

MOBILE DEVICE SECURITY

Your mobile devices – including smartphones, laptops and tablets – are always within reach everywhere you go, whether for work, travel or entertainment. These devices make it easy to connect to the world around you, but they can also pack a lot of info about you, your friends, and family--like your contacts, photos, videos, location and health and financial data. It's important to use your mobile device safely.



MOBILE DEVICES ARE NOT IMMUNE TO CYBER ATTACKS

Cyber criminals are creating apps that are used to infect your mobile devices & steal personal data. Only download apps from trusted app stores. Read reviews of apps before downloading. Research the app developer. Own your security by doing your research before downloading.

TIPS TO SECURE YOUR MOBILE DEVICES

UPDATE YOUR SYSTEM AND SOFTWARE

Make sure all security and critical software are up-to-date on your connected devices and keep them updated. Turn on “automatic updates” on your devices if you’re prone to forgetting.

USE MOBILE SECURITY SOFTWARE

Security software isn't only for your desktop or laptop. There are security products you can use to protect your tablets and phones as well.

PASSWORD PROTECT YOUR DEVICES

Make sure you require the use of a passcode or extra security feature (like a fingerprint) to unlock your phone or mobile device in case either is misplaced or stolen.

SET UP THE “FIND MY PHONE” FEATURE ON YOUR DEVICES

This will allow you to find, remotely wipe data, and/or disable the device if it gets into the wrong hands.

MOBILE DEVICE SECURITY

TIPS TO SECURE YOUR MOBILE DEVICES

ACTIVELY MANAGE LOCATION SERVICES

Location tools come in handy while planning navigating a new place, but they can also expose your location – even through photos. Turn off location services when not in use.

GET SAVVY ABOUT WIFI HOTSPOTS

Do not transmit personal info or make purchases on unsecure networks (such as free wifi at the cafe or hotel). Instead, use a virtual private network (VPN) or your phone as a personal hotspot to surf more securely.

STOP AUTO CONNECTING

Disable remote connectivity and Bluetooth. Some devices will automatically seek and connect to available wireless networks. And Bluetooth enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment systems. Disable these features so that you only connect to wireless and Bluetooth networks when you want/need to.

PROTECT PHYSICAL DEVICES

Ensure your devices are with you at all times. Don't leave devices unattended with strangers.

APP WITH CARE

Review and understand the details of an app before downloading and installing onto your device. Only download from trusted sources. Be aware that apps may request access to your location and personal information. Delete any apps that you do not use regularly to increase your security.

ADDITIONAL RESOURCES



NCSA: Vacation Travel Security Tips

<https://staysafeonline.org/resource/cybertrip-vacation-advisor/>



CISA: Mobile Security Tip Card

https://www.cisa.gov/sites/default/files/publications/Mobile%20Security%20Tip%20Card_5.pdf



FCC: Smart Phone Security Checker

<https://www.fcc.gov/smartphone-security>

