nefarious but often accompanied by spyware, exploits internet habits to better target users with advertisements. Spyware collects usernames, passwords and two-factor authentication data, financial and banking information, sites visited, articles read, products viewed, and so on. Cybercriminals either employ the captured information in their own fraud schemes or sell the information on marketplaces focusing on the sale of stolen user data.

Phishing and Smishing Attacks

Most mobile devices connect to the web and are subject to the same threats posed by accessing the web via a computer, to include phishing and smishing attacks, which can lead to device compromises. Email, text, or other messaging services can contain malicious links or damaging attachments, which if clicked or opened could grant mobile device access to cybercriminals.

Malicious Applications

Mobile device users should understand that their information is not inherently safe while stored on their device or in their available applications. Downloaded and installed applications, generally with user permission, collect stored mobile device information. While a user may have downloaded an application from a legitimate app store, applications such as third-party applications, apps not developed by the device or device operating system manufacturer, could contain vulnerabilities, holes in their coding, or be malicious, containing malware, to gain access to sensitive information.

Open Wi-Fi

Accessing an open Wi-Fi, an internet connection that does not require a password or utilizes encryption, is an enticing convenience when needing to access the web while out and about. But this convenience comes with a risk, making devices and device-maintained data vulnerable to anyone nearby or cybercriminals waiting for the unsuspecting victim.

Some cybercriminals create faux Wi-Fi hotspots and when unsuspecting individuals connect, the cybercriminals effortlessly steal the connected individual's information.

Report a crime to U.S. Army Criminal Investigation Division

Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

DISTRIBUTION:
This document is authorized for the widest release without restriction.

"DO WHAT HAS TO BE DONE"

Poor Security

Not properly securing mobile devices with an effective PIN, password, or biometric authentication will afford cybercriminals easy access to a user's device. Do not underestimate the importance of physical security.

Mitigating Threats and Vulnerabilities

- Use strong passwords and two-factor or biometric authentication. Do not make it easy for cybercriminals to access data on lost or stolen devices.
- Never leave mobile devices unattended in public or semi-public places. If unavoidable, lock the interface and then the device in a secure location
- Turn on a device's auto-lock feature. Enabling auto-lock with a strong password ensures others cannot easily access a device, even when left unattended.
- Carefully contemplate accessing an open, unsecured Wi-Fi hotspot. If using an unsecured Wi-Fi site, use a Virtual Private Network (VPN). Or, simply use a VPN whenever connecting to Wi-Fi whether from home or in public. There is no downside other than perhaps a small decrease in network speed.
- Exercise caution when considering whether to click a link in an email or text message, even if the sender is known.
- Be selective when choosing to download an app. Check required app permissions and only download apps from trusted providers (i.e. the app store associated with the mobile device). If the app or source appear questionable, it should probably not be downloaded and installed.
- Manually manage mobile device and application location and navigation options. Do not rely on an operating system or application update to keep location and navigation preferences current.
- Keep antivirus software up to date. Most major providers of antivirus software provide mobile device antivirus applications. As always, check with your device manufacturer for compatibility and only download the antivirus application from a trusted provider.
- Ensure the mobile device operating system is current.

Additional Resources

National Security Agency – Mobile Device Best Practices

Purdue University – Mobile Device Security Best Practices

Mobile Device Security

Mobile Device Cybersecurity Checklist for Organizations

To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to: Subscribe CPF

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer, along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.