Transgender Media Lab Safety Plan (Public)

Carleton University

Version 1.2. Last updated April 2, 2026.

Written by Aliisa Qureshi, Jada Gannon-Day, Laura Horak, Aaron Mauro, and Adam Milling

Acknowledgements: Edited by Kate Higginson. Layout and graphics by Kit Chokly. Ideation and conversations by Rina Khan, Orvis Starkweather, Kit Chokly, Maddie Murakami, Mel Racho, Imogen Frances, and Constance Crompton. Special thanks to Aaron Mauro and Rebecca Godderis for meeting with us and sharing your invaluable knowledge on safety and security.

Contact: laura.horak@carleton.ca

Summary of version changes

v1.1 Added people to acknowledgements and special thanks after getting their permission and added graphics.

v1.2 Added text to TMP layout, adjusted references and heading styles.

Table of Contents

How to cite this document:

The Transgender Media Lab, "Title, v.0.0" (Ottawa, ON: Transgender Media Lab, Carleton University, 2026).

What to Do in an Emergency

If you think you might be in immediate danger, your first lines of contact are:

At Carleton: Campus Safety Services Emergency Line: 613-520-4444 (ext. 4444 from any campus phone)

In the Lab Office: Campus Safety or the panic pendant. If you press the panic pendant in the lab office, it will send a notification to Campus Safety Services. They will call the office and/or come to the office in person.

Elsewhere in Canada and the US: 9-1-1

If you are not comfortable interacting with police or campus safety services: call a member of the Safety Working Group.

As soon as you are safe, please call or text the Safety Working Group.

In all other cases (e.g., if you feel uncomfortable or suspect a personal threat, a cybersecurity threat, or a threat at an event), call or text someone from the Safety Working Group. The Safety Working Group will help you and the team through the protocols outlined in this plan.

We recognize that for our communities, the police or campus safety officers may bring more danger than safety. Therefore, when possible, our first approach is always de-escalation.

Dealing with these kinds of things can be very stressful and bring up feelings of anxiety, embarrassment, and shame. For information on available options and support, see Appendix C Care Plan.

Notes:

- Even if you are not on campus or in Ottawa, Campus Safety Services can coordinate an investigation and connect you with relevant resources and authorities where you are. However, if they judge that there is an unmanageable risk to you or other people on campus, they may call Ottawa police even without your consent.
- If you can't speak freely, you can call Campus Safety and leave the line off the hook and they will come investigate. If you are using a cell phone to call, you will have to indicate verbally where you are so that they can find you.
- We recognize that for our communities, the police or campus safety officers may bring more danger than safety. An understanding of these complexities is foundational to how we approached this safety plan focused on safety, autonomy, and care.
- For secure communications use phone or Signal. The team communication platform is not recommended.

Contact Information

[Detailed redacted]

Transgender Media Lab

Safety Working Group

Name: Email:
Mobile Phone:

Name: Email:
Mobile Phone:

Name: Email:
Mobile Phone:

Carleton

Office of Risk Management: Coordinates Carleton's Response

Name: Email:
Mobile Phone:

Campus Safety Services

Name: Email:
Mobile Phone:

Information Security

Name: Email:
Mobile Phone:

Access to Information and Privacy Manager

Name: Email:
Mobile Phone:

General Counsel

Name:

Email:
Mobile Phone:

University Communications

Name:

Email:
Mobile Phone:

Name:

Email:
Mobile Phone:

Head of Film Studies

Name:

Email:
Mobile Phone:

Chair of the School for Studies in Art and Culture

Name:

Email:
Mobile Phone:

Dean of the Faculty of Arts and Social Sciences

Name:

Email:
Mobile Phone:

Other

Introduction

"Safety in dominant culture terms has almost always meant protecting the interests of the powerful and maintaining the status quo. As we advocate for safety, we need to ask ourselves, safety for who? What does safety really look like? A vibrant, life-giving queer and trans rights movement must define safety not as the absence of discomfort or even the absence of risk, but as the presence of our social values. That is to say, safety as freedom. Safety as care. And safety as solidarity across difference.

The culture in which we live has taught us that in order to be safe, we must exert our will over others, that the problems of social conflict and risk can only be solved through social control, the rule of law and order, discipline and punishment. The end goal of this securitarian logic is that we become numb to violence, oppression, and even atrocities so long as they are carried out in the name of safety.

What is a vision of safety that is creative, rather than destructive? That encourages rather than strangles life? That grows out of a politic not of control and policing but rather freedom, care, and solidarity? Who do we need to become to bring that world into being?

> Safety as freedom – *the freedom to be who we are and express our truths without the fear of being punished for it.*
>
> Safety as care – *knowing that we can turn to the people around us for help when we are hurt, harmed, or in need.*
>
> Safety as solidarity – *responding to fear and scarcity by banding together rather than turning against one another.*

When I dream of a radically safe future for queer and trans people, I dream of a strong web of community that is intentionally and purposefully connected to the world around it. We bind ourselves to one another because we know we need each other not only to survive, but to thrive. We have freed ourselves from the illusion that safety is about locking people away and are grounded in the truth that safety comes from giving people what they need. All we need to do is start practicing – to start embodying safety in shapes of freedom, care, and solidarity, bound together by love."

