Privacy and Security Tips For Your Mobile Devices

Personal Information is like money. Value it. Protect it.

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 and your friends and family, like your contacts, photos, videos, location, health and financial data. It's important to use your mobile device safely.

Secure your devices

Use a strong password and set a short *inactivity-until-locked* time to secure your device. These security measures can help protect your information if your devices are lost or stolen and will keep prying eyes out.

Lock down your login

Your username and password alone are not enough to protect key accounts like email, banking and social media. Strengthen online accounts and use authentication tools when available, such as a one-time code entered through an app on your mobile device. Some sites refer to this as either Two-step authentication, Two-factor authentication or Multi-factor authentication.

Encrypt it

Encryption is the scrambling of data so that only the authorized person (the password holder) can read it. Encryption works. High-profile news stories in 2016 demonstrated that even large, well-funded organizations have trouble breaking into encrypted devices. New devices now almost always have encryption capability built-in and the feature is routinely enabled by default.

If you want to be safe, check that encryption is enabled on your device.

Limit password attempts

It is important to stop someone from simply trying passwords repeatedly until they guess correctly and completely bypass your device's encryption and password protection. Manufacturers provide two ways of limiting password attempts: The device can either (a) insert a time delay between multiple password guesses or (b) erase the data after a certain number of failed attempts. It will vary from device to device but wherever you can, set your device to erase all data. Backups are vital. **Do not** enable *delete-after-X-failed-password-attempts* until you have a strategy for regular backups.

Don't jailbreak or root your device

Some users modify their mobile device's operating system – a process known as jailbreaking (on iOS) or rooting (on Android). Users make modifications for several reasons including: to add features to the device, to have greater freedom choosing applications or to bypass certain security settings. The result of jailbreaking and rooting is almost always a weakening of security on the device.

Privacy and Security Tips For Your Mobile Devices

Be choosy with apps and delete when done

Only install apps from an official app source (e.g. Apple's App Store, Google's Google Play). Even then, avoid downloading apps with negative privacy or security-related user feedback and apps with no feedback at all.

Many of us download apps for specific purposes or have apps that are no longer useful or interesting to us. It is good security practice to delete apps you no longer use.

Keep your mobile devices and apps up to date

Your mobile devices are just as vulnerable as your PC or laptop. Having the most up-to-date security software, web browser, operating system and apps is the best defense against viruses, malware and other online threats.

Limit location information

Your mobile device will likely have a GPS receiver that has the ability to pinpoint its location to within a few meters. Android and iOS devices maintain a log of your device's location, and apps on your mobile device may request access to your location in order to provide personalized services. Consider periodically deleting the cumulative record of your location, or activating GPS only when needed.

Now you see me, now you don't

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

Get savvy about Wi-Fi hotspots

Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your mobile device while you are connected. Limit what you do on public Wi-Fi and avoid logging in to key accounts like email and financial services on these networks. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection on the go.

Consider using *Find My Phone*

Find My Phone capability is available for most smartphones and tablets either through your vendor (Apple, Google, Samsung, etc.) or a dedicated anti-loss app. Bundled features usually include: remote *wipe*, remote *PIN change* and the ability to remotely *take a picture*. Remember: *Find My Phone* features must be setup **before** loss or theft occurs.

Safely dispose of your device

You may be required to return a mobile device to a service provider or vendor, or you may be selling or recycling your device. In any of these situations, first wipe all sensitive information on the device.

Sources:
staysafeonline.org
Office of the Information Privacy Commissioner & Auditor General of BC - Mobile Devices: Tips for Security & Privacy October 2016