DIGITAL SELF-DEFENCE TOOLKIT

A Guide for Understanding and Reporting Technology-Facilitated Gender-Based Violence

PEI Coalition for Women's Leadership

CONTENTS

ACKNOWLEDGEMENTS

Land Acknowledgement

We recognize that the PEI Coalition for Women's Leadership is located on ancestral and unceded Mi'kmaq territory. We extend our deepest respect to all Mi'kmaq and other Indigenous peoples living on the land of Epekwitk, within Mi'kma'ki. We are all Treaty People.

Background

Technology-facilitated gender-based violence, and the poor regulation of many social media platforms, are threats to our democracy and the wellbeing of our communities. These issues will continue to directly impact who steps into leadership positions in this country, and who does not. The Coalition hopes the *Digital Self-Defence Toolkit* will provide education on tech-facilitated violence, and support those experiencing it.

During the initial toolkit development, the Coalition received invaluable guidance from staff members of the following PEI non-profit organizations:

Jane Affleck, Native Council of PEI
Sarah Dennis, Community Legal Information
Lucky Fusca and Adam MacIntyre, PEI Transgender Network
Khousmita Gopaul, ResourceAbilities

As the project progressed, the Coalition was privileged to learn from the following experts whose academic research and professional experience on technology-facilitated violence and Canadian Law significantly informed this toolkit:

Suzie Dunn, Assistant Professor, University of Dalhousie
Rhiannon Wong, TechSafety Canada
Constable Robert Yaschuk, L Division of the Royal Canadian Mounted Police (RCMP)
Courtney Clarke, Our Time to Lead
Hannah Jones, Community Legal Information
Women's Network
PEI PEERS Alliance
Family Violence Prevention Services
Pride PEI
United Way Maritimes
BIPOC USHR

A special thank you from the Coalition team to **Mag Lillo**, of Ruby Square Graphic Design, for their incredible work on this toolkit. Thank you again to all contributors!

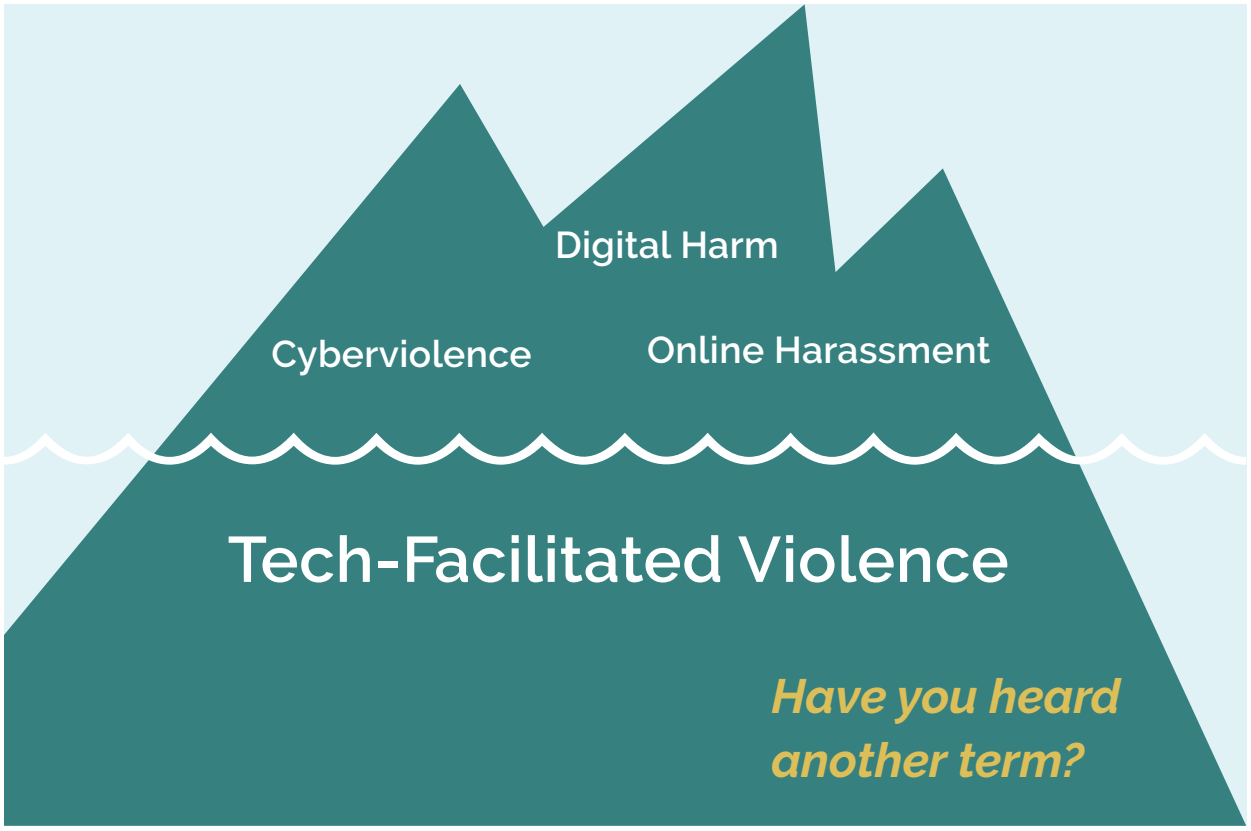
This *Digital Self-Defense Toolkit* was made possible by the Prince Edward Island Interministerial Women's Secretariat, with financial support from the Government of Canada Department for Women and Gender Equality in support of the National Action Plan to End Gender-Based Violence.