> — Kai Cheng Thom[1]

[1] Kai Cheng Thom. "We Are Not Safe Till We Are Free: Redreaming Queer & Trans Safety." Substack newsletter. Kai Cheng Thom (blog), September 20, 2024. https://kaichengthom.substack.com/p/we-are-not-safe-till-we-are-free.

As Thom writes, the dominant culture assumes that we must exchange freedom for safety. We are told we must sacrifice our values for solidarity and care to be secure in our person. The rule of law demands order through discipline and punishment. This coercive, often violent, social control is a securitarian logic that requires that we become numb to violence, oppression, and even atrocities in exchange for safety. Bodily autonomy and personal freedom are expressions of truth. Creative expression in art, writing, and action is also an expression of freedom that can demand safety or celebrate it. Security is an expression of values. Communities we belong to can be overlapping, heterogeneous, and sometimes in conflict. We belong to nations, cities, and organizations that overlap systems of care that include and exclude, but we must be able to demand equity in care at all levels.

The Transgender Media Lab (TML) was founded by Dr. Laura Horak in 2020 to create an institutional home for students recruited to research trans media-making and build the Transgender Media Portal (TMP), a website and database of trans+ and Two Spirit filmmakers and their works. The purpose of the TMP is to make audiovisual work by trans+, Two Spirit, nonbinary, intersex, and gender-nonconforming people more available to artists, activists, festival programmers, researchers, instructors, and the public. We hope to promote the careers of today's trans+ and Two Spirit filmmakers, call attention to older works so they can be programmed and preserved, jumpstart research on these films, and provide artists and others with access to an innovative tradition of work.

Our lab's core values are:

- Radical Honesty & Listening
- Community-Oriented and BIPOC Trans Centred
- Challenging Hierarchies
- Care Ethics

To see more about how we determined these values and how they shape our actions in the lab, see the Transgender Media Lab Handbook on our Policies page.

We are also working to create networks with other researchers and organizers who share our values so that we can contribute to each others' collective survival.

Given these values, we embrace Kai Cheng Thom's concept of safety as freedom, care, and solidarity. We reject surveillance and colonial, carceral solutions. We commit to working with staff at Carleton University and our community partners to keep ourselves, the people we work with, and the filmmakers featured in our Portal as safe as possible, without mistaking control and policing for safety. We will undoubtedly make mistakes. We commit to growing and learning from these mistakes. This plan is a living document, and we welcome feedback at transgendermediaportal@gmail.com.

Organization and Decision-Making

Here is how our lab is structured (as of March 11, 2026):

[Redacted image]

Image description: *A diagram of the TML's organizational structure. The Community Advisory Board is at the top. Then there are four overlapping teams: the Operations Team; Community Accountability, Research & Data Wrangling (CARD) Team; Design, Infrastructure & Systems (DSI) Team, and Safety Working Group.*

All safety-related incidents will be addressed by the lab's Safety Working Group (which includes the lab director) in collaboration with the person or people affected by the incident. In general, we will try to follow the lead of the affected people.

However, if the Safety Working Group judges that there is a continued threat to members or affiliates of our lab, they may choose to take additional action not directed by the affected people. We will do our best to avoid involving Campus Safety or police unless consented to by the affected people.

Likewise, if the affected person or the Safety Working Group contacts a Carleton staff member, that staff member and their team will work with us to decide on next steps together. However, you should know that if the staff member judges that that safety of the Carleton community is at risk (e.g. if there is an outstanding threat to Carleton students, weapons involved, or if you pose a risk to yourself or others), they may initiate additional action not directed by the affected people, such as contacting the police. We acknowledge that the police often pose more of a threat to our communities than anything else, and we have communicated this to the head of Carleton's Risk Management and Campus Safety Departments.

Confidentiality and Data Management

Investigation

During a Safety Incident investigation, members of the Safety Working Group may gather information from multiple computer systems and/or conduct interviews with relevant personnel. All information gathered or discovered during a Safety Incident will be **strictly confidential** throughout the investigative process. All members of the Safety Working Group are trained in information security and data privacy best practices. At the conclusion of the investigative process, the Director will brief the TML Operations Team on the relevant details of the incident and the investigation. A Post-Incident Review (PIR, see page 32 below) will be drafted by the Director and used to re-evaluate and revise this Integrated Safety Plan. During this phase, no confidential information will be shared unless it is strictly relevant to the investigation and/or the incident itself.

Affected Stakeholders

In the event the incident involves the unauthorized access or disclosure of confidential or sensitive information about lab members, affiliates, and/or filmmakers in the Portal, the Transgender Media Lab may communicate information relevant to the incident as well as any additional requested information to which they have a right (e.g. specific student records, staff records, etc.) to relevant Carleton University staff members. If the Transgender Media Lab is made aware of direct threats against lab members, affiliates, and/or filmmakers, the Director will inform those parties of the scope and substance of those threats through private communications, such as an email or telephone call. The Transgender Media Lab reserves the right to withhold certain information at the discretion of the Safety Working Group if that information may jeopardize current or future investigations or pose a security risk to the Transgender Media Lab or other entities.

In the event the incident is limited to Transgender Media Portal systems not containing confidential or sensitive information, it will be at the discretion of the Safety Working Group whether to share information related to the incident with outside stakeholders.

Communication Guidelines

Initial communication to any affected stakeholders should occur as expeditiously as possible upon the identification of the incident. This communication should be from official Transgender Media Lab or Carleton University communication channels. In some cases, this may include an initial communication (letter, email, phone call) that simply states that the Transgender Media Lab is aware of the issue and is addressing it, with the promise of a follow up.

Communication with news media will be initiated by Carleton University's Department of University Communications and/or the lab's director. Incoming news media calls and requests for information will be directed to the lab director or a designee. A communication response plan (talking points, interview refusal statement, etc.) will be formulated as needed.

How to De-Escalate

Because our communities can't count on Campus Safety or the police to keep us safe, we do our best to keep ourselves safe. One of our most important tools to accomplish this is de-escalation. The tools of de-escalation can serve us in matters small and large, from an internal disagreement to an uncomfortable confrontation with hostile members of the public. If you're on the spot, don't hesitate to grab a lab member for help. See Event Safety for how to plan in advance for these types of situations.

We are building on the teachings of a long line of social justice activists before us. This guide draws on Rebecca Godderis's training, Neighborhood Anarchist's Deescalation Skills & Mindset handout, and the Direct Action Movement's De-Escalation Skills and Tactics.

Be aware of what things make you feel more stressed. If you find yourself in a situation where you don't feel comfortable, be quick to ask for help from someone else.

One of the best gifts you can give is to hold space for someone, to listen compassionately, and to bear witness. When someone shares with you something intense from their lives, validate their experience. You can say "That must have been really difficult for you" or "Thank you so much for telling me." People don't need solutions or answers as much as compassion.

Be sincere, respectful, and honest. Respect breeds respect.

Have confidence in yourself. You will not always say the "right" thing. People can feel if you are interacting with kindness and respect and their connection with you will grow. Rapport is organic and is nurtured in every moment. People are going to remember how you make them feel, not what you say.

These are the principles of a community predicated on care:

- Be empathetic and non-judgemental.
- Respect personal space.
- Use non-threatening nonverbals (gestures, facial expressions, movements, and tone of voice).
- Remain calm, rational, and professional.
- Focus on feelings.
- Redirect confrontational messages.
- Set boundaries.
- Allow time for decisions.

The following strategies can be used when attending events or managing public confrontations:

- Practice with Role Play: Run a few test scenarios with event organizers to be prepared and resolve any issues in the protocol flow.
- Eye Contact: Maintain regular eye contact with event organizers or eyes on group messages to be aware of any potential situations arising.
- Pre-Established Signal: Establish a known non-verbal signal, spoken signal, and message signal that can be communicated to begin a protocol for de-escalation. For example, have a specific non-verbal signal to call for backup or support that will enter de-escalation if you are overwhelmed, and have another signal to begin emergency procedure to leave a bad situation.
- Rely on Code of Conduct: When speaking to a threat actor, calmly enforce event rules or code of conduct and ask them to leave if necessary.
- Attempt De-escalation: to have them lower their voice, stop disrupting, acknowledging concerns if appropriate.
- Offer Options to Threat Actor: participate in the event calmly, talk to event organizers calmly after the event, leave written feedback, or leave.
- Stay United: Maintain a unified and non confrontational approach, avoid overlapping speech at the disruptor.
- Divide Roles: One person leads communication with the disruptor(s), another monitors the physical safety, the crowd, etc.

After the incident is over:

- Document the situation. Capture the date and time and describe the facts of the incident in a digital document with a version history, such as iOS Notes, Google Docs, or similar. Have a witness corroborate your documentation, if speaking to the police might be necessary.
- It's normal to feel a lot of hard emotions and physical reactions after the incident is over, sometimes hours or days later. Check out Appendix C. Care Plan for strategies on how to respond to these reactions.

Procedures for Different Types of Attack

Attacks on Personal Safety

We recognize that trans artists, researchers, activists, and everyday trans people are too often subjected to harassment and attacks from individuals, politicians, police, and immigration enforcement officers.

This section outlines the kinds of attacks commonly leveled against trans people, how we try to prevent them, and what we do in case an attack occurs.

Introduction: Common Types of Attack

Attacks on personal safety can include threats to physical safety, mental health, reputation, and damage to places and things. According to the research, common incident types include:

1) Malicious Speech

- Disinformation from media and politicians
- Transphobic and sexist social media harassment
- Fraudulent Freedom of Information requests
- Complaints about the project to the school president and provost and to the project funder
- ate mail
- False claims about groups or individuals
- “Canceling” by starting mass public shaming campaigns directed at us as individuals or as a group
- Email and social media contact (team accounts, personal accounts): These may include threats, insults, or disturbing images.
- Publishing names, faces, addresses on media without consent (“doxing”)
- Reporting us to police for "child grooming" or other bogus accusations
- Targeting team members' other projects
- Writing to institutions we’re affiliated with, defaming us
- Threatening lawsuits against us
- Weaponizing social justice and anti-oppression movements to launch targeted attacks (i.e., targeting pro-Palestine team members with accusations of antisemitism)
- Misrepresenting the site as “grooming” children into the “transgender lifestyle”
- Pressuring SSHRC or other project funders to reduce funding for projects like these
- Wide-reaching Gamergate-style attacks from people who might not have a strong ideological drive but want to cause chaos

- Revenge porn, sextortion, claiming to have accessed a target's web camera without their knowledge, threatening to release embarrassing images and personal information if instructions are not followed.

2) Threat of physical harm

- Doxing: tracking down and sharing private information, including phone numbers and home addresses
- Showing up at home, office, or places of work
    - stalking
    - yelling
    - threatening
- injuring (ranges from pushing & punching to attacks with knives or guns)
- Bomb or Bomb threat
- Swatting and fake “wellness checks”: falsely reporting a threat such as a bomb threat, mass shooting, domestic violence, murder, hostage situation, or mental health situation to instigate a dangerous and potentially violent response from emergency services
- Surveillance to stalk, follow, and/or monitor individuals.
- Spyware and stalkerware, including sophisticated programs like Pegasus
- Location tracking: AirTags, Find My, location tagged photos/videos, reverse image search, and Google Reviews are all capable of leaking your location in real-time or near real-time
- Unwanted touching, threats of sexual violence, and sexual harassment (eg. repeated and/or unwanted questions about genitals).

3) Destroying or stealing money, equipment, information

- Ransack lab office, director’s office, any other team members' offices
- Use HR info to steal our identities or to steal money from us
- Infiltrating our systems, collections, to cause chaos or gather intelligence for fascist groups
- Hack and leak our shared file storage and publish everything to defame us, the lab, & Carleton
- See cybersecurity policy for more on stealing passwords, data, etc.

4) Other

- Targeting by state-level threat actors (politicians, police, secret police, etc.)[2]

[2] Florida governor Ron DeSantis has banned textbooks, dictionaries, and lecture topics from Florida public schools and universities due to their content on race and gender. Provinces like Saskatchewan and Alberta have also introduced anti-trans policies over the past year (Long, 2024; Amnesty International, 2024).

- State-level threat actors using information from the Portal to target trans people in their areas
- Infiltrating our networks and platforms to cause chaos, distrust, and discord within our community or gather intelligence for fascist groups[3]

These different categories are porous and can lead to each other. For example, malicious speech online can lead another person to publicize our addresses and yet another person showing up at our home or office and physically harming us. And threats of physical harm have mental health repercussions even if the threat is not carried out.

For more information on the types of attacks trans activists in Canada regularly experience, see JusticeTrans's "Understanding & Fighting Back against the Anti-Trans Movement in 'Canada'" in Appendix G.

Prevention

How to prevent attacks on personal safety? Being visible as a trans project is essential for achieving the project's goals–celebrating and circulating trans-made films. However, visibility also puts one at risk. In many cases, threat actors do not need to have any information beyond what is publicly available to carry out threats: e.g., the names of people in the lab, lab affiliates, and filmmakers in the Portal; our affiliated institution; the lab's email address and social media handles; and filmmakers' social media handles. Other threats require additional information such as team members' personal email addresses and social media handles.

Only a few threats require confidential information such as home and office addresses and passwords. While we try to keep confidential, sensitive, and internal data safe to prevent those types of threats, we cannot prevent the threats that only rely on public information. All we can do is prepare to respond quickly and effectively.

To prevent incidents, all members of the lab are required to follow the Zebra Crossing digital safety checklist Levels 1 and 2. Members will use multi-factor authentication (MFA) for all accounts, where available. See Attacks on Cybersecurity for more information on digital safety.

In our grants, we will budget for mental health support and adequate time off for researchers in the lab. We oppose casualization by creating jobs that pay fairly.

[3] See, for example, Cervini, Eric. Spying Before Stonewall: How the FBI Secretly Tracked Gay Activists in the 60s. June 8, 2020. https://www.vice.com/en/article/the-fbi-secretly-tracked-gay-activists-in-the-60s/; 1. "Ghetto Informant Program," Wikipedia, July 5, 2025, https://en.wikipedia.org/w/index.php?title=Ghetto_Informant_Program&oldid=1298852561.

Before doing anything that we garner publicity for the project, we will:

- Brief our chair, dean, Coms, and the office of risk management to explain why we are at risk and to prepare them for any complaints.
- Notify our partner organizations and build a coalition of authoritative public facing institutions to build resiliency.
- Work with University Communications to prepare press statements designed to anticipate and counter disinformation. We will create a simple key message, written for those who care about the topic and are interested.
- Develop a response plan with pre-prepared press statements in the event of a hostile response that features disinformation, false claims, or defamation.

Detection

In many cases the threats will be easy to detect, such as if a person sends us an email or shows up at our door. However, sometimes the threats will not present themselves so blatantly.

How we identify more subtle threats:

- Use Google Alerts on the name of the lab, the portal, the names of the lab members, as well as “trans” + Ottawa and “trans” + Carleton.
- Before public events and launches, have lab members review rightwing forums looking for evidence that the lab/portal will be targeted. (See Event Planning protocol for more on this.)
- Stay up to date on anti-trans movements and movement actors in Ottawa, Ontario, Canada, and North America. Save documentation in a separate encrypted folder in our shared file storage. Print web pages to PDF to include date and time.
- Recommend that team members check bank accounts and credit card statements every month for unusual activity.

More information about what to do if you have a compromised device or account can be found in the Care Plan.

Assessment

Once threatening activity has been detected, the lab’s Safety Working Group will work with the person affected by the threat to collaboratively decide on next steps.

The first step is to determine the **level of intervention** required.

Considerations

- **Likelihood:** What is the likelihood that the threat will take place?
    - **Unlikely:** little precedent and few favourable conditions to facilitate them
    - **Likely:** clear precedents and/or favourable conditions to facilitate them
    - **Unclear:** low information masks potential threat, but it remains important to err on the side of caution
- **Impact:** What is the potential impact of a harmful event?
    - How **many people** are affected?
    - How **long-lasting** is the effect?
- What other harmful situations does it **enable**?
    - Is there **danger to others**, who may not be directly targeted?
- **Adversary:** Identify the person/organization/entity behind the threat. Consider their capabilities, their limitations, and their history of past hostile actions.
- **Target:** identify all potential targets of the threat, including information, systems, and people. Consider physical, emotional, and financial harms as well as harms against reputations.
- **Resources:** What resources and information is needed to carry out an attack? Where might they get this information?
- **Opportunity and ability:** Where and when might the attack take place?

Response (See also Care Plan)

In the case of an incident, responses to many different aspects of the incident's impact will need to be considered. These include:

1. Physical safety
2. Mental health
3. Reputational harm
4. Damage to things
5. Accountability/restorative justice for the person doing the harm (when possible)
6. Prevention of further harm (when possible)

The Safety Working Group and affected person will work together to determine the most appropriate response. We will take care to ensure that mental health support is available to all lab members affected by the incident. (We recommend that the affected person review the Care Plan, which explains resources for trauma-informed support.) We will also determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so.

Initial Response

If there is an imminent physical threat, the affected person (or people) should call Campus Security (if on campus) or 911 (if off campus) or a trusted friend or family member.

If there is malicious speech addressed to an institutional or personal social media account, that account and all related accounts should immediately be made private. (See Appendix E)

Throughout this process, it will be critical to preserve all possible evidence and document all measures taken in detail. These reports should be saved in an encrypted file only accessible to the Safety Working Group.

Remediation and Recovery

Once the cause has been determined, the Safety Working Group will work to address harm caused and prevent future harm. (Again the affected individual should see the Care Plan for how to take care of themselves and heal from the incident.)

Potential actions include:

- Report incident to:
    - 9-1-1
    - Ottawa Police
    - Ontario Provincial Police
    - Federal Cyber Centre: https://www.cyber.gc.ca/en/incident-management
    - Carleton Campus Safety
    - Carleton Risk Management
    - Carleton ITS Security
    - Carleton Equity and Inclusive Communities
    - Carleton FASS Dean
    - Carleton's General Counsel and/or Access to Information and Privacy Manager
    - Social media platform (e.g. Facebook, Instagram, Bluesky)
- Track how the incident evolves.
- Set social media accounts to private (See Carleton's Guidelines to Social Media.)
- Block offending account(s).
- De-escalate. (See How to De-Escalate.)
- No response.
- Work with the Department of University Communication to:
    - Write up a statement and release it strategically on our social media and email listserv (e.g. on LinkedIn, not X).
    - Create a press release and send it to the media.
    - Monitor social media commentary.

    - Monitor email inboxes.
    - Remove contact information from all university websites.
    - Filter media requests.
- Work with University Safety to monitor on-campus offices around key dates.

Documentation

Regardless of whether it is determined there is a security threat, the Safety Working Group will accurately document the scenario in a Security Incident Log, which is saved in an encrypted file only accessible to the Safety Working Group. All Security Incident Logs will be stored in a single location so incident information may be reviewed in the future.

This report should contain information such as:

- Who reported the incident
- Characteristics of the activity
- Date and time the potential incident was detected
- Nature of the incident
- Potential scope of impact

See Appendices for Incident Log and Incident Report Templates.

Attacks on Cybersecurity

Cybersecurity is a team sport. We all have a role in maintaining the security of our research data, infrastructure, and associated information. As our lab's central project is a website and we host many of our lab's files online and on our personal computers, we are vulnerable to cybersecurity attacks.

