STOP | THINK | CONNECT™

Security and Safety Tips for Mobile Devices

STOP. THINK. CONNECT.

Take security precautions, think about the consequences of your online behavior, and enjoy the Internet with more peace of mind.

Keep a Clean Machine.
Just like our desktop computers, the software on our mobile devices (e.g., laptops, smartphones, and tablets) must be kept up-to-date and free from malicious software. Unclean or unsecured mobile devices face a greater risk of exposing personal data.

- **Protect all devices that connect to the Internet.** Laptops, smartphones, tablets, gaming systems, and other web-enabled devices all need protection from viruses and malware. Ensure all your devices have the latest protections installed.
- **Keep software current.** The best defenses against malware, viruses, and other online threats include having the latest mobile security software, web browser, and operating system.
- **Know the source of your app.** Fraudulent apps often masquerade as popular products. Be sure to verify you are downloading the legitimate app and only download from trusted app marketplaces.
- **Do not "jailbreak" your mobile device.** Running non-standard apps will prevent the installation of security updates from the manufacturer and will also likely void your device warranty.

Restrict Device Access.
Mobile devices contain a significant amount of personal information, such as contacts and saved login information. Lost or stolen devices can be used to gather information about you and, potentially, others.

- **Secure physical access to your device.** Be aware of your surroundings when using your device in public.
- **Lock your mobile device.** Use a strong passcode or passphrase, facial recognition, or fingerprint authentication to assist in restricting access to personal information on your device.
- **Think before you app.** Understand and be comfortable with what information (i.e., location, your contacts, social networking profiles, etc.) the app would access and share before you download it.
- **Clear data on your old devices.** Erase all your personal data before selling, exchanging, or disposing of your old mobile device.

Connect with Care.
Exercise caution and use common sense when connecting to open/public Wi-Fi networks.

- **Get savvy about Wi-Fi hotspots.** When using public Wi-Fi, limit the type of business you conduct and adjust the security settings on your device to limit who can access your phone.
- **When in doubt throw it out:** Links in email, posts and texts are often the ways cybercriminals try to

steal your information or infect your devices.

- **Be mindful of what is at-risk.** Open networks are vulnerable to monitoring, allowing user information (browsing history, passwords) to be collected. Connect to trusted, secure networks as they provide unreadable (encrypted) transmissions or use a virtual private network (VPN).
- **Be mindful of remote connectivity**: Disconnect Wi-Fi, Bluetooth, near field communication (NFC), or other remote connectivity services when not using them.
- **Protect your $$:** When banking and shopping online, check for web addresses with "https://" or "shttp://" which means the site takes extra measures to protect your information. Sites beginning with "http://" are not secure.

Be Web Wise.
We can all take steps to keep ourselves safe and secure online. Understand the steps to take to stay safe online.

- **Stay current.** Keep pace with new ways to stay safe online. Check trusted websites for the latest information and share with friends, family, and colleagues to encourage them to be web wise.
- **Own your online presence.** Set security and privacy settings so that you are comfortable with the information you share and to block those that you want to keep form having contact with you.

Be a Good Online Citizen.
Being safer online makes the online world more secure for everyone. Practicing good online habits benefits the global digital community.

- **Share about others only as you would be comfortable having them share about you.**
- **Never give out anyone else's personal information** (e.g., email, social media handle, mobile number) to a third-party without that person's permission including photos and videos

Visit http://www.stopthinkconnect.org for more information.

APEC Asia-Pacific Economic Cooperation | National Cyber Security Awareness Month | NATIONAL CYBERSECURITY ALLIANCE | EUROPEAN CYBER SECURITY MONTH | Organization of American States