Online Privacy and Security

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.

Online Misogyny and Abuse

What Are Online Misogyny and Abuse?

Online misogyny is when the internet and related technologies are used as tools to target, harm, and express hatred toward women.

Online misogyny can start with:

- Sharing sexist attitudes, jokes, and memes
- Treating women like objects
- Stereotyping women
- Sending unsolicited porn or “dick picks”
- Harassment
- Catfishing (i.e. using a false identity to trick someone into a relationship)

And lead to more serious abuse like:

- Doxxing (i.e. posting your personal info online and/or encouraging others to target you)

- Hacking or impersonation
- Image-based abuse (e.g. posting intimate photos)
- Stalking, electronic surveillance, monitoring
- Trafficking and exploitation
- Threatening or inciting rape and murder
- Committing crimes against you or your family

What Are the Impacts of Online Misogyny And Abuse?

Online misogyny can have a range of psychological and emotional effects and may impact the way a woman views the world. It can lead to feelings of:

- Fear, for self or loved ones
- Anxiety, stress, and panic
- Sleeplessness
- Lowered self-esteem or confidence
- Isolation and loneliness
- Powerlessness and loss
- Anger, cynicism, suspicion, mistrust
- Depression, suicide

Experiencing online misogyny may cause a woman to disengage from online spaces or censor herself. This impacts her basic human rights protections including the right to freedom of opinion and expression and the right to privacy.

Over time, a woman who disengages from online spaces to feel safe or to protect herself and her children may lose technical knowledge, employment opportunities, social contacts, access to services, and other benefits provided by technology.

How Common Are Online Misogyny and Abuse?

The United Nations reports that 73% of women online have been exposed to online abuse and that women are 27 times more likely to experience online harassment than men. The online abuse that younger women (ages 18-24) experience often includes more dangerous forms of stalking and violence.

What Causes Online Misogyny and Abuse?

Online misogyny and abuse start with harmful attitudes and beliefs about women. The internet can make it easier to abuse someone anonymously and without the repercussions that exist in real life.

Some misogynists work together to target women they disagree with, generally with the motivation to silence, control, and cause fear. Women are often targeted simply for being women.

Online misogyny is not the fault of the woman being abused. We all have the right to access technology without fear or abuse.

How Do I Know if Online Misogyny Is Happening to Me?

Sometimes it can be hard to tell what someone actually means online or what their intention is. For example, when a guy you really like posts a comment about how sexy you are using a pic where he's down-bloused you (i.e. taken a pic of your breasts/cleavage) without your knowledge or consent, it might be confusing. Is it a compliment or a form of online misogyny and abuse, or both?

To figure out how you feel about a scenario, there are a few questions you might ask yourself:

- While he might be sharing his appreciation of your body, do his actions communicate respect, boundaries, consent, trustworthiness, and care?
- What other images may have been taken or shared? How do you want to be portrayed online and who has power over this?
- What other behaviours or patterns might give you clues about his values, empathy, and character?

Tips for Women Experiencing Online Misogyny and Abuse

There are actions everyone can take to protect women from online misogyny and abuse. We can act individually or as a group, in a multitude of ways, to address the harmful attitudes and beliefs that lead to violence against women.

1. **Secure your tech (accounts, devices, games, and social media**) using WSC's Online Privacy and Safety Tips found within our Technology Safety and Privacy Toolkit.
2. **Ignore, block, and/or report the trolls and abusers if safe to do so.** This may help you regain your voice. Most social media platforms have settings for ignoring, blocking or reporting abuse. Check out our resources for more information.
3. **Connect with others who will support and guide you.** You can find local resources on www.sheltersafe.ca.
4. **Prepare to take care.** Pause and prepare yourself before you read online comments or check messages from someone who has abused you. Consider going offline for a time to nurture yourself and regain balance, but don't be silenced. Sharing what you are going through with someone supportive may help.

*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. If you are experiencing online misogyny, see the YWCA Canada's Project Shift or Hack*Blossom's DIY Guide to Feminist Cybersecurity for more helpful resources. You can also 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 WESNET's Tech Safety project, based on their resource Online Misogyny and Abuse.

Internet Browser Privacy Tips: In-Browser Settings

Internet browsers are the first step to accessing the Internet. They are also the first step to both increasing your online privacy and controlling your personal information. Google Chrome, Mozilla Firefox, and Safari all provide in-browser

privacy settings for users. These options include private browsing, controlling activity logs, deleting cookies, and others.

For survivors of abuse and stalking, using these privacy options may increase their privacy and safety, particularly if they are concerned that an abusive person is physically monitoring their device activity. They can also help survivors have more control over how their personal information is collected and stored when they are online. However, browser privacy options are not going to protect from remote spying or monitoring if the perpetrator is using stalkerware. Learn more about stalkerware on phones and computers.

This document discusses various options that can enhance a user's privacy in Google Chrome, Mozilla Firefox, and Safari. This info sheet is up to date as of October 2022. It is best to search for "how to" on these sites directly for the most up-to-date information.

Here we discuss the following options:

- ***Private browsing*** allows users to surf the Internet without the browser collecting history. This is helpful if you are concerned that someone may be monitoring your internet activity by going through your browser history. However, private browsing **will not prevent someone from knowing what you're doing online** if they are looking over your shoulder or are monitoring your device with stalkerware.

- ***Do not track*** is a setting that allows users to opt out of third-party tracking, such as advertisers on a website that you're visiting. This feature is only for third-party tracking, which often tracks users for behavioural advertising purposes; it doesn't prevent the website that you're visiting from collecting information about you.

All the browsers discussed here allow users to delete their browser history. Keep in mind that if someone is monitoring your computer use, deleting your browser history may appear suspicious.

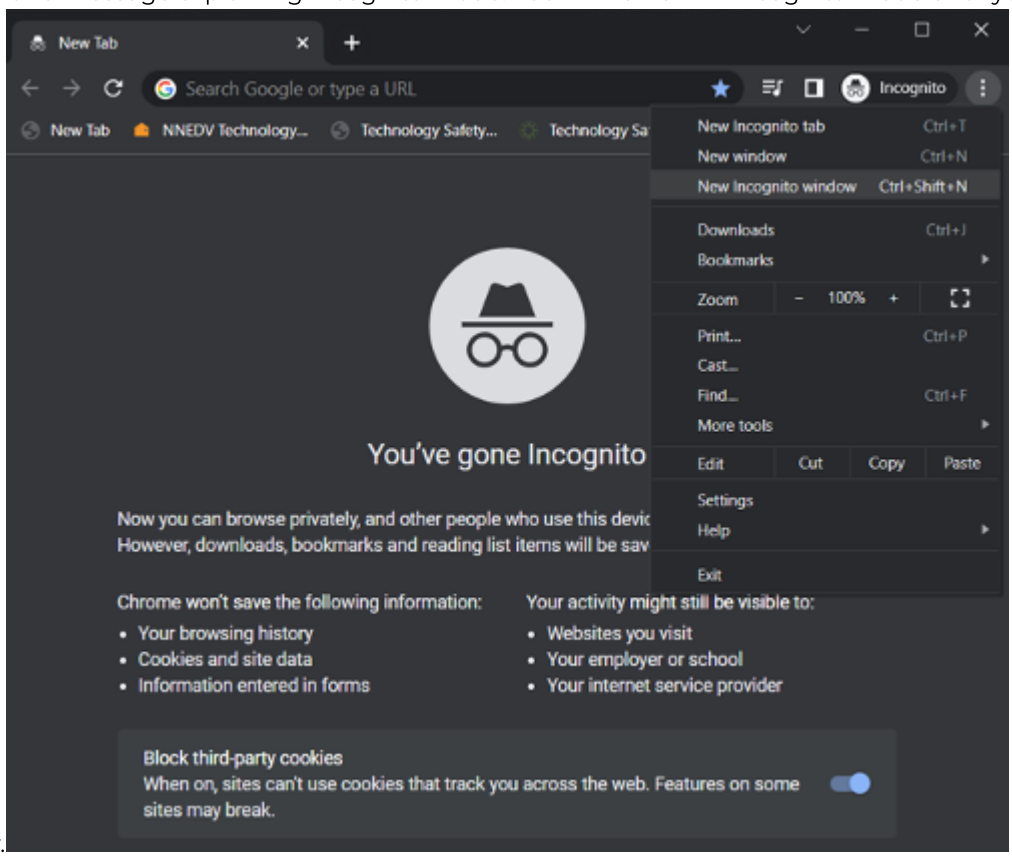
However, regularly deleting your browsing history can increase privacy.