Prince Edward Island CANADA

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

INTRODUCTION

Have you ever heard the term "cyberbullying"? What about "harassment", "cyber violence", or "digital harassment"? What do these words make you think of? Has someone you know received abusive text messages or calls? Had private information shared without your permission? These terms are just the tip of the iceberg. To learn more about them, we need to discuss technology-faciltiated violence (TFV).



TFV is used as a tool to silence, harass, intimidate, and limit a person or group's full participation in society, often threatening their safety or wellbeing. Technology has become a huge part of our society, making it nearly impossible to avoid interacting with it in some way. We're often told to "just log out" or "ignore the hate," but that's not always an option.

To be more specific, technology-facilitated violence (TFV) involves misusing technology such as computers, smartphones, GPS devices, cameras, and artificial intelligence (A.I.) to hurt or control (Tech Safety Canada, 2024).

This digital self-defence toolkit focuses on technology-facilitated gender-based violence (TFGBV), particularly in online spaces, and the misuse of technology to commit abusive acts. It explains the different types of tech-related violence, and offers safety tips. The toolkit also includes a reporting log to help users document and report incidents. This resource is framed with the well-documented understanding that women and gender-diverse people in Canada are statistically more likely to experience TFGBV. We hope this toolkit helps women and gender-diverse leaders better understand these issues, and that it sparks conversations about how to counter TFGBV and TFV together.

The following actions are just a few real-world examples of TFV or TFGBV that are happening in Canada and around the world right now:

- Leaving threats of physical violence on Facebook posts
- Sending an e-transfer of $1 to a bank account after a no-contact order
- Monitoring someone's location through Snapchat
- Sharing someone's home address over social media with harmful intention
- Using someone's online accounts without permission
- Creating and sharing A.I. generated images to damage a person's reputation
- Sharing a private photo of someone without their consent
- Repeatedly calling a home phone or cellphone during the night
- Sending non-consensual photos over text message
- Using a person's phone, hidden camera or app to watch them
- Using technology to find out what someone is doing without their permission

To understand the root causes and origin of contemporary gender-based violence in Canada, we must understand the historical and present day impacts of colonialism. Settler monarchies and institutions invaded Indigenous lands, creating colonial structures, policies, patriarchal narratives, and systems of control. It is important to remember that these narratives harm everyone; their impacts have led to forced loss of cultural identity, loss of community connections, and created immense generational trauma, the impacts of which are ongoing today. It is also vital to recognize the ways Indigenous women, girls and Two Spirit (2S) people continue to be more affected by gender-based violence nationally, namely the ongoing crisis of missing and murdered Indigenous women, girls, and 2S people, and the mass incarceration of Indigenous women (Reclaiming Power and Place: The Final Report of the National Inquiry into Missing and Murdered Indigenous Women and Girls, 2019). This issue is inseparable from ongoing settler colonialism and the cultural genocide of the Indigenous people in Canada, connected directly to modern day gender-based violence.

TECH-FACILITATED VIOLENCE IN PEI & CANADA

Tech-facilitated violence impacts all people who exist in spaces where technology is used. However, some individuals and groups of people are more impacted than others, particular women, BIPOC individuals, persons with disabilities, and members of the 2SLGBTQIA+ community *(Deplatforming Misogyny: report on platform Liability for Technology-Facilitated Gender-Based Violence*, 2021).

If you are reading this, and have experienced some form of tech-violence, you are not alone.

To understand these statements, let's turn to the current data.

Remember!

The problem is not technology or the internet, but poor safety policies and built-in human bias that has led to new ways for people to be abusive. Social media platforms should have a greater responsibility to the people using their platforms, and they must be held to account.

The PEI Coalition for Women's Leadership will continue advocating for legal and systemic level changes to help protect individuals from these harms.

In 2025, the Canadian Women's Foundation published a research report called "Challenging Gendered Digital Harm", which revealed that:.

- **In Canada, 61% of women and gender-diverse people have experienced gendered digital harm, compared to 53% of the overall population.**
- **Members of the 2SLGBTQIA+ community, Black women and Indigenous women are amongst those most frequently targeted.**
- **30% of Indigenous women experience unwanted behaviour online.**
- **Youth (ages 18–25) and underserved communities are twice as likely to consider or engage in self-harm or suicide as a result of experiencing digital harm.**
- **84% of women and 87% of 2SLGBTQIA+ take more actions to feel safe from online hate and abuse compared to 77% of men**

Statistics Canada found that young women (18-29) are nearly twice as likely to experience TFV compared to young men of the same age range.

(Statistics Canada, 2023).

Two Canadian organizations, the Open Digital Literacy and Access Network (ODLAN) and Wisdom2Action learned that 80% of Two Spirit, Transgender, and Non-binary (2STN+) working professionals surveyed had experienced transgender online hate directed at them or the 2SLGBTQIA+ organization they worked for.

(Navigating Digital Harms, 2025).

The most prevalent forms of Two Spirit, Transgender, and Non-binary (2STN+) online hate identified in the report include but are not limited to:

- **Accusations of predatory sexual behaviour towards children**
- **Transphobic and homophobic slurs**
- **Threats of physical violence**

What impact does this have on individuals and communities?

Tech-facilitated violence (TFV) can have an immediate and long-lasting impact on a person's mental, emotional, and physical well-being. In the moment, survivors may experience intense fear, anxiety, and a loss of control. The impacts of TFV and TFGBV can range from:

- **Self-censorship**
- **Withdrawal from online spaces**
- **Safety concerns**
- **Long-term harm to their careers, relationships, and health**
- **Harm to self or others**

The 2025 Canadian Women's Foundation study indicates that 55% of perpetrators are men, and in 23% of cases, survivors didn't know the gender of the person targeting them.

