U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow @arcyber

Mobile Devices

Everyone's on the go these days and taking smartphones, laptops, tablets, and other devices along to get information, shop, manage documents, and of course communicate with friends and family. But those conveniences may also come with threats and vulnerabilities. Consider these recommendations from the Departments of Defense and Homeland Security.

What are some basic strategies for safe computing with mobile devices?

BEFORE YOU GO:

- Update mobile software to improve your device's ability to defend against malware. Setting devices to update automatically ensures you have the latest versions of security software.
- Back up information, including contacts, photos, videos, and other mobile device data, using another device or a cloud service.
- Use strong PINs and passwords, and set devices to lock after a brief period of inactivity.
- Understand app permissions before accepting them. Check privacy settings and know what permissions you're giving an app before you install it.
- Consider installing security that offers remote location wiping that can locate a lost or stolen device and erase all its data.

WHEN OUT AND ABOUT:

- Disable devices' remote connectivity and Bluetooth when you're not actively using them. Some devices automatically seek and connect to available wireless networks or other devices.
- Use caution connecting to public wireless hotspots on airplanes or in an airport, hotel, train or bus station, restaurant, or internet cafe. Use only secure sites with addresses that begin with https://, and only after confirming the name of the network and the exact login procedures with appropriate staff to ensure the network is legitimate. Do not conduct sensitive activities, such as online shopping or banking using a public wireless network. Using your mobile network connection is generally more secure than using a public wireless network.
- Avoid using publicly accessible computers in hotel business centers, libraries, and cyber cafes. These machines may not be running the latest operating systems or antivirus software. Cyber criminals may have infected these machines with viruses or other malicious software such as keylogger malware that captures users' keystrokes and gives criminals the ability to obtain personal information such as credit card numbers and passwords. Unsecured wifi networks can let criminals within range nab your personal information.
- As with any network or device, use caution downloading or clicking on unknown links. Delete emails that are suspicious or from unknown sources. Review and understand the details of any application before installing it.

- Wait to post pictures from trips and events to avoid letting criminals know where to find you and that your house is empty, making it a prime target for break-ins.

SOME THINGS TO KNOW ABOUT PHYSICAL SECURITY OF MOBILE DEVICES:

- Keep your devices locked when you are not using them, even for a few minutes. That's all it takes for someone to steal or destroy your information.
- To prevent theft, unauthorized access, or loss of sensitive information, never leave mobile devices, including any USB or external storage devices, unattended or unsecured in public places such as taxis, airports, airplanes, and hotel rooms.
- Meal times are optimum times for thieves to check hotel rooms for unattended devices, and conferences and trade shows offer thieves a wider selection of devices that are likely to contain sensitive information and more opportunities for thieves to access guest rooms.
- Immediately report stolen phones to law enforcement and the phone service provider.
- Reset phones to factory settings before disposing of them or selling them to wipe your data.

For more good information on protecting your mobile devices, check out the Army Criminal Investigation Command fact sheet at https://www.cid.army.mil/Portals/118/Documents/Cyber-Flyers/Cyberflyer_MobileDeviceProtection_07-26-2022.pdf