Google Chrome

Private Browsing: Incognito Mode

1. In a new window, click on the Chrome menu ⋮ icon.
2. Choose **New Incognito window.**

3. A new window will open with a message explaining incognito mode. You will remain in incognito mode until you close this browser window.



Do Not Track:

1. On your computer, open Chrome.
2. At the top right, click More ⋮ > **Settings**.
3. Click **Privacy and security** > **Cookies and other site data**.
4. Turn **Send a "Do not track" request with your browsing traffic** on or off.

History:

1. On your computer, open Chrome.
2. At the top right, click More ⋮ > **History**.
3. On the left, click **Clear browsing data**.
4. From the drop-down menu, select how much history you want to delete.
5. Check the boxes for the info you want Chrome to clear, including **Browsing history**.
6. Click **Clear data**.

Additional Privacy Options:

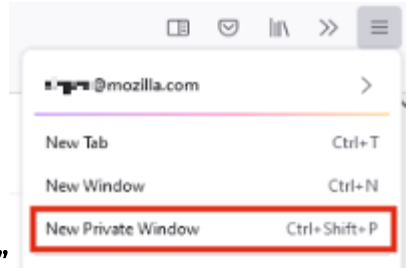
1. On your computer, open Chrome.

2. At the top right, click More ⋮ > **Settings**.
3. Click **Privacy and security**.
4. Choose what settings to turn off.
    a. To control how Chrome handles content and permissions for a site, click **Site settings.**
    b. To delete information from your browsing activity, like your history, cookies, or saved passwords, click **Clear browsing data**.
    c. To control how Chrome handles cookies and tracking, click **Cookies and other site data**.
    d. To manage safe browsing and protection, click **Security**.

Google also offers a Privacy Checkup that allows you to review the privacy settings of any Google products you use, such as YouTube. Visit https://myaccount.google.com/privacycheckup/ for more information.

Mozilla Firefox

Private Browsing



1. Click the menu button ☰ and then click "**New Private Window"**
2. A new window will appear explaining Firefox's Private Browsing option. You will remain in this mode until you close this browser window.

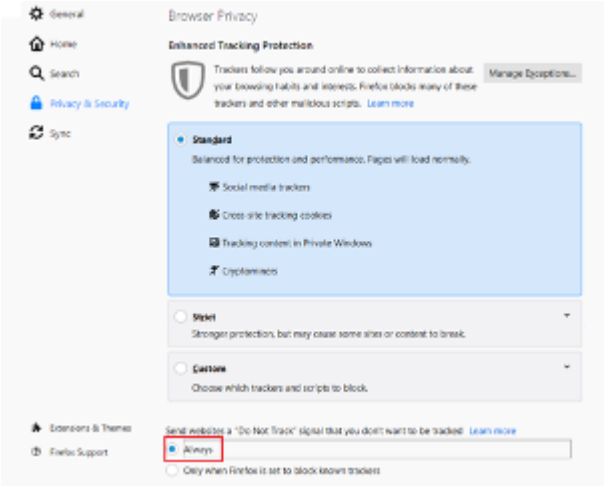
There is also an option to always browse privately. See here for more info.

Do Not Track:

The **Do Not Track** feature is turned off by default, except in Private Windows, where it is always on by default. To always use Do Not Track:

1. Click the menu button ☰ and select **Settings**.
2. Select the **Privacy & Security** panel.
    a. This takes you to the Enhanced Tracking Protection section of your Browser Privacy settings.

3. Under **Send websites a "Do Not Track" signal that you don't want to be tracked**, choose **Always**.

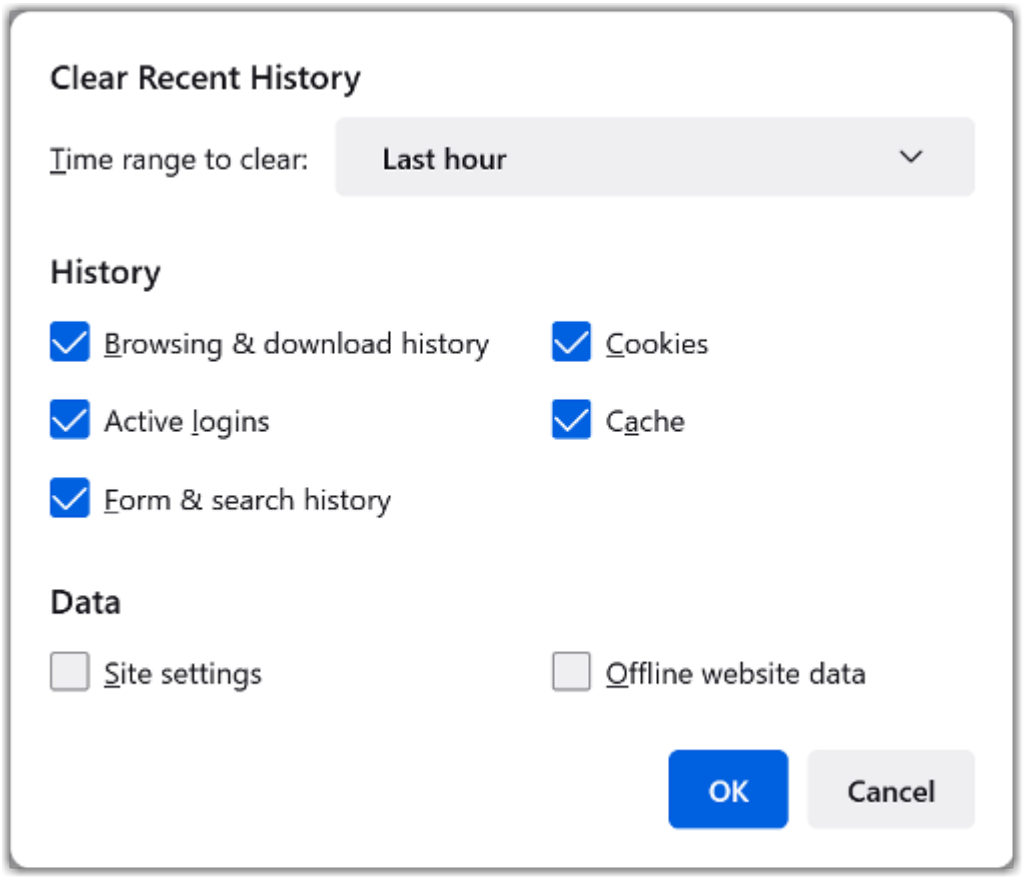


4. Close the **about: preferences** page. Any changes you've made will automatically be saved.

To learn more about how Firefox protects you from trackers in Private Windows, see SmartBlock for Enhanced Tracking Protection.

History:

1. Click on the menu button ☰ to open the menu panel.
2. Click **History** and select **Clear Recent History**.
3. Select how much history you want to clear:
   a. Click the drop-down menu next to **Time range to clear** to choose how much of your history Firefox will clear (the last hour, the last two hours, the last four hours, the current day or everything).



b. Use the checkboxes to select what information you want to clear from your history. Your choices are described in the What things are included in my history? section above.

