Cyber Safety

Technology can be a very useful tool; however, it can also make a person vulnerable in many ways, particularly for survivors of family violence. An abuser may misuse technology to stalk, control, harass, threaten, or bully their victim. For example, if a family/joint plan is in the abuser's name, they may be able to make changes to the victim's account, and access emails, texts, and other accounts linked to other devices (cellphone, tablet, computer, etc.). They may install software to monitor cellphone use or location, or reset passwords to gain access to personal information, such as online banking. They may share private photos online without consent. Technology facilitated violence is a crime. If you feel unsafe, call the police or talk to someone you trust.

The following are suggestions for how you can keep yourself safe while using technology.

1. Cellphone Safety

□ - Call your phone company and ask who is allowed to access and make alterations to your account information. Ask to put a verbal password on your account so that nobody else can make changes on your behalf.

□ - When you call your phone company, ask about what settings are currently on your cellphone, particularly any phone tracking software.

□ - To protect your privacy, ensure that any location tracking settings are turned off such as ‘find my iPhone’, snapchat maps location, google maps location, or location on dating applications. When searching for stores in your area, do not enable websites to use your location.

□ - Change your phone number and set your caller ID to private caller or blocked number.

□ - If you are especially worried about your phone number or location being tracked, consider getting a ‘pay-as-you-go’ phone.

□ - Remember that for incoming calls, caller ID can be spoofed to falsify the phone number displayed. Be sure to answer your phone with caution; the number on the screen may not always reflect who is calling. Voices can also be spoofed to mimic a male or female voice and conceal a caller’s identity. To learn more about spoofing, visit https://crtc.gc.ca/eng/phone/telemarketing/identit.htm (Government of Canada)

2. Computer Safety

□ - Enable firewalls and antivirus software to your computer; hit agree when asked if you would like these to be updated automatically.

□ - If you suspect your computer is being monitored, change all of the passwords on your accounts immediately. Consider using a different computer (e.g., a PC at a public library) for any private communication and web browsing.

□ - Remember to log out of your online accounts and apps when you’re done using them.

□ - Follow safe browsing tips listed below to further protect your computer use.

3. Internet Browsing Safety

□ - Use anti-virus software and ensure you update it regularly or set it to update automatically.

□ - Browse in incognito mode to keep history and data from saving on your computer.

□ - Periodically clear your history, cookies, and any saved passwords and data.

- □ Click “no” when sites or apps offer to download your contact list to help connect you with your friends, or when they offer to save your password.

- □ Many online resources for family violence have a Quick Escape Button, which closes the webpage you are on and opens a more generic webpage (e.g., the weather). However, in most cases, your browsing history can still be obtained by hitting the back button. Keep this in mind when browsing sensitive material.

4. Social Media and Accounts

- □ Don’t post anything on your social media that you would not want your abuser to see. Even when your privacy is set high, it may still be possible for them to view your content.

- □ Review your privacy settings on your social media and accounts and make sure your information is not set to “public” or “friends of friends”.

- □ Change your passwords for all hardware and accounts. A secure password is over 12 characters; contains letters (mixture of capital and small), numbers, and symbols; and doesn’t contain any identifying information, such as your full name or birth date. When prompted for security questions, ensure that your answers are not easy to guess.

- □ Create email addresses and usernames that don’t contain identifying information, such as your full name or birth date / year.

- □ Talk to friends and family about what you are comfortable with them sharing about you on their own accounts.

- □ Do not open attachments from an unknown sender or untrusted person.

For more information on cyber safety, view the resources below:

- **A guide for Canadian women experiencing technology-facilitated violence: Strategies for enhancing safety.** https://bcsth.ca/wp-content/uploads/2019/03/BCSTH-A-guide-for-Canadian-women-experiencing-technology-facilitated-violence-2019-1.pdf

- **Get cyber safe.**

  https://www.getcybersafe.gc.ca/index-en.aspx

- **A decision aid for women affected by intimate partner violence: *iCAN Plan 4 Safety*.**

  https://icanplan4safety.ca/

- **Technology safety & privacy: A toolkit for survivors.**

  https://www.techsafety.org/resources-survivors

- **Sample-technology-facilitated violence log.**

  https://bcsth.ca/techsafetytoolkit/sample-technology-facilitated-violence-log/