STOP | THINK | CONNECT™

Mobile Device Security Tips

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 and laptop computers, the software on our mobile devices (e.g., smartphones and tablets) must be kept up-to-date and free from malicious software.

- **Protect all devices that connect to the Internet.** Smartphones, tablets, gaming systems, and other web-enabled devices all need protection from viruses, malware, and other online threats. The best defense against online threats is to keep your mobile security software, web browsers, and operating systems up-to-date.
- **Monitor your device's data usage and investigate discrepancies.** An unexplained spike in your device's data usage could indicate the presence of spyware. Running security software to identify and remove unwanted software could protect your bill—and your personal data.
- **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.
- **Keep apps up to date**. Apps are periodically updated to add new features and better security. Ensure your apps are regularly updated and delete apps you no longer use.
- **Do not "jailbreak" or "root" your mobile device.** Running non-standard apps may prevent the installation of important security updates from the manufacturer and may 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 others.

- **Secure physical access to your device.** Be aware of your surroundings when using your device in public. "Shoulder surfing"—looking over a victim's shoulder to capture passwords, personal identification numbers, or other data—has become a greater threat in recent years.
- **Lock your mobile device.** Use a strong passcode or passphrase, facial recognition, or fingerprint authentication to restrict access to the personal information on your device.
- **Remotely manage your device.** Many mobile devices have features that allow users to remotely find, lock and erase content should their device is lost or stolen.
- **Think before you app.** Understand and be comfortable with what information (e.g., location, your contacts, social networking profiles) the app would access and share before you download the app.

- **Protect your data.** Back up your data onto a personal computer, an external hard drive, a flash drive, a network, or the cloud. Keep track of any stored passwords on the device and be sure to change these if your device is lost or stolen.
- **Clear data on your old devices.** Erase all your personal data and saved passwords before selling, exchanging, or disposing of your old mobile device.

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

- **Be mindful of what is at risk.** Open networks are vulnerable to monitoring, allowing user information (e.g., browsing history, passwords) to be collected. Use a virtual private network (VPN) or connect to trusted, secure networks as they provide unreadable (encrypted) transmissions.
- **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.
- **Be mindful of remote connectivity**. Disconnect Wi-Fi, Bluetooth, near field communication (NFC), or other remote connectivity services when not using them.

Be Web Wise.
We can all take steps to keep ourselves safer and more secure online.

- **Stay current.** Keep pace with new ways to stay safer online. Check trusted websites for the latest information and share with friends, family, and colleagues to encourage them to be web wise.
- **When in doubt throw it out.** Links or attachments in email, posts, and texts are often the ways cybercriminals try to steal your information or infect your devices.
- **Protect your money.** When banking and shopping online, check for web addresses with "https://" which means the site takes extra measures to protect your information. Sites beginning with "http://" are not secure.
- **Own your online presence.** Set security and privacy settings so that you are comfortable with the information you share. In addition, block those that you want to avoid contact with.

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, photos, videos) to a third party without that person's permission.

Visit http://www.dhs.gov/stopthinkconnect for more information.

Homeland Security
National Cyber Security Awareness Month
NATIONAL CYBERSECURITY ALLIANCE
APEC Asia-Pacific Economic Cooperation
Australian Government
STAY SMART ONLINE
EUROPEAN CYBER SECURITY MONTH
Organization of American States
More rights for more people