4. Click the **OK** button. The window will close and the items you've selected will be cleared from your history.

Safari

Private Browsing

Browse Privately One Time

1. In the Safari app on your Mac, choose **File > New Private Window**, or switch to a private window that's already open.
   A private window has a dark Smart Search field with white text.
2. Browse as you normally would.

When you use a private window:

- Browsing initiated in one tab is isolated from browsing initiated in another tab, so websites you visit can't track your browsing across multiple sessions.
- Webpages you visit and your AutoFill information aren't saved.
- Your open webpages aren't stored in iCloud, so they aren't shown when you view all your open tabs from other devices.
- Your recent searches aren't included in the results list when you use the Smart Search field.

- Items you download aren't included in the downloads list. (The items do remain on your computer.)
- If you use Handoff, private windows are not passed to your iPhone, iPad, iPod touch, or other Mac computers.
- Changes to your cookies and website data aren't saved.

Websites can't modify information stored on your device, so services normally available at such sites may work differently until you use a non-private window.

Note: None of the above applies in non-private Safari windows you may have open.

Always Browse Privately

1. In the Safari app on your Mac, choose **Safari > Preferences**, then click **General**.
2. Click the **Safari opens with** pop-up menu, then choose **A new private window**. If you don't see this option, choose **Apple menu > System Preferences**, click **General** and make sure **Close windows when quitting an app** is selected.

Do Not Track:

1. In the Safari app on your Mac, choose **Safari > Preferences**, then click **Privacy**.
2. Select **Prevent cross-site tracking**.

Unless you visit and interact with the third-party content provider's own website, their cookies and website data are deleted.

Social media sites often put Share, Like, or Comment buttons on other websites. These buttons can be used to track your web browsing – even if you don't use them. Safari blocks that tracking. If you still want to use the buttons, you'll be asked for your permission to allow the site to see your activities on the other websites.

History:

1. In the Safari app on your Mac, choose **History > Clear History**, then click the pop-up menu.
2. Choose how far back you want your browsing history cleared.

Additional Privacy:

Check out Apple's Privacy Preferences here.

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 Internet Browsing Tips.

Online Privacy and Safety Tips

We've all heard it before – nothing that happens online is ever truly private or anonymous. And while this is true, it's also true that there are ways people can increase their privacy and feel safer online. This tip sheet is for anyone looking for ways to stay connected and also want to feel safer and keep their information more private.

Signing Up for Accounts

- Create email addresses and usernames that don't contain identifying information such as your full name or birth date/year.
- Use different usernames and profile pictures for each site, and have more than one email account for different purposes like work, school, and social groups. You can also consider using a picture that isn't of you for your profile photo.
- Be thoughtful about sharing personal information beyond what's necessary to create an account or set up a profile. Sometimes sites don't make it obvious that the information being requested is optional, so look out for the fine print!
- Click "no" when sites or apps offer to check your contact list to help connect you with your friends already on their site.
- Opt out of having your profile be searchable on the site itself, and from showing up in general search results like Google.

Passwords

- The best passwords are at least 12-15 characters long and contain letters, numbers, and symbols.
- Use different passwords for accounts that contain sensitive or personally identifying information.
- Log out when you're done and opt out when asked if you want the device, browser, site, or app to remember your password.
- Read more about Password Safety.

Privacy Settings and Policies

- Read the privacy settings guides that many social media sites now offer and adjust your privacy settings to meet your needs. Here are links to a few of the major sites' privacy guides:
  - Safety@Facebook
  - WhatsApp Safety Tips
  - Instagram Safety Centre
  - Safety & Privacy on Twitter: A guide for survivors of harassment and abuse
  - Google Safety Centre
  - TikTok Safety Centre
  - How to Stay Safe on Snapchat

- Read the privacy policies of apps and sites to find out who else has access to your information and how they can get it. Many sites and apps will share information if they receive a subpoena or court order, which is important for women who have or may have court-related interactions with the person who abused or stalked them.
- Read more about Privacy Considerations When Posting Content Online.

Social Media

- Social media is built to be social. Some information is by default always public, while you can choose who sees other information and posts. Regularly review who is in your friends or followers lists, and be aware that your friends' friends may be able to see your posts.

Friends and Family

- Talk to your friends and family about what they can and can't post online about you.
- Don't forget that your employers, churches, sports teams, groups, and volunteer organizations may share your personal information online. If you have concerns about what kind of personal information these groups are sharing online, you could consider contacting them to see if they can remove your information from their sites.

Safe Web Browsing

- Use anti-virus software, keep it updated, and regularly scan your devices.
- Periodically delete history, cookies, temporary internet files, and saved forms and passwords from your web browser.
- Learn more about Internet Browser Privacy Tips.

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 Online Privacy and Safety Tips

10 Easy Steps to Maximize Tech Use Privacy

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.

Being Web Wise

Information about our lives, including personal information, is increasingly ending up online. Many of us have concerns about the security and privacy of this sharing. Women experiencing domestic violence, sexual violence, and stalking have even more complex safety risks and concerns when their personal information ends up on the Internet.

How Does My Information Get on the Web?

To understand how information about you is getting collected, shared, and archived online, you need to first understand how information gets posted online. Information ends up on the Internet in one of two ways: either you post it or someone else posts it.

Information You Post

Below are some examples of ways you could be sharing personal information online:

- Posting updates on social networks
- Sharing your location by "checking in" through social-based location apps or features such as Snap Map
- Commenting on articles or blogs or writing reviews on shopping sites
- Creating wish lists or liking certain content through sites like Amazon, Etsy, or Pinterest
- Sharing photographs or videos online
- Interacting with other users through virtual worlds or online games
- Inadvertently sharing personal information online, such as location data when uploading photos

Even if the information you post may not seem to be identifying, it can reveal a lot about you. Posting a picture of your local school's mascot or a favourite restaurant might inadvertently reveal your location. If the location setting on your phone is turned on for your camera application, uploading pictures taken with that camera may contain the exact location of where that picture was taken.

If you have joined any website where you create a profile page, make sure you know who can see that information. Depending on the site, that profile information may be available to other users. Typically, the default settings will allow anyone who visits that site (family members, potential employers, and stalkers) to see your personal information. Keep in mind that even if you are allowed to "lockdown" your account through the privacy settings, some account or profile information may always be public (e.g. your user name).

Safety Tips

- If you join sites where you create an account and profile, check to see if you're allowed to change your privacy settings to minimize what others can see about you. These sites are meant to draw in as many people as possible and, by default, your information may be available to anyone.

- Learn what the company does with the information you share with them by reading their privacy policy. Most companies will share your information with other business partners or even sell it to advertisers and marketers. Your personal information is valuable for many reasons, particularly for marketing and advertising companies. This could pose a safety risk if a woman's private and confidential information such as physical address is obtained by the wrong person.

Information Others Post About You

Anyone can post information about you, including your friends, family (including your children and current and former partners), employers, faith communities, community groups, school, government, information brokers, and others. Information about you can come from different sources including:

- Court Records
- Employer staff directories
- Web directories
- Faith community/work/school newsletters
- Social networking sites

Information about you may be published on the Internet from less obvious routes. Your information could be sold to advertisers, marketers, and data brokers. Information brokers compile data from public agencies, phone books, consumer surveys, warranty cards, merchants (local and chain stores), contests, social media activity, other websites and more. Your information is combined and then sold to others who want information about you, including media outlets, law enforcement, employers, landlords, banks, credit card companies, car companies, the federal government, and private investigators.

Safety Tips

- Ask organizations that you are a part of if they have any publications or websites and what personal information they publish on these sites. If you are concerned about your privacy and safety, ask them not to publish your information.
- Be aware of what schools or employers may post online about you and your children.
- Ask friends and family members not to mention you, tag you, or post pictures or videos of you online.

How Do I Know What's Already on the Web?

