TELUS Wise

How to protect your privacy online.

Created in partnership with Media Smarts

Using the Internet is like stepping in wet cement: the footprints you leave there can last forever. Any time you visit a website or use an app, you leave a digital footprint. Sometimes we're aware of when we leave these footprints, like when a photo or post is shared, but sometimes, you may not know what kind of information you leave behind.

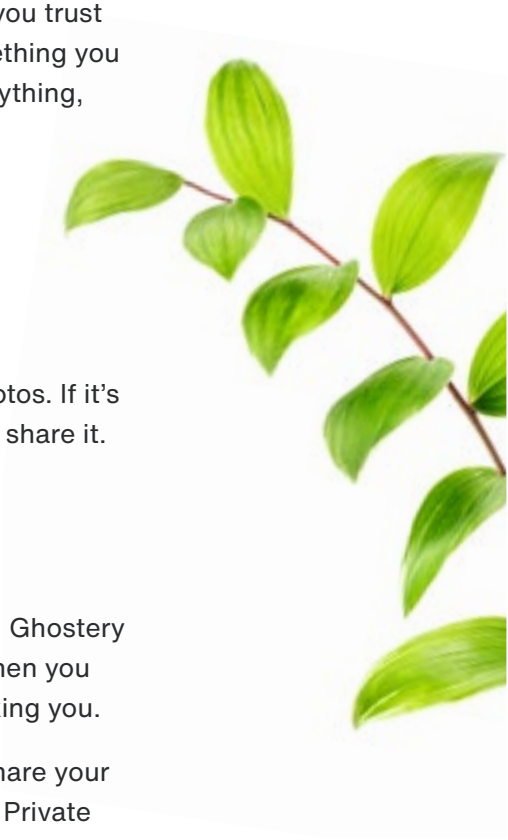
Luckily, there are things we can do to control how much information about us is collected and what is done with it.

Making good choices about what you share online

- Never enter private information like your full date of birth, credit card numbers, usernames or passwords anywhere online, unless it's a website you trust and know is secure. You can tell if a site is secure if it has a padlock in the address bar and a web address that starts with https (instead of http).
- If you're using public Wi-Fi, understand that it's less secure than your home network. Remember, network names can be edited, so sometimes, hackers set up fake networks and name them something like "Public Library" or "Coffee Shop Wi-Fi" to spy on people or install malware on their devices. Double-check to make sure you're connecting with the right network.
- Never do anything like online shopping or check your bank account on public or shared computers. Even if the computer is in a safe place like your school library, there's a chance that someone might be able to see what you're typing and sending. It's best to use shared computers only for browsing as opposed to logging into your personal accounts.
- Consider covering the cameras on laptops and other devices by placing a sticky note or webcam cover over top. Cybercriminals can potentially gain access to your cameras (or microphones) and record you without your knowledge or consent.

Social media

- When you post photos or anything else on a social network, think about who might be able to see it. Almost all social media platforms have privacy settings that give you some control over who sees what you post, but remember, your friends could still share your photos or posts with a larger audience.
- Think carefully about who you accept as a friend. Don't accept friend requests from people you don't know face-to-face in real life.
- No matter how carefully you use your privacy settings or how much you trust your friends, you have to assume there is always a chance that something you share online might be seen by the wrong people. Before you post anything, ask yourself four questions:
  - Is this how I want people to see me?
  - Could somebody use this to hurt me?
  - Would I be upset if they shared it with others?
  - What's the worst thing that could happen if I shared this?
- Don't forget to think twice before sharing other people's posts or photos. If it's something that might hurt or embarrass any of the people in it, don't share it. If you're not sure if they want it shared, ask first.



Controlling what apps and websites know about you

- Add an extension or plugin to your web browser, like Privacy Badger, Ghostery and Disconnect, to control what information is collected from you when you visit a website. These extensions will block most websites from tracking you.
- Use a search engine, such as DuckDuckGo, that doesn't collect or share your web searches or log your personal information, and use Incognito or Private Mode in your browser.
- On a phone or tablet, check the permissions to see what information each app collects. You can then turn off anything that you don't want collected. On an iPhone or iPad, go to Settings, tap Privacy and then go through each category, like Microphone or Camera, to see what different apps are collecting. On an Android device open Settings, tap Apps & Notifications, then tap App permissions.

Staying safe online is about staying informed on the kinds of threats that exist and making time to ensure your accounts and personal information are secure.

telus.com/**wise**