TOP 15 TIPS

MOBILE DEVICES: TIPS FOR SECURITY & PRIVACY

Smartphones and tablets have become the most personal of computers we've ever used. They have social media content, location-tagged photos and streams of text messages. This kind of personal information didn't exist on our laptops and desktop computers. And because we carry our mobile devices everywhere, the information on them is at greater risk of loss and theft.

All of this means that securing our mobile devices has become increasingly important. Below are 15 effective security and privacy measures. They're in priority order — if you're only able to do some then **start at the top and work down.**

IN ORDER OF PRIORITY...

1. Password protect your device
2. Lock your screen
3. Encrypt it
4. Limit password attempts
5. Use anti-malware software
6. Don't jailbreak or root your device
7. Be choosy with apps
8. Limit app permissions
9. Keep software up-to-date
10. Limit location information
11. Review voice commands
12. Promptly report lost/stolen devices
13. Bluetooth, WiFi, NFC
14. Safely dispose of your device
15. Consider using *Find My Phone*

1. PASSWORD PROTECT YOUR DEVICE

A password is your first line of defence, and everything that follows hinges on it. On a mobile device it might be known as a password, PIN or passcode. In any case, make sure it's at least six characters long and can't be easily guessed by someone else.

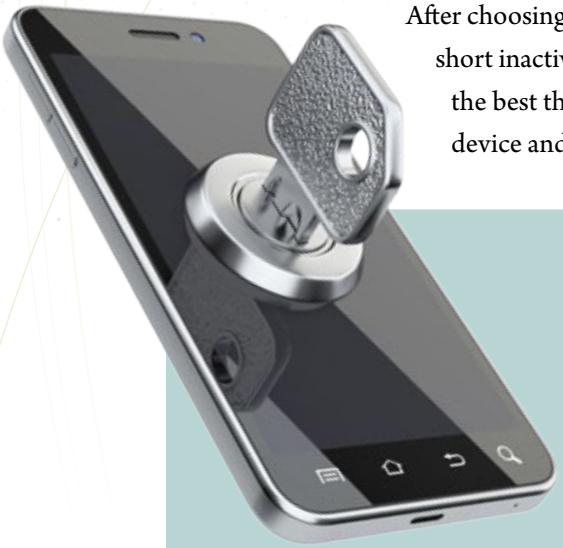
Q: What about swipe patterns or fingerprints instead of passwords?

Although convenient, swipe patterns do not have enough variety, and biometrics, like fingerprints and face recognition, are still easily fooled by fake fingers and photographs. Future technologies may improve the reliability of biometrics, but for now, the best advice is to stick with a good password.

BONUS MARKS:

Clean your screen occasionally. A thief might figure out your password from smudges you leave behind.

2. LOCK YOUR SCREEN



After choosing a strong password, setting a short inactivity-until-locked time is by far the best thing you can do to protect your device and the information on it.

Q: Isn't having to type my password most times I check my device going to be a pain?

Okay, but balance the inconvenience with the fact that without a secure lock screen, whoever finds your device will have access to *everything*.

Q: How short should my inactivity-until-locked time be?

Short enough that a savvy thief, nosy co-worker or family member can't access it between when they grab your device and the screen locks. Think: *a small number of minutes.* Or even under a minute, if you can. Remember what's at stake. If it's not locked, a snoop or thief can access your social media accounts, photos, personal files, shopping applications (apps), messaging (email, texts, etc.) and any websites where you've saved the password.

Work devices:

If your employer doesn't enforce a minimum inactivity-until-locked time, or if you would like to improve your security with a shorter time, then you may be able to set your own. In most remote management situations, the shortest time "wins." That is, whichever is shorter (yours or your employer's) will apply.

Personal devices:

You need to choose the settings yourself. Remember, screen blanking is not the same as a locked screen. Two settings can be at play. The first setting is how long it takes from inactivity until the screen goes blank (for power saving). Only after the screen goes blank does the time start counting down until locked. The total time matters (for security), so if you've extended the time to blank beyond normal make sure you appropriately shorten the time to lock. You can easily test it by trying to access your own device after it has been blank for a short time.