- **Use a search engine like Google or Bing to search for yourself.** Search engines like Google index the web and create virtual card catalogues that link to the actual content. Search engines have existed since the web was developed and they are getting faster and smarter every day. Most search engines periodically "archive" or "cache" websites by saving copies of every webpage so that users can still access the content even if the website is offline, has changed, or is otherwise unavailable. This means that any information ever published online could potentially be available forever (or as long as the Internet exists). Even if a website is changed to remove inaccurate or dangerous information, the old web content might still be indexed by a search engine.

- **Browse online directories for your information.** Online phone directories like canada411.ca include reverse phone look-up features where someone can search for a phone number to find the name associated with that number, the address, and a map of the location. Even if your phone number is unlisted through your phone company, your

address, phone number, and a map to your house may be available through records obtained from marketing companies and other databases.

- **Browse websites where you think your information may be posted.** Visit websites for groups and places that you're connected to: your job, faith community, sports teams, community and volunteer groups, etc.

Can I Remove Inaccurate or False Information, or Information I Don't Like, from the Internet?

Search engines like Google and Yahoo typically aren't responsible for posting your personal information on the Internet. They simply search to find all the websites that list your information. To fully remove your information, you would need to go to each individual site and request that your information be removed.

Depending on the accuracy and sensitivity of the information, it may be best to leave it alone. Many women experiencing violence prefer to leave inaccurate information online to obscure the accurate information that is also available. If the information you find on the web is abusive or potentially dangerous, you can contact the website and ask them to remove the information. Most social networks will have reporting options where you can flag abusive content. Websites will remove content based on their terms of service and community guidelines.

Some sites might require additional information from you to prove that you are indeed the person the information is about. Only share what you're comfortable sharing. For example, if you're asking for a site to remove your phone number, but you must give them your physical address, driver's license number, and a photograph to process the removal, that may be more information than you're comfortable sharing.

Also keep in mind that removing what an abusive person posted might alert them that someone complained, and some perpetrators may respond by increasing their stalking, harassment, or abuse. Think through possible retaliation from the perpetrator in your safety strategies. If the information published about you on the web is extremely dangerous, inaccurate, or otherwise damaging, talk to a domestic or sexual violence counsellor (you can find one near you on www.sheltersafe.ca) for help and speak to an attorney in your area to learn about your legal options.

How Do I Prevent Further Information from Being Posted?

The best way to prevent more information from being posted online is to prevent the information from being collected in the first place. Although this is easier said than done, here are some tips to get you started:

- When a cashier asks for your phone number or postal code, you don't have to share it. In situations where you must provide a phone number, consider giving your work number instead of your home number. You can also use a virtual phone number, like Google Voice, to have a number not connected to your personal information to share.
- If you register for a grocery/drugstore discount card program, fill in very little information. Some stores have a "store card" that you can ask to use.
- Use a pen name when writing letters to the editor or posting online.
- Give donations anonymously.
- When possible, avoid paying with debit or credit cards.
- If you belong to organizations that have a website, ask that your name not be included in publications and ask that you not be "tagged" in photos that are posted.
- When looking for jobs, don't post your resume on any career sites. Instead, search the web for available jobs and send resumes directly to those you're interested in.

- Ask friends not to blog about you, post things about you on their social networking pages, or post photos or videos of you.
- Check all of your privacy and security settings on sites that you use, both on your computer and on your phone, to ensure that you're not inadvertently sharing information.

In addition to preventing information from being posted online, you can try to monitor what does get posted. Set up a Google Alert that will email you any time it finds your name online. When signing up for alerts, share as little personal information as possible.

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 Being Web Wise.

Privacy Considerations When Posting Content Online

Some people may not care that the things they share about themselves can be viewed by anyone, but other people may be more concerned. Here are some questions to consider when posting content online.

Who Will See This Information?

Sometimes we don't realize how far and wide our information is shared, especially when we think we're just posting updates about ourselves to our friends. With the Internet and search engines, such as Google Search, everything online is indexed and searchable. Even sites where you think only members or followers can see the content could be public or seen by others who aren't members.

Think carefully about what you share online, and whether you are comfortable with it being seen by a wider audience. Some social networks or sites have privacy settings that allow you to choose or block who can see the information you share.

What Are You Sharing?

The kind of information you share can reveal a lot or very little about you. Sometimes we share personal information about ourselves without even realizing it. Landmarks in a picture or even blogging about the great restaurant you had dinner at the night before could indicate where you are. Decide if what you are sharing is okay for others to know.

Be careful when sharing information about your friends and family because you may reveal something that they don't wish others to know. If you are sharing things about them, do you have their permission?

What Is the Site's Privacy Policy?

Do you know what the owners of the website do with the information you give them? Even if the information you share isn't posted online, it may be shared with advertisers or third parties. Many sites have privacy policies that spell out what they do with the information you give them.

Is the Information You Share Illegal or Against the Content Policies of the Site?

Many sites don't allow violent or discriminatory content and, if you do post negative content, they could remove your content or close your account. If you are sharing information about others, be careful about not sharing copyrighted materials, false information, or harassing content because that could open you up to civil or criminal legal action.

How Much Control Do You Have Over the Information that You Share?

Some people believe that because it's content you posted, you own it and can control it. But you really don't have much control once it's out there. Others can share it, talk about it, and even change it. If you originally posted it on your personal website, blog, or social media page, you could take down the original post. However, it will likely be difficult for you to have it removed once it's on someone else's website or if someone else has posted a screenshot of your content.

What Can I Do to Increase My Privacy?

- Be thoughtful about what you share online.
- Be careful about what you post about other people.
- When creating online accounts, read the instructions carefully. Often this is when you can opt-out of the site owners collecting and sharing your information.
- Browse the web more safely by running anti-virus and anti-spyware software on your computer.
- For more tips, check out our Online Privacy and Safety Tips.

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 Considerations for Posting Online Content.

Tips for Using Video Sharing and Hosting Sites

More people are watching videos on YouTube, TikTok, Facebook, and other platforms than ever before. While video content on these platforms can open doors to new information and resources, survivors of violence should be aware of

the risks that come with watching videos in these spaces.

Here are some considerations when watching, interacting with, or sharing videos.

1. Delete Browsing History

Web browsers on computers and mobile devices often store and save information about the sites you've visited and the videos you have watched. If you think your computer, tablet, or phone is being monitored, consider deleting your browsing history as it can reveal the sites you visit and may identify what you have viewed. Periodically delete history, cookies, temporary internet files, saved forms, and passwords from your web browser if safe to do so.

2. Use Private Browsing, When Safe

When searching for videos, or watching videos that you want to keep private, you may want to consider using an Incognito/In-Private Browser. Private browser windows keep history and cookies from being stored once the window is closed. It also means that any accounts you are logged in to in the regular browser window will not be logged in to in the private window.

Using these private browsing options can limit what data is tracked and stored. It is important to note that the websites you visit may still be visible if you don't close the window once you are done viewing. View our Internet Browsing Privacy Tips to learn more. Use our Online Privacy and Safety Tips for more information on how to maintain safety and privacy in online spaces.

You may also consider using browsers and search engines that are built with privacy in mind. Privacy-forward browsers that do not track your activities and work to keep third parties like advertisers from tracking your activities include Firefox, Epic, Tor, and Brave. Privacy-forward search engines include Startpage, DuckDuck, and Swisscows. Be mindful that you may have to install these browsers on your device.

3. Log Out of Accounts

Some video-focused social media platforms (e.g. YouTube) give you the option of creating an account. When you create an account, these sites often store specific data about what you have viewed and what you have searched for. They often will make suggestions about future videos you may want to watch based on that history. If you want to keep that information out of your account so that others can't access it, or so someone else who uses your account doesn't get video suggestions that may reveal private information about you, view videos without logging in to the account. Likewise, these accounts, such as YouTube or TikTok, may be linked to other accounts on your phone such as your Google or iTunes account. These accounts may share or back-up information from the video platforms that you do not want to be shared or stored.

4. Beware of the Comments

Often, video-sharing services such as TikTok, YouTube, or Vimeo allow users to post comments under videos. If you choose to post a comment on a video, viewers may view or access your username and profile. If you have concerns about this, be mindful of what videos you comment on. While many times comments can be empowering, some use comments to troll, attack, and harass users. Take caution when posting comments and learn about the site's policies for reporting harassment.

5. Consider Using a Safer Device

If you think that someone is monitoring your computer, tablet, or mobile device, try using a different device or using a different browser that the person hasn't had physical or remote access to in the past, and doesn't have access to now (like a computer at a library or a friend's phone). This can hopefully give an option for video viewing that cannot be monitored by this person.

6. Check Privacy and Account Settings

Every platform has privacy and account settings that give users the ability to lock down their accounts to viewers, limit the types of videos that are shown, and increase password or account security. Some platforms offer many different options for securing and ensuring privacy settings are engaged, while others offer limited ability to make changes. Check your privacy settings under your account information to determine which privacy settings are best for you. When using YouTube, Vimeo, or any other video-sharing site, ensure that your settings are secured to your desired level, and check these settings frequently. If you don't know how to find these settings, use a search engine to search for account, privacy, or security settings on your desired platform.

7. Trust Your Instincts.

Abusers, stalkers, and perpetrators are often very determined to maintain control over their victims, and technology is one of many tools they use to do this. If it seems like the person knows too much about you, they could be getting that information from a variety of sources such as monitoring your devices, accessing your online accounts, tracking your location, or gathering information about you online.

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 Tips for Using Video Sharing and Hosting Sites.

Tips for a Secure Email Account

An email address is more than just another method for someone to contact you. An email address is essential for most transactions these days, from activating a smartphone to making online purchases to setting up an online account. Your email account may contain sensitive and important communication and is often connected to important accounts, such as your bank. Ensuring that your email address is secure – that only you have access to it – is critical.

This tip sheet offers suggestions on how to make your email address as secure as possible.

Which Email Service to Choose

If you are worried about someone hacking your email (via man-in-the-middle attacks), an end-to-end encrypted email service may be what you want. For example, ProtonMail is completely encrypted and you can set it up so that the email is no longer available after a certain time. Other free encrypted email services include Tutanota and Mailfence.

Keep in mind, however, that these services may be slightly more complicated to use than traditional email. For example, some encrypted email services may require that the person to whom you're sending the email also uses the same email service or that to read the email, they click a link and read the email on a web browser. Keep in mind that encrypted email will not prevent someone from seeing your email if they know your email address and password or if you are using a monitored device.

It is possible to use a popular commercial email service, such as Gmail or Yahoo, and still have a secure account. Email security often comes down to passwords, the security of the device used to access email, and good email security and privacy habits such as those covered in the rest of this document.

Setting Up an Email Address

Email privacy and security start when you first create the email account.

Use Non-Identifying Information

Survivors of abuse and stalking may not want an email address that easily identifies them. When you set up an email address with a commercial email service, your email address doesn't have to use identifiable information like your name. You can use anything for your email address, such as *brightredstar3@gmail.com*.

During the setup, the email service provider will ask for information to associate with your email address, including your name and date of birth. You can use a pseudonym and a fake date of birth.

Just remember the pseudonym and birthdate you use in case you need that information to verify your account. Some email services also ask for your gender, mobile number, and a secondary email address. Some services allow you to bypass those questions without entering anything; this will vary according to the email service. For example, Gmail requires a name, username, password, date of birth, and gender; however, you can leave the mobile number and current email address blank and continue. Yahoo Mail requires a name, email address, date of birth, and mobile number while gender is optional. Outlook Mail only requires your name, email address, and password.

Use a Password No One Else Knows

For most people, the security of their email account comes down to whether anyone else knows their email address and password. Don't use a password that someone else can guess or a password that you also use for other accounts. Create a unique password that you can remember without having to write it down and is either a long phrase or contains letters, numbers, and characters.

Use Two-Step Verification

If you have a second email address or a secure mobile number (i.e. no one else has access to it), you can set up two-step verification. If someone tries to log in to your email account from another device or location, the email service will send a code to the second email or mobile number. The code will be required to sign in to the email account, in addition to the password. If you (or the person trying to log in to your email account) don't have access to that secondary email or mobile number to view the code, you can't sign into your account.

This is useful only if you have a secondary email or mobile number that no one else has access to.

If someone else does have access to that email/mobile phone, they could sign in to your account even with two-step verification, or it may let them know when you try to sign in to your account from a new location or device. Depending on your situation, you may not want to have two-step verification turned on until you first secure the secondary email and mobile number.

If you don't provide a secondary email or mobile number, the email service may periodically ask that you provide one when you sign in to your email account later on. In most cases, you can ignore these requests and hit continue or OK without entering anything. Secondary email and mobile numbers can be a very useful security step – but only if it works for you. If you don't have a secondary email or mobile number, or the email or mobile number you have has been compromised by someone else, entering this information will not make your account more secure.

Make sure your secondary email account and mobile number are secure before you use either.

Review Security Notifications

Some email services will notify you of any security events in your account – such as changing your password, logging in from a different location or device, or changing any other security settings.

The security notifications may be sent to your secondary email address. Similar to the issue with two-step verification, if someone else has access to that secondary email address, they will know whenever you make any security changes to your account. You can choose to limit the notifications you receive or change the secondary email address to one that is more secure. (You can generally find the security notifications in the Security Settings section of your email account.)

Practice Good Email Habits

In addition to having a strong password and using the security features (e.g. two-step verification) the email service provides, practicing good email security and privacy habits is important to ensure that no one else can sign in to your email account or read your email.

Use Secure Devices

Try not to log in to your account on devices (e.g. mobile phones, tablets, computers) that the perpetrator has access to or is monitoring. Depending on how the device is being monitored, the person monitoring it may be able to see your email address and password if you log in on that device.

Always Log Out

Whenever you log in to your email account, whether it is on your own device or someone else's, always log out or sign off. Don't just close the web browser or app or shut down the device, as that will not log you off. If you don't log off, anyone who uses the device after you will be able to see your email account. Even on your own devices, logging off is helpful in case someone picks up your phone or computer or you lose it.

If you check your email on your mobile phone via the email app or on your computer/laptop via an email program, you may not be able to easily log off. In this case, you have a few options. Putting a passcode or password on the device will help limit this access. In some cases, you may even want to remove the email account from your email app or program. Some people do this when they are travelling or are concerned that someone untrustworthy could have access to their

device. You can always check your email via the web browser or configure the email app or program to access your email after you are sure that your phone or computer is secure.

Don’t Allow Your Browser or Mobile Phone to Remember Your Email Account or Passwords

Some email services (Gmail, in particular) have an option where the web browser will remember your account unless you tell it not to. The next time you (or anyone else) open the email sign-in page, your email address will be listed and all that is required is for someone to enter the password. Don’t allow the web browser to remember your email account, particularly on devices that you don’t own. This permission request will often show up as “Do you trust this browser?” Choose “no.”

Some web browsers and mobile phones will ask if you want it to store your email passwords or to “remember me.” In this case, it will remember both your email account and password. If you are concerned that someone else may have access to your devices, don’t allow them to store your passwords. This may be convenient for some less sensitive accounts, such as your Netflix log-in, but you want your email account to be secure.

- **Don’t Click on Links from Unknown or Suspicious Individuals**

For further security of your account and device, don’t click on links from unknown or suspicious individuals or provide personal information via email or an email link.

- **Don’t Send Personal Information through Email**

If someone (even if it’s your bank or utilities company) is requesting personal information (such as passwords, credit card information, and bank information) via email, don’t email back with the information. Instead, find the phone number for the company and call them back with that information.

Be Cautious When Giving Out Your Email Address

Since email addresses are what people use to contact you, you will need to give them to people.

However, you may not want to give out your email address to everyone who asks, particularly to stores or when setting up unimportant online accounts. Below are a few ways to provide an email address without having to give out your primary email address.

- You can create a junk email account for when you have to provide an email address but don’t really want to receive emails from them. This email account is specifically for junk mail and should not be set up to receive important information such as statements from your bank, or be connected to important accounts, such as your mobile phone service.

- Some email services let you create short-term email accounts. These email addresses last 10 minutes to 24 hours, so they’re very temporary. When you give out that email address, the emails are sent to that particular email service’s website where you can check for the sent email. This is helpful for when you need to provide an email address to “confirm” signing up, but you don’t want to provide your actual email address. Keep in mind that some of the

temporary email services have no privacy, which means that anyone who knows the fake email address can see all the emails sent to that fake email address (examples of public temporary email services: Mailinator or Maildrop). Other temporary email services include Guerrilla Mail or 10-Minute Mail.

- A more long-term solution to protecting your email address is a service like Abine Blur. Abine Blur is a web browser extension for desktop and mobile that acts as a forwarding service. It "blurs" your real information so the receiver gets an anonymized email address, and not your actual email address. When they reply, Abine Blur forwards the reply back to you to your real email address. On your end, you're sending emails back and forth like normal, but on the receiver's end, they only see the anonymized email address.

[RW1]Link 1.24

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 Tips for a Secure Email Account.

Passwords: Simple Ways to Increase Your Security

Domestic Violence Can Make Password Safety More Complicated

An abusive partner or ex-partner often knows much more about you than others, and this can put your personal information stored in accounts and devices at risk. The perpetrator may coerce you to share passwords or may even be able to guess them.

It is important to create a safety plan before changing your passwords if the perpetrator is likely to become more abusive if they cannot access your information in the same way. You can contact your local anti-violence organization to develop a safety plan.

What Makes a Password Less Safe?

The perpetrator's intimate knowledge about you means that these common password habits are NOT safe for someone experiencing violence or abuse:

- Using common passwords, like ABC123 or password
- Using your own, children's, or pets' names or birthdays in passwords
- Using the same passwords for all accounts

- Answering backup questions with answers that an abuser may know or be able to guess (e.g. your mother's maiden name or your favourite colour).

Good Password Habits

Use Different Passwords for Different Accounts

That way, if someone discovers one of your passwords, they won't have access to all your accounts.

Avoid Using Keychains

Resist using keychains via your browser (e.g. Safari or Google Chrome) to store your passwords. These are little messages that you may see at the top of your browser that ask if you would like the browser to store your password. But do consider using a password manager (see below).

Be Strategic with Your Secret Questions and Answers

Those secret questions aren't really secret. Someone who knows you (or someone who can Google) may be able to guess where you went to high school or your favourite colour. There's no rule that you have to be honest when answering those secret questions so make up an answer that you will remember but someone else can't guess or make use of the option to create your own secret question if available.

Keep Someone from Cracking Your Password by Testing It

It's not just someone who knows you who can guess your password. Computer programs can easily and quickly crack passwords. Words that come out of a dictionary are easier for these programs to decode. Create a mix of words and symbols or phrases, and make it long so it's more difficult to crack.

You can:

- Check to see if your email address has been breached at Have i been pwned?.
- Test your password at How secure is my password? to see how easy it would be for a password-cracking software to guess. You'll be surprised at what you learn! For example, "blahblah" would only take 5 seconds for a program to crack, but "blahblahblahblah" would take 35 THOUSAND years! (Now don't go and use that one – figure one out for yourself!)

Finally, ensure any recovery email addresses and phone numbers are current and are your own before enabling 2-step verification or multi-factor authentication as an additional security step.

Keep It Simple

If you make your password too complex or difficult, chances are you'll forget it and get locked out of your account. Your password should be a phrase or words with numbers mixed in that you can easily memorize. If you must write down your password, be cautious about where you keep it.

Sticking it underneath your keyboard or on your monitor isn't the most secure place. You also don't want to keep it somewhere where someone else could easily find it by going through your belongings. Or, instead of writing down the password itself, write down a hint so you can remember what it was.

Keep Accounts Separate

Sometimes services like Facebook or Google give you the option to sign into other accounts using the accounts you already have with them. This can be convenient, but if someone gets the password to your Facebook, for example, they may be able to access many other accounts easily.

Don't Share Your Password

Before you share a password, make sure this person is someone you can trust, now and in the future. Most of our online accounts hold a significant amount of personal information about us, and you might not want it shared with others.

Change Your Password Often

If you think someone knows your password, changing it will keep them from further accessing your accounts. It's also good practice to get in the habit of changing your passwords now and then.

Uncheck the Remember Me or Keep Me Logged In Feature

While these features make it super easy to access accounts, it also makes it easy for someone who's using the same computer or device to access those accounts. Be especially careful to uncheck those features if you're logging in to an account on someone else's device or a public computer.

Always Remember to Log Off

Your account may remain open for days if you don't log off, allowing others access. Some accounts, such as Facebook and Gmail, allow you to see other places where you've logged in and deactivate those log-ins.

Delete the Account or App

If you're using an app on a smart device that doesn't allow you to log off, you might want to consider deleting the app or account. This is an additional hassle, but you can weigh the sensitivity of the information in that account and the risk of someone else accessing that information.

Suggestions for Making Passwords Easier to Remember

Those experiencing violence often have way more on their minds than remembering a lot of passwords. Sometimes that can be related to things like trauma, sleep deprivation, stress, or depression. It is not your fault if you find yourself forgetting passwords. Try these suggestions for making passwords easier to remember:

Choose Four Things

Create a password with four different things that are not related. Try listing them in alphabetical order to help you remember their order (e.g. CoconutElephantMicroscopeNetball)

Write a Sentence

Write a sentence and misspell or use a non-English language for some of the words (e.g. MifavouriteactorisNicoleKiiidman).

Consider Using a Password Manager or Vault

These can not only store your passwords in one secure area, but they can also generate strong and unique passwords so that you don't have to put the energy into doing that yourself. We recommend researching reputable tech sites to select a password manager that you feel is right for you. Many of these offer free subscriptions at a base level – all that is needed is one rock-solid password to "lock" the vault and all of your other passwords within it.

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 Tips for a Secure Email Account.

Image-Based Abuse and the Non-Consensual Distribution of Intimate Images

What Is the Non-Consensual Distribution of Images?

In Canada, the non-consensual distribution of images is the sharing of an intimate image, without your consent, when you expected the image to be kept private. An intimate image is one where a person is nude, exposing their breasts, genitals, or anal region, or is engaged in sexual activity. It can be any visual recording, including a photograph or video recording.

In the context of domestic violence, perpetrators will often share or threaten to share intimate photos or videos of women to manipulate, punish, or control them. Many of these videos or photos are posted and shared online to popular social media sites, pornography, or “revenge porn” websites.

When posted online, some intimate images include identifying information of the individual, such as their full name, address, phone number, and place of employment or school, which can create a significant risk of further abuse, stalking, and harassment by other perpetrators. Women have reported being contacted by strangers asking for lewd sexual favours or more photos after their pictures or videos and personal information were posted online.

Perpetrators may also send, or threaten to send, images directly to friends, family, and others in the community who know the victim via email or texting.

A perpetrator can come into possession of intimate photos or videos in various ways.

- They originally took the photo or video,
- They were sent the photo or video by the person in the video (a selfie).
- They stole the image (by accessing the person’s phone, computer, or cloud account).
- They photoshopped another image to look like the person.

Impact on Women

The effects of this violence can be devastating, impacting every part of a woman’s life and future. Many women are re-victimized in their school, workplace, or community; and some have attempted or committed suicide as a result. Unfortunately, a significant amount of victim blaming exists in some of these cases, with people suggesting that women should not have shared the images in the first place. Even when the images were obtained without consent or permission (e.g. secretly recording someone or recording a sexual assault), the woman’s actions are often questioned. However, the focus should not be on her actions, but rather on the distribution of intimate images without consent by the perpetrator.

