Digital Smarts

Securing Your Devices

This resource provides some practical first steps for securing devices against common forms of device tracking and covers actions such as turning off Bluetooth, WiFi and location sharing; renaming your device; checking for spyware and app permissions; and doing a factory reset.

These are general tips on keeping your devices secure. The exact steps may be different for different devices and may change over time.

On iPhones and iPads, you can usually find a setting by tapping "Settings" on the Home Screen, then swiping down to show the search bar. (For help, see http://tiny.cc/iphonesearch.)

On Android devices, swipe up from the Home Screen: a search bar will appear that says "Search Your Phone and More". Type the setting you're looking for in the search bar.

Turn off Bluetooth and WiFi when you're not using them

Bluetooth and WiFi make your device visible to other devices. When you're not using them, turn them off by going into **Settings** or tapping the **Bluetooth** and **WiFi** icons.

You can also go to your Bluetooth settings (**Settings > Bluetooth**) and look for any devices that are paired with your phone. If there are any you don't recognize, unpair them.

Turn off location sharing

Location sharing and apps like "Find my Phone" still work if your phone is turned off, so you have to switch them off in the settings. On an iPhone, open **Settings** > Privacy > Location Services or search for "Location Services", and turn off location sharing.

On an Android device, open **Maps**, tap your profile picture and then Location sharing. Tap the profile picture of anyone who *shouldn't* see your location, and then tap "Stop".

Icon key

Settings	Bluetooth
WiFi	Toggle
Maps	Three dots

©2023 MediaSmarts

Securing Your Devices

Rename your devices

Even if you never changed your phone's name, it still has one that identifies it. On an iPhone, tap **Settings** > General > About > Name, or search for "Name", then enter a new name and tap "Done".

On an Android device, tap **Settings** > About phone > Device name, or search for "Name", then put in the new name and tap "OK".

Check for spyware

"Spyware" means apps that let someone else spy on your device. Check to see if there are any apps that you don't recognize. On an iPhone, swipe right on the Home screen until you see the App Library.

Tap the search box at the top of the screen, then scroll through the list of apps and remove anything you don't recognize.

On an Android device, go to **Settings** > Apps and notifications > See all apps, or search for "Apps".

There are also apps you can use like *Certo* and *Incognito* that will scan your devices for spyware, but you should know that there is always a chance that spyware may still be on your phone.

Check app permissions

You can also stop any app from collecting or sharing things like your location. On an iPhone, tap **Three dots** > Privacy & Security > App Privacy Report to see what each app is sharing, or search for "Privacy Report". Tap each app to change the settings.

Icon key

⚙	•••	⏺
Settings	Three dots	Toggle

On an Android device, download the *DuckDuckGo* app from the Play store and then open it. Tap **Settings** > App Tracking Protection and then slide the **toggle** to the right.

Factory reset

If you've done everything else and still think someone might be tracking your phone, you can do a factory reset. However, this will delete all data, including any evidence on your phone. If you reset your phone, you can't restore from a saved backup because whatever was tracking you might be reloaded: you have to start over completely.

If you're sure you want to do this, on an iPhone, you can tap **Settings** > General > Transfer or Reset iPhone, then Erase All Content and Settings. You can also search for "Reset" to find this setting.

If you have an iPhone you can also turn on Lockdown Mode, which protects you from most kinds of spyware. It also limits how much you can use apps like FaceTime and Safari. See https://support.apple.com/en-ca/HT212650 for more about Lockdown Mode.

On an Android device, start by going to **Settings**, then search for "Reset". Look for a result like "Factory reset" or "Erase all data" and tap it.

MediaSmarts

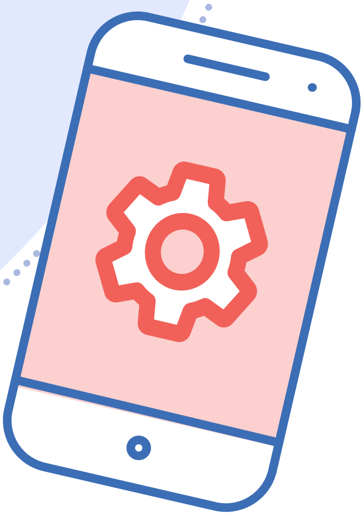
Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada

Digital Smarts

Communicating Safely

This resource provides some practical first steps for communicating safely online to avoid common forms of online tracking and covers actions such as signing out of accounts, turning off location sharing, reviewing privacy settings, and changing passwords.