Our Cybersecurity plan is based on the NIST Cybersecurity Framework (see Further Reading). Carleton University ITS has not given us permission to use their processes and forms directly. However, we have access via the AVRC CSU (computing services unit), so we are aligned and in liaison with Carleton ITS processes.

Introduction: Common Types of Attack

Types of cyber incidents that may threaten the organization are:

- Unauthorized attempts to gain access to a computer, system or the data within
- Service disruption, including Denial of Service (DoS) attack
- Unauthorized access to critical infrastructure such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malware
- Non-compliance with security or privacy protocols
- Data theft, manipulation, alteration, or corruption (including misgendering and misnaming filmmakers in the Portal)
- Unauthorized distribution of data, including doxing attack
- Phishing, baiting, and other forms of social engineering attacks on users or participants
- Theft of passwords to break into team or personal accounts, enabling not just data theft but the potential to steal identities and funds

Prevention

To prevent incidents, all members of the lab are required to follow the Zebra Crossing digital safety checklist Levels 1 and 2.

Members will pay special attention to the following requirements:

- All members will use multi-factor authentication (MFA) on all accounts, when available.

- All members will use unique passphrases for each account used in the course of research activities.[4]
- All lab passwords will be stored on the team's password manager.
- All lab members are *strongly* recommended to use password managers for their personal accounts as well, including their personal email accounts
- Lab members will not use the communication platform desktop app, but instead access it on their web browser.
- Members will check https://haveibeenpwned.com once per semester to determine whether their accounts and/or passwords have appeared in data breaches.
- Remote Desktop Protocol (Microsoft RDP) may never be used by members.

The team will decide on a pre-arranged code, signal, or phrase to communicate a compromised device or account without alerting the attacker. Examples of simple signal phrases could be "_____" or incorporating a specific emoji into a message.

Crossing Borders

When travelling to hostile legal jurisdictions such as the United States, members will limit access to research materials on digital devices. Because normal legal rights are suspended in border crossings, it is reasonable to expect search and seizure of mobile devices, laptop computers, and mobile devices. Research files and member contacts should not be stored on devices as static files during travel. Research materials should be accessed remotely during travel, using standard secure authentication methods. Border agents cannot compel individuals to log into services, so members must log out of all online services on a laptop. Removable media, such as a harddrive or flashdrive (USB key), should be encrypted or simply not taken on trips to hostile jurisdictions. Mobile devices should be in "lock down" mode and locked with bio-authentication systems. See the following documentation for locking down your devices for Android or iOS. Devices should remain password protected, encrypted, and in "lock down" for the duration of your visit.

Protecting the Server

Our service provider, _____, recommends enabling additional logging, automated server backups, and Fail2Ban, as well as setting up a firewall. Based on our project's specific needs, we have set up a firewall and also turned off password access to the server.

[4] Communications Security Establishment Canada. "Best Practices for Passphrases and Passwords (ITSAP.30.032)." Canadian Centre for Cyber Security, September 17, 2019. https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032.

Detection and Assessment

All team members, regardless of their duties, should be on the lookout for the following symptoms on their personal computers and the lab's servers.

Signs a computer may have been compromised include:

- Abnormal response time or non-responsiveness
- Unexplained lockouts, content, or activity
- Locally hosted websites won't open or display inappropriate content or unauthorized changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Settings changes
- Data appears missing or changed
- Unusual behavior or activity by staff, students, partners or other actors
- Unprompted authentication requests through MFA, either in app, text, or email notifications

Signs a cell phone may have been compromised include:

- An attacker's access to the device
- Strange activity on the device including a rapid change in battery life
- Consistently dropped calls
- The phone shutting down
- References to personal information like text messages, files, and photos

If you receive an email that seems to be from one of your own accounts, you can check whether it is real by clicking into your "Sent" and "Trash" email folders on the targeted account to determine whether the email was sent from your account. If the email is not in your folders, the attacker is likely not in your account but has instead mirrored the account to make it look like they are in your account. Do not click any links in the email or respond.

The project Web Developer will maintain current logs and backups of all server content and activity for one year at minimum. These logs and backups will be used to verify a breach, respond to an active attack, evict attackers, and restore damaged systems.

Once anomalous activity has been reported, it is incumbent upon the Safety Working Group to determine the level of intervention required. Other members of the Safety Working Group may be required to provide input during this phase to help determine if an actual security threat exists. If it is determined there is an active security threat or evidence of an earlier intrusion,

the Director will alert the entire Safety Working Group immediately so that the situation may be dealt with as expeditiously as possible.

Security Incident Reporting

If you witness suspicious activity or behaviour on your personal or lab computer or software, please report a security incident to the Safety Working Group as soon as possible.

In an email addressed to the SWG members, answer the following questions to the best of your ability:

- What are the symptoms?
    - Describe software behaviour and potential causes with screenshots, if possible.
- What is the time and date of the suspicious behaviour?
    - Providing specific dates and times will assist in assessing log data.
- What software is your computer running?
    - List your operating system, browser, browser extensions, and other software and settings. Please include software version numbers if possible.
    - What may be the cause?
- What project systems have been/are being/will be impacted?
    - Consider digital assets such as our shared file storage, our server, our Git repository, our listserv, and all associated hardware. How widespread is it?
- Which project stakeholders are affected?
    - Please include contact information, if possible.