The digital platforms where this violence occurs often amplify harm rather than prevent it. Social media companies are primarily driven by engagement metrics and advertising revenue, meaning that posts generating strong reactions, such as those fueled by misogyny, racism, and hate, are often prioritized by algorithms. This creates a feedback loop through which harmful content gains visibility and traction, locking users into viewing toxic content.

How does technology and harassment factor into women's leadership, and foster a healthy democracy?

Cyberviolence, digital harm, and tech-violence impact who you see running for office, and who ends up staying there. The people who hold elected positions in Canada make decisions that impact your everyday life. Increased diversity in these roles means more community members will have a voice at the table. When it comes to supporting a healthy democracy,

> *"On election day I posted a photo of myself on my campaign X/Twitter account reminding everyone to vote. Under that tweet I received 35+ separate replies from accounts questioning my mental stability, and hate speech related to my gender. Some of the accounts were from PEI, but most were not local as far as I could tell."*

(2023 PEI Provincial Election Candidate)

Did you know that tech-facilitated violence has been used to target women and gender-diverse leaders on PEI?

You can read more about this in the Coalition's report: *Technology-Facilitated Gender-Based Violence: Report on the prevalence of TF GBV during the 2023 PEI Provincial Election*.

equal representation also matters. Research reveals a strong correlation between the status of women in a country, and this country's democratic health; the Georgetown Institute for Women, Peace, and Security (WPS) Index is just one example. After measuring 96 democratic countries, it was proven that the status of women is significantly associated positively with key democratic dimensions, namely; election integrity, freedom of association and assembly, and checks on executive power (Exploring the links between women's status and democracy, Georgetown University 2023). TFGBV and TFV is used to reduce this diversity, to silence and intimidate. To counter this, we must understand the language of this harassment, and know what to do if we, or someone we know, is targeted.

73% of Canadian women are concerned about the online harassment they'd face if they ran for public office, compared to 63% of Canadian men.

(*Equal Voice* 2023)

> *I did get threatened. A guy must have found my personal email, I don't know how. There were thinly veiled physical violence threats, with a lot of cursing. I determined which district he was from so we avoided his house and the area during campaigning. I was told to maybe call the RCMP, but nothing further. It seemed like no one knew what to do.*

DEFINITIONS

Understanding the Language of Tech-Facilitated Violence

The following terms define and describe technology-facilitated gender-based violence, and its common forms. The individual impacts and consequences of tech-violence are often downplayed because of the false perception that abuse taking place online or through technology cannot really cause harm. This is entirely false. It is important to name these acts when we see them, allowing us to understand and take action. Keep in mind, technology is constantly changing and so the language used to describe these behaviours evolves too (*Technology-facilitated Gender-based Violence: Making All Spaces Safe*, 2021).

Technology-Facilitated Gender-Based Violence (TFGBV): Any act that is committed, assisted, aggravated or amplified by the use of information communication technologies or other digital tools that results in or is likely to result in physical, sexual, psychological, social, political or economic harm or other infringements of rights and freedoms. This form of violence is directed against someone because of their gender, disproportionately impacting women, girls, and Two-Spirit, trans, and non-binary people (UN Women).

Cyberbullying: Using digital messaging such as group messages, texts, emails, direct messages to harass, intimidate or harm others; this term is typically associated with children and youth.

Cyberstalking: The use of technology to stalk and monitor someone's behaviours in real-time or historically. This can include putting Apple Airtags on someone's car or monitoring their movements via location sharing on Snapchat or Instagram maps.

Digital-to-Physical-Violence: When prior or ongoing online threats and digital hate speech escalate to real-life/in person stalking or physical attacks.

Doxing: Using an online platform to publicly reveal a person's private details such as a home address, personal email, phone numbers, workplace, family contacts, and/or photos of their family members, to locate and cause harm. (See *"Deadnaming"* in the Glossary).

Cyberviolence

A term that is becoming more common, and while it is close to the definition of TFV, it is not the same.

The prefix of the word is "cyber" which refers to "involving, using, or related to computers, especially the internet".

This definition therefore excludes the use of technologies that do not involve computers or the internet, such as cameras, landlines, etc.

(*Cambridge Dictionary*, 2024).

Hacking: Using technology to gain access, illegally or without permission, to systems or resources to attack, harm, or incriminate someone. This includes stealing data, getting personal information, changing information, violating privacy, or infecting devices with viruses.

Image-Based Abuse (IBA): The use of images to coerce, threaten, harass, objectify, or abuse a target. This involves taking, creating, threatening to share, or sharing intimate and/or sexual images without consent. This can include sexual, but also non-sexual images. A non-sexual image is any photo that a target defines as private; for example, a photo is shared on social media of a Muslim woman, not wearing a hijab, when she always wears a hijab in public. (See "*Non-consensual Distribution of Intimate Images*", "*Creepshots*", "*Sexploitation*", "*Sextortion*", and other terms in the Glossary)

Impersonation: Stealing someone's identity to threaten, intimidate, or damage their reputation. This can look like using someone's photos to create a fake profile and posing as a trusted friend to get private information. (According to most of the common social media platforms, impersonation does not include obvious parody accounts.)

Online Defamation: Releasing fake information to the public that harms someone's reputation and aims to humiliate, threaten, intimidate or punish them. This is especially common for public figures like politicians, activists and journalists, but anyone in a visible position of leadership is more likely to be targeted.

Online Harassment: Using online platforms to repeatedly contact, threaten, and/or scare another person through offensive, degrading, or insulting comments, messages, and/or images. (See: "*Cross Platform Harassment*", "*Digital Hate Speech*", and "*Digital Threats*" in the Glossary)

Perpetuator: Someone who uses technology to hurt another person or group regardless of their intention; this word should be understood as potentially applying to everyone, since everyone is capable of both causing harm, but also learning from mistakes.