3. 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. Newer devices now almost always have encryption capability built-in and the feature is routinely enabled by default.

If you have an older device, or just want to be safe, check that encryption is enabled. If you're encrypting an older device after-the-fact, be aware that you'll have to start with a fully charged battery and the process of encrypting the first time may take 10 minutes or more (during which you can't use your device).

4. LIMIT PASSWORD ATTEMPTS

It's 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. Both methods are effective and most manufacturers use a combination. All you have to do is turn on the feature, where applicable. It will vary from device to device but wherever you can, set your device to erase all data (or introduce delays) after 10 failed password attempts. This is a good trade-off between allowing you some mistakes and stopping or slowing down a data thief.

Work devices:

If the mobile device is remotely managed by your employer they can add in the *erase-after-X-failed-password-attempts* capability, even if the feature was originally lacking on your device. This can be good and bad. It's good since they have one more way to prevent unauthorized access to corporate information, but it could be bad if your own information is at stake. Solution? Always backup or remove your own information (e.g., photos) as soon as you can from your work device. Get to know your employer's acceptable use policy and, if they allow some personal use, what portions of the device they may erase.

Personal devices:

Backups are vital. Do not enable *delete-after-X-failed-password-attempts* until you've sorted out a strategy for regular backups. As of this writing, Apple calls the feature "Erase all data on this iPhone after 10 failed passcode attempts" and it's off by default. Most Android devices use the delay attempts method rather than *delete-after-X-failed-password-attempts*, so you should be fine even as you are sorting out a backup regime.

5. USE ANTI-MALWARE SOFTWARE

Malware (malicious software) is a growing problem on mobile devices. Mobile device malware includes all of the traditional scourges — viruses, spyware, worms — and now Ransomware, which locks out files and then demands a ransom payment before access is restored. To maximize your chances of avoiding malware, install and run an anti-malware program.

Q: Which anti-malware product should I use?

Work devices: If your employer recommends or provides an anti-malware product, use that one. If you're allowed to decide whether or not to use anti-malware software, remember: it's almost impossible to never store anything personal — photos, texts, website passwords, etc. — on your device and that information could be exposed to malware. There is no downside to protecting yourself with anti-malware software.

Personal devices: Check if your employer's anti-malware software license allows for personal use. If so, use their product on your device. Alternatively, check out independent reviews such as the periodic ones at www.av-test.org or www.pcmag.com to help you choose a product. If in doubt, the biggest names in legitimate anti-malware software — there are commercial and free ones — are all safe bets.

Q: What about Apple or BlackBerry devices?

All devices are vulnerable to malware. As of this writing you cannot install anti-malware on Apple's iOS devices and BlackBerry recommends against it. But the best advice is to install anti-malware software on devices whenever it is appropriate as long as you don't modify (root or jailbreak) the operating system to do it.

Work devices: Follow your employer's guidance.

Personal devices: Anti-malware use may not apply to iOS and BlackBerry as of this writing but it could in the future. Stay abreast of developments and install anti-malware software *whenever it's appropriate.*

6. 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). Motivations to make the modification usually include one or more of the following: to add features to the device, to have greater freedom choosing applications (unless modified, most devices are limited to official app stores) or to bypass security settings made by your employer. The result of jailbreaking and rooting is almost always a weakening of security on the device. Don't jailbreak or root your device.

7. BE CHOOSY WITH APPS

A major attraction of mobile devices is the functionality that additional apps bring. But not all apps are benign. Some apps have been designed to steal information, and others to spy on the owner. On our own it would be difficult to tell the good apps from the bad. But official app stores have the technical resources and are able to weed out most of the bad ones.

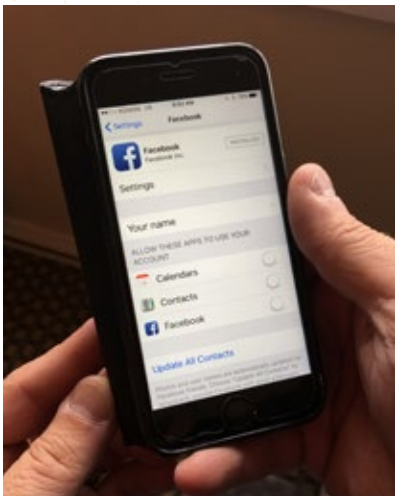
So, only install from an official app source (e.g. Apple's *App Store*, BlackBerry's *BlackBerry World*, Google's *Google Play* or Microsoft's *Windows Store*). Even then, avoid downloading apps with negative privacy or security-related feedback and apps with no feedback at all.

Apps may also store personal information on servers located outside of Canada. This may contravene privacy legislation to which your employer is subject, such as the *Freedom of Information and Protection of Privacy Act*, or contractual obligations of your employer. Check with your employer prior to installing apps that may store personal information outside of Canada.

Work devices:
One exception to the "official sources" rule is if your employer provides their own app store. For employees, that becomes another official source.

Personal devices:
Stick with the official app sources listed to the left.

8. LIMIT APP PERMISSIONS

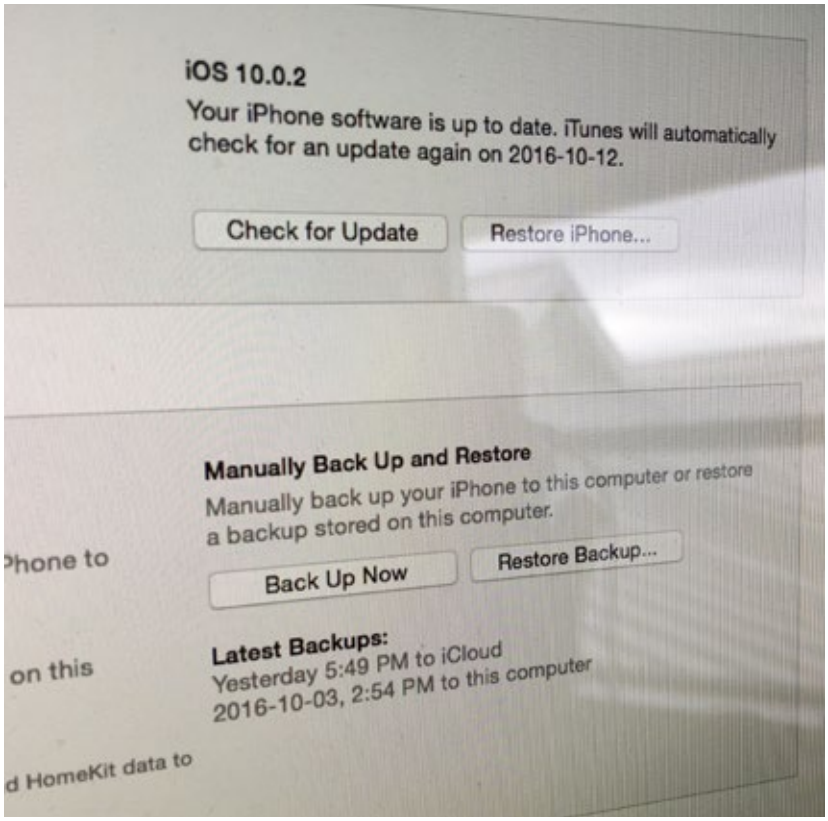


Apps may request access to various sources of personal information on your mobile device. The need for some of these access permissions may be obvious, such as a photo editor requesting access to photos stored on your device, while others may be less obvious, such as a game requesting access to your contact list. During the installation of an app most mobile operating systems will ask your permission to allow the app access to information on your device. Take the time to review these requests, and consider whether the information being requested makes sense to you. With recent versions of Android and iOS, users can refuse access to certain information on a mobile device and still continue to install and use the app, often without any obvious loss of functionality.

