10 Easy Steps to Maximize Tech Use Privacy

A Note on Language

In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

We live in a world of constant technology use and lots of sharing. Technology has made it easier for families, friends, co-workers, and long-lost classmates to connect. Our online lives are just as important to us as our offline ones. But what you share doesn't always stay within these circles and can be shared much more broadly than expected.

So what can you do? Here are some quick ways to ensure that your tech use and sharing are done more safely. Although these may sound simple, these easy steps can make a big difference in your privacy.

1. Log Out of Accounts and Apps

Log out of your online accounts and apps when you're not using them. Uncheck the Keep Me Logged In feature and don't allow the web browser to remember your password to automatically log you in. If you stay logged in, it will be easy for anyone to pick up your computer, tablet, or smartphone and post from your accounts, pretending to be you. Logging out of your account is even more important if you're using someone else's device.

2. Use Strong Passwords

Use passwords to prevent strangers, partners, parents, and children from accessing your accounts. Don't use the same password for more than one account, a password that someone who knows you can easily guess, or a one-word password that can be easily cracked. Create a password system so that you use unique passwords only you will know.

Read more about password safety.

3. Review Privacy Settings

Review the privacy settings on all your online accounts, particularly your social media. Most sites allow users to limit what others see, whether it's status updates or profile information. Don't forget that it's more than just social networks like TikTok, Snapchat, Facebook, or Twitter that have privacy settings. Most online accounts, such as Amazon and Google, allow you to limit who can see your profile information.

4. Minimize Location Sharing

Smartphones have GPS location capability so you could be sharing your location without even realizing it. You can control which app has access to your location by turning off that option on your smartphone. Most phones have location privacy options in the settings. Some social network sites also allow you to manage your location privacy through the site's privacy settings.

5. Don't Include Location Coordinates in Your Pictures

Did you know that when you take a picture on your smartphone, you could inadvertently share your location as well? That means that the selfie you just posted and uploaded online could contain your exact GPS coordinates. You can turn off this capability through the privacy setting on your camera app. Don't forget that even if you turned off the location option for your camera app, the photosharing app that you're using may share your location – so turn off the location option for this app as well.

6. Be Thoughtful about Connecting Social Media Accounts

You can connect your Instagram to your Facebook or your Pinterest account to other social networks. It may be easier to update them all with just one click, but this also means that a lot more people will have access to lots of information about you. It also makes it more difficult to lock down your privacy. So be thoughtful about which social media accounts you connect.

7. Be Careful When Using Free Wireless Networks

Free internet is always awesome, but you pay for it by being more vulnerable to risks. Using open wireless networks at your local coffee shop or community centre can leave you susceptible to hackers accessing your private information. If you're going to check bank accounts, buy something where you have to give your credit card information, or do anything sensitive, wait until you are back on a secure network. And if your personal wireless network doesn't have a password on it, put one on it.

8. Use HTTPS Everywhere

Not all websites are created equal. Some sites are more vulnerable to viruses, which makes your computer/tablet more vulnerable. However, some sites have a secure version – you can tell by looking at the link in the URL address bar. If it

starts with https, it's a secure page. If it starts with http, it is just a normal page.

An easy way to ensure that you're using the secure page whenever you can, is to download the HTTPS-everywhere browser add-in. Each time you go to a site, it'll try to open the secure (https) site rather than the normal one. If the site doesn't have a secure page, it'll default to the normal page.

9. Use Incognito, Private Browsing, or InPrivate Browsing

You can choose to browse the internet privately in Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari. Private browsing means that someone can't open your web browser after you've used it and go through the history to see which sites you visited. Browsing privately is safer if you're using a friend's computer or tablet or are on a public computer. Be aware that you have to close the browser to erase your history. If you leave it open, users after you can still see your browsing history.

10. Use More than One Email Address

Email addresses are free, so have as many as you want! You can use one specific email address with a super strong password for your banking and shopping. Use another email for all the junk mail and accounts you have to create to use a particular web service.

You could even consider using different email addresses for different social media accounts. Using different emails for different accounts is safer because if someone guesses one of your email passwords, they don't have access to all your accounts. You can even go one step further and download a service that "masks" your account address so that you're never using your actual email address.

Trust Your Instincts

If you are living with abuse or have separated recently, it may not be the safest option to update your passwords or take extra privacy steps. You know your situation best so trust your instincts. If it's going to make the abuse escalate, then perhaps leave those steps for now and get some support and safety planning ideas from a domestic and family violence or sexual assault specialist service. You can find one near you on www.sheltersafe.ca.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from NNEDV's Safety Net project, based on their resource 10 Easy Steps to Maximize Online Privacy.

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

Women and Gender Equality Canada
Femmes et Égalité des genres Canada
Canada