Have you heard of Community Legal Information's guide on what to do if your intimate images are shared?

Check out this resource:

HOW TO PREVENT & RESPOND TO TFV AS AN INDIVIDUAL

Before we get into community-level action, let's talk about the individual costs of preventing and addressing tech-violence, and the possible financial barriers.

Wellbeing Costs

It is important to recognize the emotional burden required to take personal protective measures against technology-facilitated violence. Being targeted can impact your physical and mental well-being, your income, your sense of safety, your confidence, and more. Remember that turning to friends, family and community support is a sign of strength. You do not have to address this alone.

Financial Costs

The financial costs of protecting yourself can be high. Some individuals can afford additional safety measures, like a virtual private network (VPN) service, virus protection software, and password managers while others cannot.

These are the top five basic prevention tips, serving as examples of individual steps you can take to increase your safety.

TOP 5 BASIC TECH SAFETY TIPS

1. **Use strong passwords and usernames (do not use your pets' names!)**

UNSAFE PASSWORD HABITS

- Using common or obvious passwords such as "QWERTY123" or "Password"
- Using your birthday, a loved one's birthday, or significant anniversary dates
- Using one password for every account
- Using answers that others might know or guess for questions to verify your identity (e.g., your mother's maiden name, your favourite colour, the model of your first car)

How secure is my password?

Test it out with Tech Safety Canada:

If someone spent 10 minutes looking at your Facebook or Instagram profile, would they be able to figure out your password?

SAFER PASSWORD HABITS (Tech Safety Canada, 2024).

- Use passphrases: words that are different but not related
- Change letters to symbols or numbers (instead of 'a' use @, instead of 'E' use 3) Example: H@ppyw@t3rbottl3
- Test your password at how secure is my password: www.security.org/how-secure-is-my-password/
- Use a secure password manager
- Change your passwords every 6 months
- Do not allow your Google or Facebook account shared access to your passwords for other websites or accounts

2. Log out of accounts and apps

Uncheck the "keep me logged in" option, and don't let web browsers save your passwords for automatic login. This prevents others from using your device to pretend to be you through your accounts. Write down your login information on paper or use a password manager.

3. Turn off location sharing

Smartphones can track your location, and some apps will sell your data to third-party corporations. You could be sharing where you are without even knowing it. Stop apps from using your location by turning off this feature in your phone's privacy settings. Social media accounts also have privacy settings to limit who see your location.

Did you know Instagram recently implemented location sharing on their platform? Make sure to review your privacy settings regularly, especially after an app updates on your device!

4. Use private browsing

You can browse the internet privately using Mozilla Firefox, Microsoft Edge, Safari, and DuckDuckGo. Private browsing stops others from seeing which websites you visited. This is safer when using a friend's computer or a public one, or if you suspect that someone is monitoring your device without your permission. Note that this action is not a guarantee of privacy; for example, Google Chrome is currently facing a lawsuit because its incognito mode has been found to breach privacy.

5. **Use two-step verification**
   To set up two-step verification, you'll need a second email address or a secure mobile number. If someone tries to log in to your account from a different device or location, the email platform, bank, or other service will send a code to your second email or phone. You'll need this code along with your password to sign in. If you don't have access to the secondary email or phone, you can't log in.

HOW TO PREVENT & RESPOND TO TFV AS A COMMUNITY

Ending tech-facilitated violence (TFV) and tech-facilitated gender-based violence (TFGBV) isn't something one person can do alone. We need community-driven efforts that push for safer, more accountable digital spaces. Below are concrete steps you and your community can take to make meaningful change together:

Advocate to All Levels of Government

Push for Policy Change: Join forces with organizations advocating for stronger digital safety regulations. Contact your local member of Parliament (MP, i.e. federal representative), member of the Legislative Assembly (MLA, i.e. provincial representative) through email, phone, social media, and/or at events to express your desire for safer tech-usage.

Call for a Digital Safety Commission: Encourage the federal government to establish a Digital Safety Commission to oversee online safety and digital rights. This can start with sending an email or having a conversation with your MP to share why online safety matters to you and your community.

Engage with the new Canadian Minister of Artificial Intelligence & Digital Innovation, the Minister of Justice, and Attorney General of Canada, and other relevant Cabinet Ministers: Urge Ministers and/or your MP to introduce a bill that holds big tech companies accountable for enabling or ignoring harmful behaviors on their platforms.

Learn from Global Movements

Places like Australia, Chile, Brazil, the European Union, and several others are already leading the way with new regulations that address TFV. Explore their approaches and think critically. What do you agree or disagree with? What could work in your community? Sharing global best practices helps strengthen the movement for digital safety at home.

Help Hold Big Tech Accountable

Demand Transparency and Responsibility: Join campaigns or initiatives challenging tech companies that are slow to act or avoid taking responsibility for the harm happening on their platforms.

Support Regulations with Consequences: Advocate for laws that include clear accountability mechanisms for digital platforms that allow abuse to continue unchecked.

Build Safer Online Communities

Adopt Codes of Conduct: Encourage your workplace, school, or volunteer spaces to adopt online codes of conduct and clear rules of engagement that prioritize digital safety.

Create Alternative Accountability: Not all harm needs to, or should, go through the criminal justice system. Advocate for and support community-led models of accountability that center survivors and repair.

Support Education and Learning About Online Misogyny: Organized hate-groups currently exist on multiple online platforms, with the goal of spreading and directing hate towards women, transgender, and gender-nonconforming people. Providing and encouraging education on terms like "manosphere", "incel", and the "red pill", as well as the critical thinking skills to spot this content, are vital to ending the support for these movements. This education is especially important for young men and boys, as these groups actively target and recruit from these demographics.