Terminology

The non-consensual distribution of images is often referred to as “revenge porn” or “cyber harassment.” Other terms used for this form of violence include sexploitation or sextortion (i.e. when someone blackmails another person by threatening to reveal explicit images) and e-venge, referring to the electronic distribution aspect.

The currently preferred term is “non-consensual distribution of images.” This terminology does not focus on the action of the woman (which can be victim-blaming) or the motivations of the person who shared the image (which is often not revenge), but instead focuses on the lack of consent by the victim in either the recording or distribution of the intimate images.

Further, images do not have to show nudity or genitals (which is often the criteria used to determine whether an image is considered pornographic) or be sexual in nature. The term intimate image also encompasses photos or videos that may be intimate based on the victim’s cultural/social background but do not depict nudity or sex (e.g. sharing a photo of a woman without her hijab to cause shame and embarrassment or extort her).

What Can Women Do?

Document What's Happening

For many women, their first instincts are to get the images removed from the Internet immediately. Before you do that, consider if you want to document or capture any evidence so you have a record of what was posted and by whom. This will be important if you decide you want to report it – either to the police, a lawyer, or other reporting processes.

Here are some tips for documenting evidence:

- Capture the URL where the image was posted.
- If the URL doesn't include it, identify which website it was posted on.
- If the website shows who posted the image, also capture (by taking a screenshot or screen capture) the name of the person who posted it and any other profile information available about them.
- Try to capture the date/time the image was posted if possible and always record the date the evidence was collected.
- If there is any other related harassment, such as emails or texts, be sure to keep those as well.
- If the abusive person made any statements about posting your intimate image, record that in your documentation log.

Report to the Website

Many major social media websites have a process to remove non-consensual intimate images. These companies have policies that forbid non-consensual intimate images on their sites and, once reported, will remove the images. This is why you want to capture the evidence first before you report it, as once it's removed you will not have evidence of where it was posted.

Some websites do not have a reporting process to take down non-consensual intimate images. If this is the case, read their community guidelines or content guidelines to see if they will remove certain content. Some websites have content guidelines around harassing, abusive, hateful, or harmful content. While they may not have a take-down reporting process, they may allow requests for content removal if you email them or contact them. Some websites will remove content if there is a copyright infringement. This can be helpful if the photo or video was taken by you.

Be wary of websites that require a lot of personal information from you or ask for payment to remove the image. While most websites will try to be helpful, some websites may further exploit what happened to you by requesting personally identifying information so they can post it alongside the intimate image or blackmail you for money to remove the content.

Remove Your Image from Search Engines

For some women, the biggest worry is that these images will come up if someone searches for them. You can submit a request to Google or Bing and ask that they remove the URL links with your image from search results. This way, when someone searches your name, it's not the first thing that comes up.

If the image has been shared without consent, see the Cyber Civil Rights Initiative Guide to getting content taken off the Internet.

Report the Abuse

One option is to report to the police. It is an offence according to the Canadian Criminal Code to distribute non-consensual images.

Seek Support from an Anti-Violence Program

If the intimate image-based violence is part of a pattern of domestic or sexual violence, seek support from an anti-violence program in your community. They can help you with other things that are happening, along with the image-based abuse.

Tech Safety Tips

Here are some tips that may be helpful:

- If your photos and videos are automatically uploaded to an online cloud service, check to make sure that those accounts are secure and that someone else doesn't know the password. It is always a good idea to make sure that all your online accounts are secure and that no one else but you knows the passwords.
-
- Review the privacy settings of your social media accounts, so you know who sees what you share. You may want to review your friends and followers, and if there is anyone you don't want to see your information, you may unfriend them or remove them as a follower of your account.

- Put passcodes on your devices, particularly devices that have photos and videos of you.

- Consider creating a Google Alert for your name so that if anything is posted online with your name, you will get an alert. This will be best for someone with a name that isn't very common. Also make sure you'll be okay getting an alert, even if that means you'll know each time your intimate image has been re-posted. Some women find this helpful to do, while some women feel that this can be difficult.

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 Image Based Abuse.

Resetting Your Wi-Fi Network

Once you no longer live with your abusive partner, it's important to take steps to secure your technology and online accounts to prevent the abuser from accessing your important information. This includes resetting your Wi-Fi network. This is because anyone on your network could easily take a look at what you're doing, what your passwords are, and

other private information with just a few simple software tools. This document explains how to reset your Wi-Fi network so that you can be assured that your Internet connection, and the devices in your home that depend on it, are safe.

Step 1: Find Your Router

The first step is to know where your Wi-Fi router is in your home. With so many electronic devices plugged into our walls, it can sometimes be hard to figure out which one is your actual Wi-Fi router. If you're unsure which device is your Wi-Fi router, try unplugging the device you suspect it is. Does your Wi-Fi internet access go away? If so, that was the one! Plug it back in and move on to the next step.

Step 2: Find Your Manual

Some of the next steps involve looking at your Wi-Fi Router's manual. The exact steps to take can be very different depending on which model you have. Try finding your router's model number. It should be listed somewhere on the back or side. Then enter your Wi-Fi router brand (e.g. Linksys) and model number into a google search and add the word "manual" at the end. The manual should be one of the first few results Google returns. If you cannot find the router brand contact your internet provider (e.g. Rogers, Shaw, Telus, Northwest Tel) for the information. They may even be able to help assist you through the reset process.

Step 3: Clear Existing Settings

Now that you've found your Wi-Fi router and manual, it's time to clear out all the existing settings on your Wi-Fi router, because there is no way to know exactly what the person who originally set up your router has done to it. To do this, find the "reset" button on the back of the router. Often these buttons are just small holes that you can only push in with a pen, unfolded paperclip, or the back of an earring. If you can't find it, try looking for the words "reset button" or "factory defaults" in your Wi-Fi router's manual.

Hold the reset button down (again, you may have to use a paperclip or the back of an earring to push it). You should see all the lights on the Wi-Fi router flashing to let you know it's about to be reset. Keep holding that button down. When the reset is done, the lights should stop flashing.

Step 4: Set It Up Again

With your Wi-Fi router reset, you now need to set it up again with a new password.

The first step is to connect to the reset router's Internet. Look in your computer's list of available Wi-Fi connections for the new Wi-Fi connection. If you had a custom Wi-Fi network name before, that name will have been erased. Your network name will now be something generic, usually named similar to your Wi-Fi router brand. If you see a lot of Wi-Fi networks in the list of networks you can connect to, make sure you're standing next to the Wi-Fi router and try connecting to the one that has the strongest signal. When you connect to the Wi-Fi network, there shouldn't be a password. If there is, look for a default password printed on your Wi-Fi router or in your router's manual. Some routers may have the default network name for your router printed on the router along with the default password.

Step 5: Access Your Router's Settings

Once your device is connected to your Wi-Fi router, it's time to get into the Wi-Fi router's settings. The settings can be found by going to your browser and entering a special address made specifically for Wi-Fi router settings. Open your web browser and try entering each of these special addresses until you find one that gets you to your Wi-Fi router's settings page:

- 192.168.0.1
- 192.168.1.1
- 10.0.0.1

If none of those addresses take you to the settings, this article can help show you how to find your Wi-Fi router's address depending on what kind of device you're using.

If you visit one of these addresses and see instructions to download an app to modify the router's settings, follow those directions to download the app to a smartphone and edit the router's settings there.

If you can't figure out how to get to your Wi-Fi router's settings, try calling your Wi-Fi provider. Their tech support team can likely help you access the settings.

