Computer security and privacy tips: Mobile devices

In conjunction with the Office of Administrative and Information Management Systems (AIMS), the DHS News is offering tips for using your computer safely and securely. DHS employees and contracted personnel are required to adhere to laws and regulations regarding confidentiality and Protected Health Information (PHI). These tips are designed to enhance knowledge on avoiding use that could compromise data. If you have additional questions, contact the DHS Service Desk at 412-350-4357, option 2.

Keeping mobile devices secure

Your mobile devices make it easy to connect to the world but they can also divulge a lot of information about you and your friends and family, such as your contacts, photos, videos, location and health and financial data.

For DHS employees and contracted personnel, who are required by law to protect the personal information of consumers, it is especially important to ensure that any mobile device that is used in their work is secured.

Regard personal information like money – value it and protect it. If you practice “Stop-Think-Connect” when you use your mobile devices you stand a greater chance of protection.

STOP: Make sure security measures are in place**…THINK:** About the consequences of your actions and behaviors online…then **CONNECT** and enjoy your devices with more peace of mind.

Here are some measures that you can take to improve mobile security:

• **Secure your devices**: Use strong passwords, passcodes or touch ID features to lock your devices. These security measures can help protect your information if your devices are lost or stolen and keep prying eyes out. Always be in physical possession of your devices and carefully handle them in public places and do not share your devices with others.

• **Think before you app**: Be thoughtful about who gets information about you – your contacts list, where you shop, your location – and how it’s collected through apps. Limit the installation of unsigned third-party applications to prevent the bad actors from requisitioning control of your devices.

- **Limit Wi-Fi and Bluetooth use**: Some stores and other locations look for devices with Wi-Fi or Bluetooth connections turned on to track your movements while you are within range. Disable Wi-Fi and Bluetooth when not in use.

- **Get savvy about Free Wi-Fi hotspots**: Public wireless networks and hotspots may not be secure, which means that potentially, your mobile network traffic may be intercepted or monitored. Limit your public Wi-Fi mobile usage and avoid accessing sensitive email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot for a more secure connection on the go.

- **Keep your mobile phone and apps up to date**: Your mobile devices are just as vulnerable as your desktop or laptop computers. Having the most up-to-date vendor software updates, security software, and apps is a good defense against viruses, malware and other online threats.

- **Delete when done**: Many of us download apps for specific purposes, such as planning a vacation, and no longer need them afterward, or we may have previously downloaded apps that are no longer useful or interesting to us. It’s a good security practice to delete all apps you no longer use.

- **Report lost/stolen devices promptly:** DHS requires county and contracted employees to promptly report county-issued lost or stolen mobile devices to their supervisors.

See more at staysafeonline.org.