Talk About It

TFGBV is often minimized or ignored. Start conversations with your friends, family, and community. Raising awareness is one of the most powerful tools we have. When more people understand the issue, more people can take action.

Remember

Community action multiplies impact. Whether you're voicing your concerns to a politician, organizing a new workplace policy, or just starting a conversation, every step you take helps build a safer digital world for everyone.

WHAT CAN ONLINE BYSTANDERS DO?

The intensity of technology-facilitated violence can vary. If you or someone you know is in a potentially life-threatening situation, contact the relevant authorities and/or local services you feel safe with. Being a bystander in these situations means keeping yourself safe, and carefully assessing the level of risks associated with getting involved, as well as the impacts it could have on others. The rest of this section provides clear steps on how to be a helpful bystander, and take action.

A great method of countering online hate is for people to support each other in virtual spaces. From the comments section on Facebook, to work email chains, there are many ways to show support and act as a positive role model for others who are experiencing TFGBV or TFV.

The following acronym will help you to remember actions you can take as a bystander. The AIDED model was created by the University of La Trobe in Melbourne, Australia. It has been modified for use in this toolkit to the following:

A - ASSIST in finding supports
I - INDIRECT actions
D - DIRECT actions
E - EVIDENCE of the incident
D - DIVERT the harm

Not all situations will call for every action listed above. To help distinguish when to use which method, here are some examples of the AIDED model in action:

EXAMPLE ONE

Your co-worker receives an email from an unknown sender to their office account. This message contains threats of harm, including slurs targeting their gender. The co-worker is confused about how their email was found by this person, and is unsure of what to do.

Indirect Actions: Talk with your co-worker about the event. Offer them support, and be someone to listen to if they just want to talk about the situation.

Looking for more **indepth protection methods?** Visit a resource from **Take Back the Tech:**

Are you interested in encouraging the federal government to form a **Digital Safety Commission?** Find out more here:

Assist in Finding Supports: Find out what supports are available within your organization, whether through the human resources department or a TFV policy they can follow.

Divert the Harm Away from the Target: In what ways could your workplace prevent this from happening again? One way would be to establish a general email address that receives all inquiries, and uses a CAPTCHA test to accept emails. Another would be to make sure the office team is aware of where their work emails are listed on the internet. You can also encourage them to block this unknown sender from their account.

EXAMPLE TWO

Your friend confides in you that their ex-partner, who is still a friend of yours, has been sharing intimate images of them without permission since the relationship ended. They feel very uncomfortable, and upset that these pictures are being shared.

Direct Actions: Be mindful of the relationship dynamics of everyone involved, and talk to your friend about the actions they want to take. These actions could include speaking to other people who have received the images, and asking them to ensure they are deleted from their devices.

Evidence of the incident: For example, if someone sent them screenshots of the images that the ex-partner shared, tell your friend to print copies of the exchange and to save them to a protected device, especially if they want to take legal action.

Note: On Prince Edward Island, there are grounds for legal action in Example Two, as the non-consensual sharing of intimate images is covered by the Intimate Images Protection Act (2021).

EXAMPLE THREE

An immediate family member shares their opinion about a controversial topic on a public social media platform. After their post gains attention, a group of users who disagree with them begin to harass them online with hateful comments, sending violent messages, and threatening to sexually assault them. Your family member feels frightened, and calls you for help.

Evidence of the incident: Help your family member document all private messages and public comments including the names of the users who took part in the harassment with screenshots.

Assist in Finding Supports: Your family member says they want to report this incident to the police. Use the tech-facilitated violence log in this toolkit to gather organized evidence to help build their case. You can also support them by reporting the users involved to the social media platform, and by helping them to block those users' accounts.

Remember: Although regulations vary across platforms, it is still important to report suspected or confirmed online harassment, and to block perpetuators. Before deleting harassing comments or blocking the user(s) involved, consider documenting the incident through screenshots.

Together, in tandem with efforts from government and social media companies, we can work to normalise a culture of care, create better online boundaries, and make internet spaces safer for all.

WHY SHOULD YOU LOG EVIDENCE OF TFV?

Four reasons to use a TFV reporting log:

1. **To help identify patterns of behaviour**
   You can be the target of TFV once or multiple times. It is important to date all incidents and organise them in chronological order. This may help to identify a pattern which could lead to more answers, especially in the cases where the harassment is coming from an anonymous source.

2. **To document reliable evidence to support an investigation**
   Evidence of the incident will be used to determine how or if the legal system can respond. If you choose to file a report with the police or seek legal action through the court system, you will be asked to make statements recounting the incident. This log can help you be consistent with your evidence.

3. **To provide an opportunity to take control in an emotional situation**
   You cannot control whether you are the target of TFV but you can be proactive and take control of the situation through documenting your experiences. You can decide later whether you will take the log to the authorities.

4. **To affirm and remind**
   Memories of an abusive event can become blurred over time. The log can provide a reliable recount of how you were negatively impacted. It can also offer you reassurance that this happened, addressing any doubt or dismissal that the event took place and caused harm.

SAFETY PLANNING!

To protect yourself against an abusive person finding the log, think about where you can securely hide it.

Internet Browser Privacy Tips:

When could it be helpful to bring your TFV Report Log to the police?

Depending on the circumstances, it can be important to start a file on the incident. It is also vital to note that reporting does not guarantee action; the police will look for evidence that your case matches the criminal code definition of harassment or another crime.

When you report, the police may ask you what action you want them to take against the perpetuator. Consider what your answer might be before reporting the incident.