Step 6: Log In to the Router's Settings

Once you get to the settings page, you should see a screen asking for the admin username and password. This is a different password than the one you previously used to connect to the Wi-Fi. Every router manufacturer sets a different default username and password. Sometimes these admin default passwords are written on the router itself; other times, they are written in the manual. You can also look up your router model's default password by visiting this webpage.

Step 7: Set Up a New Password

After you've logged in to your Wi-Fi router's settings, it's time to set up a new network password. Every Wi-Fi router's settings are different from each other. Look in your Wi-Fi router's manual or just try clicking on the different settings sections and look for something called "Network Name" or "Network Password." Come up with a good, strong password for your network. Write your new password down and store it in a safe place in your home. A good password is at least twelve characters of random letters and numbers. You won't have to memorize this password so it's best to make it long and complicated. Try doing a Google search for "random password generator" to find plenty of tools to help you make up a new password.

You can change the network name if you'd like. The generic name for the network is fine if you want to keep that. If you do change it, it may be wise to pick a name that doesn't identify you especially if you're living in home, condo, or apartment building with multiple Wi-Fi networks in range.

Once you've changed your network password or name, you will lose your connection to the Wi-Fi router. You now need to open up your device's Wi-Fi settings and reconnect to your Wi-Fi network, this time putting in your new password.

Step 8: Disable WPS

Before you're done, there are two more settings for your Wi-Fi router that you should consider changing.

First, go back to your Wi-Fi router Settings page and see if you can find a setting called WPS. If you find it, disable this feature. WPS is a method for connecting to your Wi-Fi router that has a serious security vulnerability that many router manufacturers have not fixed. You would never actually need this feature turned on, so it's safer to just disable it.

Step 9: Set Up a Different Username and Password (Optional)

And finally, you may want to set up a different username and password to access the Wi-Fi router's settings. This is different than the network name and network password. This is the username and password that gets used to sign in to your Wi-Fi router's settings page. Look through your Wi-Fi router's manual or click around the various settings until you find a setting that looks like "admin username" and "admin password." The username can be anything you want, but make sure the password is a different, secure, random password than what you set for your network password.

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.

Special thanks to Steven Jenkins of EmpowerDB for providing content expertise for this document.

Security Tips for Computers and Laptops

The computer (or laptop) is a common item in most households. It sits in the corner for the kids to do their homework or for us to check email and maybe pay a bill or two. At the office, we log in to it every morning and turn it off each evening.

Computers can be a vulnerable technology that perpetrators, both those you know and those you don't, can exploit to gain information about what a woman is doing. While a computer may not be as intimate to us as a smartphone, it still contains a lot of personal information, from email accounts to web browsing activity, from filling out forms and documents to saving and storing important information.

The only way to completely prevent someone from accessing your computer is to keep it disconnected from the internet or other network (such as a home network, even if it's not connected to the Internet) and put a passcode on your computer so that only you can access it. If you are concerned that someone might be getting into your computer, and you're comfortable with disconnecting it from the Internet, this might be an option. For most people, however, disconnecting from the Internet prevents them from doing what they need their computers to do. So, whether you're setting up a new computer or just reviewing your computer's settings, here are some privacy and security tips.

Prevention And Protection

These are some ways to minimize another person's ability to gain access to your computer.

Turn on Firewall Protections

Most computers and laptops (as well as tablets and mobile devices) come with firewalls already installed. Firewalls monitor data that is sent to and from your computer; when data with potentially malicious software is detected, it will prevent that data from being communicated to your computer. Essentially, a firewall will protect your computer from someone who is trying to hack it through its open connections.

On most Windows operating systems, firewall protections are turned on by default. Mac and Linux operating systems have the firewall turned off by default, but you can turn it on. To see if your computer's firewall is on, check the firewall settings under the Control Panel (for Windows operating system) or System Preferences/Security & Privacy (for Macs).

Run Anti-Virus and Anti-Spyware Software

To protect your machine from viruses and spyware, you should install and run anti-virus software. Anti-virus software will scan your computer and files you download for viruses and, if it detects any viruses, will prevent installation. Some software may quarantine the virus to keep it from infecting your computer while others will remove the virus.

Anti-virus software relies on virus definitions to detect the virus; however, cybercriminals are constantly changing viruses to infect devices. For this reason, make sure your anti-virus software is running the latest version. Most anti-virus definitions will update automatically. If yours do not, set up your anti-virus software so it does.

Anti-spyware is similar to anti-virus software, but it's specifically for spyware. If you're concerned that the perpetrator might be installing spyware on your computer remotely, running anti-spyware can be helpful.

Anti-virus and anti-spyware software will not completely prevent malware from being installed. However, it will increase your computer's protection. There are many free anti-virus/anti-spyware products available for the home user. Check online reviews for "best free anti-virus or anti-spyware" to make sure these programs meet your specific needs.

Turn Off Remote Access

If you're worried about someone remotely accessing your computer, either legitimately or without your permission, you can turn off its ability to allow remote access. You can always turn it back on if you need remote access to your computer.

How you turn off remote access on your computer depends on the operating system you are running. On a Windows computer, you want to turn on the setting that says: "Don't Allow Remote Connections to this Computer" (generally found under the Control Panel). If you have a Mac, go to System Preferences/Sharing, and uncheck "Remote Login" and "Remote Management." The best way to find specific instructions for your computer is to Google "how to turn off remote access to [your operating system (e.g., Windows 11)]."

Disable File Sharing

If your computer is connected to a network (even if it's not connected to the Internet), other devices that are connected to the same network can access the files on your computer. This may be a concern if you're connected to a public Wi-Fi

network and you have your settings set up to share. If you don't need someone else to have access to your files, disable file sharing.

How you disable file sharing depends on the operating system you're using. The best way is to Google "how to disable file sharing on [your operating system (e.g. Windows 11)]." For most Windows operating systems, the setting will be under the Control Panel and you want to select "turn off file and printer sharing." For a Mac, go to System Preferences/Sharing, and uncheck "file sharing" and "printer sharing."

Use a Non-Admin Account for Everyday Use

Some malware and "hacks" require administrative access to your computer. This means that if you're signed in as an administrator on your computer and accidentally click on a link that has malware embedded, it will download and install. However, if you are signed in to your computer as a non-administrator and set it up so that a non-administrator account cannot install software, it won't install even if you accidentally click on a link with malware.

It is, therefore, helpful to create a non-administrator account on your computer for everyday use. You can always log in on the administrator account if you need to install software or make changes to your computer. Both Windows and Macs allow you to create multiple users.

Practices to Enhance Computer Security

In addition to computer settings that you can turn on or off and running software to help protect your computer, there are other good practices that you can use to increase your computer's security and your privacy.

Put a Password on Your Computer

Locking down your computer with a password is the first thing you can do to prevent someone from gaining access to your content. While most people are worried their computer will be "hacked," the easiest way for someone to gain access to your computer is simply by having physical access to it, either because they have stolen it or are in your home. Remember, it is easier for someone who you've been in a relationship with to guess your password and have access to your device.

Don't Click on Unknown or Suspicious Links

Another good practice is not to click on links or attachments from suspicious people or websites. Because malware can sometimes be embedded in these links or attachments, opening one could install the malware. If you need to receive files or open links from an abusive person or someone you don't trust, consider using a cloud-sharing service to share files or communicate the information in another way.

Log Out of Accounts and Quit Programs

When you finish using an online account, a program on your computer, or even the computer itself, quit and log off. Leaving accounts and your computer logged in could make it easier for someone else to get into your accounts. Even if you don't think someone has physical access to your computer, it's always best practice to log out when you're done.

Turn Off Access Points When Not in Use

Turn off Wi-Fi, Bluetooth, Airdrop, or other connectivity access on your computer if you're not using it. If the access point isn't open, it will be harder for someone to connect remotely. You can always turn it on when you need to connect.

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 WESNET's Tech Safety project, based on their resource Computer and Laptop Security Tips.

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