These are general tips on keeping your devices secure. The exact steps may be different for different devices and may change over time.

On iPhones and iPads, you can usually find a setting by tapping “Settings” on the Home Screen, then swiping down to show the search bar. (For help, see http://tiny.cc/iphonesearch.)

android On Android devices, swipe up from the Home Screen: a search bar will appear that says “Search Your Phone and More”. Type the setting you’re looking for in the search bar.

Sign out of all accounts

You may be signed in to some apps on more than one device. Here’s how to sign out everywhere on *Facebook*: tap **Three dots** and then **Settings**, then “Password and Security” and then “Accounts Center”. Tap “Password and Security” and then “Where You’re Logged In”.

Now you’ll see all your *Facebook*, *Instagram* or *WhatsApp* accounts. Tap each one to see which devices you’re logged in to, and then tap “Log Out” for each one that isn’t your phone.

Icon key

••• Three dots	⚙ Settings
⋮ Three vertical dots	● Toggle

©2023 MediaSmarts

Turn off location sharing in social media

This is important if you use *Snapchat*, which shows where you are on a map. To do that, open *Snapchat* and tap your profile icon. Next tap the **three vertical dots** at top right and scroll down to the “Who Can...” section. If you tap “See My Location” a pop-up will appear that says “Ghost Mode.” **Toggle** that to “On”.

On *Facebook* or *Instagram*, you can turn location off by tapping **Settings** > Privacy > Location Services and then tapping the **Toggle** next to it. Most other social networks put it in similar places within settings like “Privacy” or “Safety”.

Icon key

••• Three dots	⚙ Settings
⋮ Three vertical dots	⏺ Toggle

Review privacy settings

All of your social network accounts have privacy settings, which you usually access by tapping **Settings** and then something like “Privacy,” “Privacy and Security” or “Audience.” Make sure that it is set to only show what you post to Friends.

Change passwords on cloud storage

If you use any cloud storage for your photos or videos, like *iCloud* or *Google Drive*, make sure that you’ve changed the password so nobody else can access it.

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada

Digital Smarts

Browsing Safely

This resource provides some practical first steps for browsing safely online to avoid common forms of online tracking and covers actions such as using privacy-focused browsers, private/incognito browsing, clearing history, and signing in with anonymous emails and strong passwords.

These are general tips on keeping your devices secure.
The exact steps may be different for different devices and may change over time.

On iPhones and iPads, you can usually find a setting by tapping “Settings” on the Home Screen, then swiping down to show the search bar. (For help, see http://tiny.cc/iphonesearch.)

android On Android devices, swipe up from the Home Screen: a search bar will appear that says “Search Your Phone and More”. Type the setting you’re looking for in the search bar.

Use a privacy-focused browser

Browsers like *Firefox* and *DuckDuckGo* are designed with privacy in mind, so they track you as little as possible. Try using one of them instead of the browser that came with your device.

Private or Incognito browsing

Most browsers have a **Private** or **Incognito** mode. This mode keeps the browser itself from recording what sites you visited, but it doesn’t stop those sites (or your internet provider, or other apps on your device) from recording what you do.

Icon key

Private or Incognito mode

Settings

©2023 MediaSmarts

Browsing Safely

Clear your history

Search for “History”. If you have a *Google* account, you can also clear your *Google* and *YouTube* history. Go to **myactivity.google.com** and switch off “Web & App Activity”, “Location History” and “YouTube History”.

To clear your browser history on Safari, tap **Settings** then Safari > Clear History and Website Data, or search for “Website Data”.

Sign in with an anonymous email

Many websites and services want you to give an email address to sign up. If you don’t need to click a verification link, you can use a fake email address created at **Sharklasers.com**.

You can also make a free, private and secure *Protonmail* address so that you don’t have to use an address someone else might recognize.

Use strong passwords

You can make a strong password by starting with a memorable phrase (like “I like bananas”) and then turning some of the letters into numbers or characters (like asterisks or exclamation marks too make it !L1keBan@nas).

But don’t use the same password for different accounts. It’s especially important to use a different strong password for your main email account, since account recovery emails will be sent there. You can also use a password manager like *1Password*. If you do, make sure the password you use for it is strong and different from all your other passwords.

Icon key

Private or Incognito mode

Settings

MediaSmarts

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada