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.)

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

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”.

Icon key

Private or Incognito mode

Settings

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.

MediaSmarts

Financial contribution from

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