Important: The Criminal Code of Canada does not specifically have a single code that covers all acts of TFV, therefore it falls into the 14 codes below:

1. Offence against the person and reputation
2. Criminal harassment
3. Mischief in relation to data
4. Unauthorized use of computer
5. Extortion
6. Uttering threats
7. False messages, indecent or harassing telephone calls
8. Identity theft
9. Sharing intimate images without consent
10. Intimidation
11. Incitement of hatred
12. Counselling suicide
13. Defamatory libel
14. Public incitement of hatred

Technology-Facilitated Violence Report Log

Use the form below to keep a record of any incidents of online or digital harm against you. Document each incident separately and include all supporting evidence of the incident through saved screenshots, photos, video and/or audio recordings. We recommend keeping your own copy of your logs if you submit them to the police. Also consider sharing this log with a trusted person who can provide a secure hiding place for this documentation if necessary for safety planning.

PEI Community Legal Information's RISE Program offers plain-language legal information to victims of sexual or intimate partner violence, or workplace sexual harassment, including up to 4 hours of free legal advice from a trauma-informed lawyer.

***Please note: if you are currently in an abusive situation, and/or suspect your devices are being monitored, consider using the device of a trusted friend, or a public device at a local library or school to access this log. If you have access to only your personal device review Internet Browser Privacy Tips at www.techsafety.ca to learn how to make your browsing data and history more private.**

This resource was adapted from the Stalking and Technology-Facilitated Abuse Log which was developed by Tech Safety Canada, a project of Women's Shelters Canada.

Technology-Facilitated Violence Report Log

Your contact information

Your name:

Date:

Preferred method of contact:
Email:
Phone Number:

Information about the perpetuator or abuser

Legal name(s) and username(s) if known:

Relationship to that person (if applicable):

Perpetuator or abuser contact information (if known)

Home address:

Phone number:

Email address:

Online account/
profile names:

Other relevant info (Usernames/accounts they interact with, the kind of content they share):

Description of the incident

Date of Incident:

Time:

Describe the incident:

Note the names/usernames of any witnesses involved:

Devices

Your devices, accounts or other technology involved in this incident.
Tick as many boxes as needed to describe the event.

- ☐ Smart phone
- ☐ Tablet
- ☐ Computer/laptop
- ☐ Child's device
- ☐ Social media platform
- ☐ Telephone
- ☐ Recording device
- ☐ Unknown, but suspect _____
- ☐ Camera
- ☐ Location tracking
- ☐ Artificial intelligence
- ☐ Gaming device
- ☐ Smart device (e.g. Alexa, Watch, TV)
- ☐ Other

Identify device type/model/make (e.g. iPhone 12):

Accounts

- ☐ Email addresses
- ☐ Social media account
- ☐ Dating app
- ☐ App
- ☐ Bank
- ☐ Government
- ☐ Other
- ☐ Not applicable

Account type (e.g. Gmail, Facebook, Banking App)

Personal consequences of the incident

Describe any behaviour or routine changes you have made as a result of this incident and describe any emotional distress caused by this incident.

Name(s) or username(s) of family, friends or others involved:

Attach any documented (screenshots, recordings) listed here:

Seeking help

Who did you report this to?

- Police
- Support service
- Therapy
- Medical
- Phone/Internet service
- Tech company
- IT professional
- Trusted family or friend
- Employer
- Other

Describe response from services ticked above:

Police reporting

If you reported this incident to the police and gave them the information above for evidence collection in your case, keep this part of the log for your own documents.

Date:

Officer title:

Police Station:

Officer badge number:

Officer name:

Officer phone number:

Compile any receipts related to this incident, and write the total dollar value these instances have cost you (e.g. device replacement, cancelling or starting a new phone plan, therapy sessions, etc.) listed here:

SUPPORT & OTHER RESOURCES

Non-Emergency Phone Numbers

- RCMP (902) 566-7112
- Charlottetown Police Services (902) 629-4172
- Summerside Police Department (902) 432-1201
- Kensington Police Department (902) 836-4499

PEI Helping Tree

This flow chart to inform Islanders of the many helping resources available on Prince Edward Island.
https://pei.cmha.ca/find-help/the-pei-helping-tree/

211 Prince Edward Island

Designed to help those in need "find the right door the first time" by connecting them to human services quickly and easily, the 211 PEI service provides Islanders and service providers with access 24/7/365 by calling 2-1-1. A database of all programs is also available on the website. www.pe.211.ca

Community Legal Information PEI

CLI is a registered charity that helps residents of Prince Edward Island understand the law and navigate the provincial justice system. The RISE program offers specific resources and support for individuals affected by sexualized violence including reporting and seeking help. People of any gender identity or expression 16 years or older can access these confidential services. https://legalinfopei.ca/

PEI Family Violence Prevention Services

This is a community organization, based on the principles of justice, equality, and peace. They are dedicated to the eradication of physical, sexual, and emotional violence in families through advocacy, prevention programs, and the provision of quality services designed to empower and support those affected by family violence. https://fvps.ca/

PEI Human Rights Commission: SHIFT

This project is aimed at addressing and preventing sexual harassment in Island workplaces through awareness, education and free training that is tailored for employers, employees, high school students and the general public.
https://www.makeityourbusinesspei.ca/

Victim Services, Government of Prince Edward Island

Victim Services assists victims of crime throughout their involvement in the criminal justice system. Assistance is available to victims of crime anywhere on PEI. If you live off-Island and are victimized by a crime that occurred on PEI, you are also eligible for services. No fees are charged for this confidential service.
https://www.princeedwardisland.ca/en/information/justice-and-public-safety/victim-services

PEI Department of Justice and Public Safety, Restorative Justice Program

The Restorative Justice program provides an opportunity for offenders and victims to engage in a safe and effective communication (direct or indirect) to share how they have been impacted by the crime.
https://www.princeedwardisland.ca/en/information/justice-and-public-safety/restorative-justice