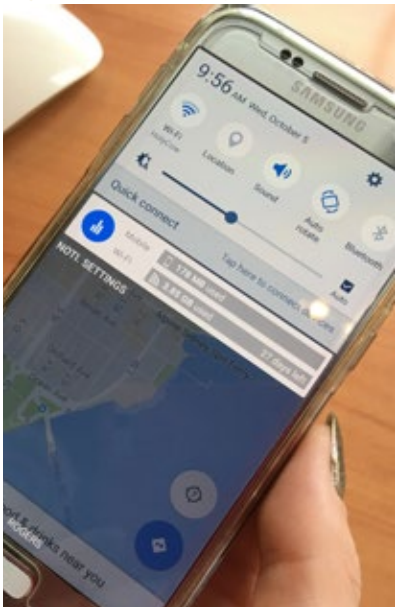
9. KEEP SOFTWARE UP-TO-DATE

Just as with desktops and laptops, timely software updates help keep mobile devices more secure. Flaws get corrected and security improvements are made when we update. So whether it's a work or personal device:

1. For operating systems, set your device to automatically get the updates
2. For apps, the three basic security rules apply:
   - if you didn't go looking for it, don't install the app
   - if you installed the app, update it
   - if you no longer need the app, remove it



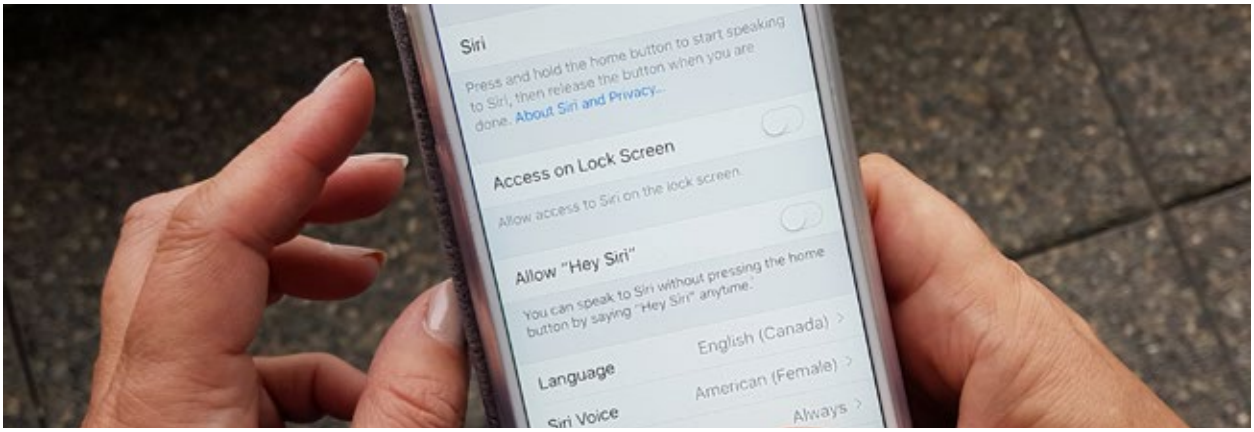
10. LIMIT LOCATION INFORMATION



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. Over time, your location information will provide a detailed picture of your daily activities, including the likely location of your home, work, and friends and family, as well as your shopping and recreational preferences.

Even though services enabled by the use of GPS are convenient, you must determine whether the benefits are proportional to the privacy costs. As those services likely do not require constant access to your location, or a comprehensive log of your movements over time, consider periodically deleting the cumulative record of your location, or activating GPS only when needed.