Response

Upon determining that a significant incident or breach has occurred, the Safety Working Group will notify Carleton ITS Security and server provider immediately. As additional information is uncovered throughout the investigation, the Safety Working Group will brief Carleton ITS Security and server provider so appropriate decisions, such as allocating additional staff, hiring outside consultants, and involving law enforcement can be made. Additionally, based on the incident, it will be incumbent on Carleton ITS Security and Carleton's Access to Information and Privacy Manager to determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so.

The Lab Director will document all interactions with internal and external partners to develop a timeline of events for the PIR process to follow.

Carleton staff should take into consideration the nature of the information or systems involved, the scope of the parties affected, timeliness, potential law enforcement interests, applicable laws and the communication requirements of all parties involved.

Compromised Personal Device

If you suspect one of your personal devices may have been compromised:

- Some steps taken to secure an account might notify an attacker that you have made changes to your account or device, such as removing a phone number or adding two-factor authentication to the compromised account/device. Before making changes, evaluate whether these changes might alert the attacker. If you anticipate retaliation, prioritize physical safety first and seek support.
- Use an alternate device, friend's phone, or a secure account to contact support, avoiding direct actions on compromised accounts.
- If you must use the compromised device, use a prearranged code, signal, phrase, or emoji to alert the Safety Working Group.
- Amnesty International offers tools and guides to determine whether your device has been compromised.
- The best way to preserve the phone as evidence is to put the device into airplane mode and keep it charged without using it.
- Going to the police can be challenging and is not the best option for every person being targeted. If you decide that this is not the best option, factory resetting the phone can remove some spyware.
- To replace the device – the safest option – contact your local Victim Services, Sexual Assault Centre, or another relevant social service agency to determine whether they have emergency device funds.

If you are concerned that stalkerware or another digital technology has been targeted at you as a form of intimate partner violence, stalking, or sexual harassment, please see the Coalition Against Cyberstalking's Resource List, the Clinic to End Tech Abuse's Get Help, and Lila.Help's list of resources for victims of domestic violence by region.

Initial Response

The first steps in any cyber incident response should be to determine the origin of the incident and isolate the issue. This may involve the immediate disconnection of workstations, servers, or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs, as well as possibly perform vulnerability scans, to ensure the incident has not spread to other areas in order to define the entire scope of the incident.

The TML Web Developer will work to:

- gain immediate access to affected systems and force all authenticated accounts to perform a password reset, using passphrases and MFA procedures;
- gain immediate access to system logs and download them to an unaffected system;
- immediately ensure the safety of all system backups and ensure they are stored on an unaffected system.

Throughout this process, it will be critical to preserve all possible evidence and document all measures taken in detail. Thorough review and reporting on the incident will be required once the threat has been removed, the vulnerabilities have been removed and the systems have been restored.

Please note, if affected systems include typical communications channels like email, the Safety Working Group will update all team members on alternate, safe communications during this time. Upon resumption of normal activities, the Safety Working Group will provide guidance regarding secure communications.

Remediation and Recovery

Once the cause has been determined and appropriately isolated, an ad hoc **Remediation and Recovery Team** will need to remove the vulnerabilities leading to the incident. This team will likely consist of the TML Web Developer, members of the DSI Team, and members of Carleton's Information Technology Services team.

The team's work may involve some or all of the following:

- Install patches and updates on systems, routers, and firewalls
- Infections cleaned and removed
- Re-image or re-install operating systems of infected machines
- Change appropriate passwords
- Conduct a vulnerability scan of any compromised machines before reconnecting them to the network
- Restore system backups where possible
- Document all recovery procedures performed and submit them to the Director
- Closely monitor the systems once reconnected to the network

Documentation

Regardless of whether it is determined there is a security threat, the Remediation and Recovery Team will accurately document the scenario in a Security Incident Log. All Security

Incident Logs will be stored together, with separate backups, so incident information may be reviewed in the future.

This report should contain information such as:

- Names and contact information for all team members
- Security Incident Report (above)
- Detail all the remediation and recovery steps
- Incident Status (active, closed, monitoring)

See the Appendices for the Incident Log and Incident Report Templates.

Technical Incident Protocol

This Technical Incident Protocol gives the practical steps to follow the Cybersecurity Incident Response Plan as described earlier in this document: Identify > Detect > Respond > Report > Review.

1. Emergency Preparation
    a. Currently, the primary lead for technical incidents is the TML Web Developer.
    b. If the primary lead is not available, another primary lead will be arranged and notified.
    c. For secure communications use phone or Signal. The team communication platform is not recommended.
2. Emergency
    a. In the case of an active and ongoing emergency, contact the primary technical lead. Keep trying to contact members of the Safety Working Group until a response is received.
    b. If not already done, the lead notifies the DSI Team that an emergency is in progress.
    c. The lead deals with the emergency, getting help as needed including from Carleton ITS and the server service provider. The technical lead updates the Safety and DSI Teams as needed.
3. Logging
    a. Log the incident on _____.
    b. Create an entry in the Incident Log.
    c. If the incident needs to be tracked for follow up actions, then also create a related task in the tracking system, which is the Strategic Action Plans at the top of the Safety Working Group Agenda + Minutes.
    d. The Strategic Action Plans also contains the current list of all security tasks that require follow up.