Mi'kmaq Confederacy of PEI, Indigenous Justice Program

The Mi'kmaq Confederacy provides important legal support to Indigenous people living in Epekwitk (PEI). They focus on helping offenders, victims, and communities who are involved in legal conflicts understand the root causes of their actions. They do this in collaboration with the Indigenous community, ensuring this program respects cultural values and traditions.
https://mcpei.ca/contact/

Cybersafe Care

This is a public education campaign and online resource designed to support parents, caregivers, and educators in helping youth use the Internet safely and responsibly. It offers guidance on topics like gaming, social media, cyberbullying, healthy screen time, and digital well-being—all with attention to PEI-specific context. It was created by the Interministerial Women's Secretariat, through the Government of Prince Edward Island.
https://www.cybersafecarepei.ca/

CANADIAN AND INTERNATIONAL RESOURCES

Open Digital Literacy and Access Network

ODLAN provides Canadian organizations who serve 2SLGBTQIA+ communities with the tools, resources, and knowledge they need to grow and develop inclusive online spaces. https://odlan.ca/

Tech Safety Canada

This website equips women, children, and gender-diverse people with the knowledge and resources they need to navigate experiences of Technology-Facilitated Gender-Based Violence. Information for survivors, supporting survivors and guides on how to secure tech devices can be found here: https://techsafety.ca/

Canadian Women's Foundation: Reclaim Your Digital Space

This foundation offers a free e-learning course that helps you build skills, knowledge, and provides resources to engage safely in digital spaces and help end gender-based digital harm.
https://learn.canadianwomen.org/courses/reclaim-your-digital-space-help-end-gender-based-digital-harm?_gl=1*eh-2bwl*_gcl_au*MjAxNDA0NjY1NC4xNzU0NTkyNDc4

Canadian Centre for Women's Empowerment

The CCFWE is a non-profit organization working to dismantle systemic barriers facing survivors of economic abuse, coerced debt, and financial exploitations. Guided by equity and trauma-informed research, we drive prevention and response through systemic change and community engagement. https://ccfwe.org/

Crash Override

This advocacy group provice support and resources for people who are experiencing online abuse. They are a network of experts, and survivors who work directly with victims, tech companies, lawmakers, media, security experts and law enforcement to educate and provide direct assistance working to eliminate the causes of online abuse.
http://www.crashoverridenetwork.com/index.html

GLOSSARY

These terms are related to and inform the foundations for technology-facilitated violence. Please note that these are not legal definitions, and may have a different definition according to Canadian Law.

Astroturfing: A misleading tactic that conceals the true supporters of a planned message or campaign, whether political, commercial, religious, or promotional. The goal is to make the message seem like it comes from genuine, independent grassroots contributors, rather than from secret, or sponsored effort.

Bot Account: This is an online account or social media profile run by software instead of a human. Bots can automate actions like posting, messaging, or interacting with users; while some serve useful roles, others are used for spam, misinformation, or manipulation.

Coercive control: A behaviour or repeated pattern of behaviours involving assault, threats, humiliation, intimidation, and/or other forms of abuse intended to harm, punish, and/or instill fear in someone.

Consent: This is an ongoing process of giving and receiving permission. This means there is an active "yes" between everyone involved who is able to authentically and legally consent to what is occurring.

Cross-Platform Harassment: The planned and organized harassment against someone by one or more people through different online platforms simultaneously.

Deadnaming: A type of direct harassment that involves revealing someone's former name against their wishes with the intention of causing harm. It is often used to expose members of the 2SLGBTIA+ community who go by a name that is different from a name they previously used and/or were assigned at birth.

Digital Footprint: This refers to the trail of information you leave behind when you use the internet. (e.g. browser history/cache). This includes data generated by the websites you visit, the emails you send, the forms you fill out, and/or the files you download.

Digital Hate: Any text-based communication (comments, posts, direct messages, emojis) or media-based (images, videos, animations, voice recordings, etc.) that attacks and encourages violence against a person or group based on their identity. This includes targeting someone's gender, race, ethnicity, disability, sexuality or any other identity factor.

Digital Threats: A statement of intention to inflict pain, injury or damage against someone, their family, and/or their property through the use of digital technology.

Discrimination: This is behaviour that results from prejudiced attitudes by individuals or institutions, resulting in unequal outcomes for persons who are perceived as different.

Dogpiling: Piling-on or dogpiling is a type of online harassment where multiple people collectively target one individual with insults, threats, and/or hostile messages. These attacks are often coordinated or occur in waves, aiming to overwhelm, and intimidate the person.

Gender-Based Violence: Refers to harmful acts directed at an individual based on their gender, or their perceived gender-identity. It is rooted in gender inequality, the abuse of power, and norms rooted in patriarchy, colonialism, and other systems of oppression.

Image-based Abuse: This is an umbrella term used to describe the following forms of TFGBV that are related to digital images (Dunn, 2020).

i. **Altered media and/or deepfakes:** Digital images, videos and audios created or altered by artificial intelligence or photo editing software to make it seem like a person is saying or doing something they never said or did. Deepfakes can be hard to tell apart from real videos and images. They are often used to create fake sexual content, such as putting someone's face in a pornographic video without their consent. People are also creating fake audio to use in scam phone calls.

ii. **Documenting or broadcasting sexual assault/violence:** This involves recording videos or live stream broadcasts of sexual violence. These videos are sometimes posted on social media, texted among peers and sold or traded to people and/or websites.

iii. **Non-consensual distribution of intimate images:** This occurs when a person's sexual or private images are shared with other individuals, or a wider audience than intended, without their consent.

iv. **Sexploitation:** This term involves profiting from websites dedicated to sharing non-consensually distributed intimate images or pur chasing sexual abuse content. Example: fake modelling job ads that trick people into sending sexual images of themselves.

v. **Sextortion:** This occurs when an individual has or claims to have a sexual image of another person and uses it to coerce them into doing something they do not want to do, or to make demands for money, by threatening to release their images.

vi. **Voyeurism/creepshots:** This occurs when a person secretly takes photos or records videos of another person for a sexual purpose. This includes cases where an abuser copies images from a target's social media page and uses photo editing software to create a new photo that depicts the target in a sexually exploitative manner.

