Being Web Wise

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.

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.

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