11. REVIEW VOICE COMMANDS



Mobile device operating systems are increasingly making use of voice commands and voice activated digital assistants, such as Apple's Siri, Microsoft's Cortana and Google Now. For this functionality to be useful, your mobile device must always be listening for your commands or questions. Also, the voice command processing typically takes place on computer servers that may be located outside of Canada. If you don't find voice command features useful, then consider disabling this feature.

12. PROMPTLY REPORT LOST/STOLEN DEVICES

Work devices: Employers are rightly more focused on avoiding data breaches than on recovering hardware. If you attempt to recover the device yourself, you may jeopardize mandatory remote wipe sequences your employer has established. **Follow your employer's procedures.**

Personal devices: Under some conditions, you might be able to electronically locate your device as long as you've prepared the service ahead of time (see #15 below).

If your personal device has telephone service (smartphones or SIM-equipped tablets), contact your phone service provider to minimize the chances of fraudulent charges.

Finally, consider filing a police report and checking relevant "Lost & Found" locations.

13. BLUETOOTH, WI-FI AND NEAR-FIELD COMMUNICATION (NFC)

Most mobile devices are equipped to transmit and receive information across short distances using Bluetooth, Wi-Fi, or NFC technology. This enables your device to wirelessly, and conveniently, connect with your home network, your wireless speaker, or to make use of "tap-to-pay" services. However, each of these networking schemes require your device to broadcast a unique identifier so that it can be identified on a network, and this can easily be used to passively track your movements through a store or around the city. Over time, this can, for example, provide a retailer with a detailed understanding of the areas you frequent in a store, or your visits to a shopping centre.

To prevent this, consider disabling Bluetooth, Wi-Fi, and NFC when not in use. You can easily do this through the drop-down options or settings menu on your device.

14. 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.

Work devices:
Follow your employer's procedures.

Personal devices:
It's not easy to completely wipe personal information from a device. Consult experts.

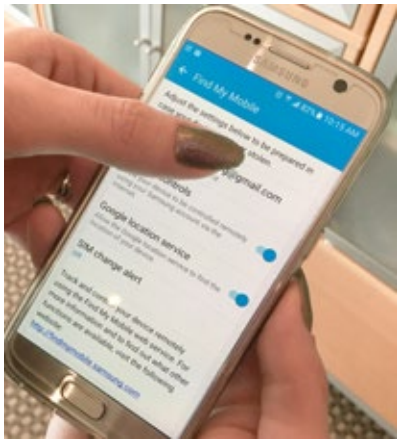
15. CONSIDER USING FIND MY PHONE

Find My Phone capability is available for most smartphones and tablets either through your vendor (Apple, Google, Samsung, etc.), a dedicated anti-loss app or as part of an anti-malware software suite. Bundled features usually also include: remote *wipe*, remote *PIN change* and the ability to remotely *take a picture.*

Work devices:
Do not use any of these features except on the advice of your employer's security team. **Follow your employer's procedures** for lost/stolen devices (see #12 above).

Personal devices:
Remember: *The Find My Phone* features must be setup *before* loss or theft occurs.

Thinking of tracking a stolen device? Okay, find the location of a stolen device and then report it to the police, along with a photo of the suspect (if you have one). **But do not confront a thief.** Your mobile device or data is not worth your safety.



OFFICE OF THE
Auditor General
of British Columbia

Location

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1

Office Hours

Monday to Friday
8:30 am – 4:30 pm

Telephone: 250-419-6100
Toll free through Enquiry BC at: 1-800-663-7867
In Vancouver dial: 604-660-2421

Fax: 250-387-1230

Email: bcauditor@bcauditor.com

Website: www.bcauditor.com

Office of the
Information &
Privacy Commissioner
for British Columbia
Protecting privacy. Promoting transparency.

Location

947 Fort Street
Victoria, B.C.
V8V 3K3

Telephone: 250-387-5629 (Victoria)

Toll free through Enquiry BC at:
1-800-663-7867

In Vancouver dial: 604-660-2421

Fax: 250-387-1696

Email: info@opic.bc.ca

Website: www.opic.bc.ca