Online Reputation: As individuals spend time online, they begin to build an online reputation. This reputation is shaped by their online behavior, including the websites and apps they publicly use, and the content they choose to post or share.

Prejudice: This term encompasses positive or negative attitudes toward a person or group, formed without just grounds or sufficient knowledge, which will not likely change despite new evidence or contrary arguments. Frequently prejudices are not recognized as false or unsound assumptions or stereotypes, and, through repetition, can become accepted as common sense notions.

Transphobia: This is defined as negative attitudes, beliefs, feelings, and/or behaviours against Two-Spirit, trans, nonbinary, gender nonconforming, and intersex people due to their being trans or being perceived as trans. The underlying foundation of transphobia is a rejection of human gender diversity beyond two fixed genders (i.e., belief in a heteronormative sex/gender binary). Two-Spirit, transgender, and nonbinary people (2STN+) face distinct forms of targeting, resulting in experiences of gender-based violence that are specific to this group.

Two-Spirit, 2-Spirit, or 2S: This English umbrella termstands for the many words used in different Indigenous languages to affirm the interrelatedness of multiple aspects of identity including gender, sexuality, community, culture and spirituality. Some Indigenous people identify as Two-Spirit rather than, or in addition to, identifying as lesbian, gay, bisexual, transgender or queer. The Two-Spirit identity label is exclusive to Indigenous people; non-Indigenous people are not welcome to use it to describe themselves.

Vote Brigading: This term describes a coordinated action to manipulate the results of an online poll, or vote (such as up or down voting videos or comments), to shift the desired outcome, and/or to highlght the content to more people as the result of many online algorithms.

REFERENCES

CYBER | *English meaning - Cambridge Dictionary.* (2024, August 21). Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/cyber

Dunn, S. (2020). *Technology-Facilitated Gender-Based Violence: An Overview.* Dalhousie University Schulich School of Law.

Equal Voice. (2023, June). *Modernizing Legislatures - What We Heard Report.* https://www.equalvoice.ca/modernizing_legislatures

Frequently asked questions: Tech-facilitated gender-based violence. (n.d.). UN Women. https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/tech-facilitated-gender-based-violence

Glossary. (n.d.). Learning Network. https://gbvlearningnetwork.ca/our-work/glossary/index.html

Home Publications Technology-facilitated Gender-based Violence: Making All Spaces Safe. (2021, December 1). United Nations Population Fund. https://www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe

Howard, J. (2024, April 2). *Online Hate and Cyberviolence.* Canadian Women's Foundation. https://canadianwomen.org/the-facts/online-hate-and-cyber violence/

Khoo, C., & LEAF. (2021). *Deplatforming Misogyny: report on platform Liability for Technology-Facilitated Gender-Based Violence, Executive Summary.* https://www.leaf.ca/publication/deplatforming-misogyny/

La Trobe University. (2021, August 18). *Bystander Action: Technology-facilitated abuse.* https://www.latrobe.edu.au/mylatrobe/bystander-action-technology-facilitated-abuse/

National Inquiry into Missing and Murdered Indigenous Women and Girls. (2019). *Reclaiming Power and Place: The Final Report of the National Inquiry into Missing and Murdered Indigenous Women and Girls* (Vol. 1a). https://www.mmiwg-ffada.ca/wp-content/uploads/2019/06/Final_Report_Vol_1a-1.pdf

Raney, T., & Collier, C. N., (2024). Gender-Based Violence in Canadian Politics in the #MeToo Era. University of Toronto Press.

Stalking and Technology-Facilitated Abuse Log – Tech Safety Canada. (2024). Tech Safety Canada. https://techsafety.ca/resources/toolkits/stalking-and-technology-facilitated-abuse-log

Statistics Canada. (2023, 02 21). *Study: Online harms faced by youth and young adults: The prevalence and nature of cybervictimization.* https://www150.statcan.gc.ca/n1/daily-quotidien/230221/dq230221c-eng.htm

Tech Safety Canada. (2024). *Passwords: Simple Ways to Increase Your Security.* https://techsafety.ca/resources/toolkits/passwords-simple-ways-to-increase-your-security

10 Easy Steps to Maximize Tech Use Privacy. (2024). Tech Safety Canada. https://techsafety.ca/resources/ toolkits/10-easy-steps-to-maximize-tech-use-privacy

The Samara Centre for Democracy, Online Abuse in Local Elections: The SAMbot Municipal Report, (Toronto: The Samara Centre for Democracy, 2023), https://www.samaracentre.ca/articles/sam-botmunicipal-elections-report/.

Vipond, E., Saied, R., & Dietzel, C.(2025). *Navigating Digital Harms: An Investigation of Transphobic Online Hate Against 2SLGBTQIA+ Organizations.* Open Digital Literacy and Access Network (ODLAN) and Wisdom2Action. (pg 25)

A guide developed on Prince Edward Island / Epekwitk for understanding and reporting cyberviolence.

This digital self-defense toolkit empowers women and gender-diverse leaders with practical strategies, resources, and support to navigate and respond to digital threats.

If you are experiencing cyberviolence, or any form of tech-facilitated violence, you are not alone. Together we can work to make our internet and tech use safer for all.

You can download a pdf of this toolkit, available on our website:

PEI Coalition for Women's Leadership