4. Reporting
    a. If the incident requires a report, create an incident report document from the template. Use the same file name convention as other documents in the folder.
    b. Turn on document history to track changes in the document (auditing).
5. Review
    a. At every meeting of the Safety Working Group, all open incidents are reviewed as part of the standing agenda. This meeting must occur at least once every three months.

Event Safety

Unfortunately, anti-trans actors often use public events, both online and in person, to attack trans people and organizations. We prepare for these kinds of attacks in advance so that we know what to do if something happens. We can keep our lab members, invited guests, and attendees as safe as possible by following these guidelines.

Introduction: Common Types of Attack on Event Safety

Common types of incidents that threaten participant safety include:

At In-Person Events

- Filming/recording the event for public shaming
- Counter-demonstration: threats, physical violence, loud music, preventing people from entering/leaving
- Audience member(s) disrupting event: yelling, threatening, making a scene, offensive actions, harassing
- Bomb threats or attack, mass shooting
- Physical damage or threat to the event space
- Venue disruptions, fraudulent or real: canceling the event or changing location last minute to sabotage or prevent large attendance
- Intimidation: pressuring event partners/host/conference organizers to defame the TML and its members or remove TML or its members from event
- Someone is upset or triggered by the content
- Someone asks an inappropriate question in Q&A
- Escalated individuals who are not registered
- Escalated individuals in Q&A
- Sexual harassment

At Online Events

- Filming/recording the event for public shaming
- Recording attendees' names for malicious purposes
- Zoombombing: disrupting, yelling, threatening, offensive actions, harassing, broadcasting offensive images and videos
- Host disruptions, fraudulent or real: canceling or interrupting the event
- Intimidation: pressuring event partners/host/conference organizers to defame the TML and its members or remove TML or its members from event
- Someone is upset or triggered by the content
- Someone asking an inappropriate question in Q&A

- Escalated individuals who are not registered; yelling
- Escalated individuals in Q&A

Prevention (See also Event Planning Checklist)

To avoid incidents, safety planning is integrated in all steps of event planning from development to coordination to execution.

We plan our events with attention to the following:

- Environmental Scanning
    - Content: Are the guests or topic considered 'controversial'?
    - Location: Are there anti- rallies happening in the locale?
    - Environment: Have there been incidents at other similar events locally or currently? What safety lessons can we implement from them?
    - Overall: What is the level or perceived risk and concerns, and how can we increase safety?
- Selecting a Venue
    - Do you have the right to ask people to leave? Can anyone come in? Is there open access to the building or room?
    - Choose venues with multiple exit routes.
    - Be aware of their security options and connect with on-site security.
    - Choose spaces with accessible exit plans and safety plans.
    - Is it an evening or day event, and how far is parking/public transportation - considering safety of people arriving and leaving the event.
- Planning with Guest Speakers and Co-Organizers
    - Ask them about their security and safety concerns, needs, past experiences, and what we can generally do to make them feel safe.
    - Inform them of safety plans so they are not panicked or lost.
    - What is their comfort level in Q&A panels? Are there questions they will not respond to? Do they want a facilitator to respond to those questions and to disruptors?
    - Have your questions peer reviewed.
- Examining the Role of Law Enforcement Services
    - Have explicit discussions prior to an event on the role and need for law enforcement services: understand what actions various law enforcement services are authorized to take that the event organizers would be unable to act on their own (e.g. escorting people out of the venue).

        - If you decide that security/police have a role, have a clear plan to keep people who are typically targeted by security/police feeling safe and comfortable.
        - The event organizers should be knowledgeable on their rights as well as the rights and limits of law enforcement services they choose to include.
    - Identify the Emergency Contact Protocol of who will be called and when, by whom, and in what order. Prior to the event, assign day-of roles. Have this readily available and downloaded offline for the event organizers during events.
    - Options: Campus Security, Police/911, venue security, trained personnel, other backup contacts/ideas?
- Assigning Day of Roles to Organizers
    - **Facilitator:** Primary speaker who actively guides the audience through the event, mediating and engaging with both audience and special guests. They would maintain control of the event while de-escalation is taking place, or perform de-escalation techniques themselves.
    - **Co-Host:** Supporting the Facilitator, the Co-Host may also speak to, mediate and guide audiences and special guests, and support by beginning de-escalation or maintaining control of the room during de-escalation.
    - **Security Monitor:** A person who is positioned with a clear view of the activity in the event room and doorways, with easy access to act and signal other organizers. They would try de-escalation techniques off the stage, so that the Facilitator can focus on regaining control of the room.
    - **Guest Liaison:** The main point of contact for artists and special guests when they arrive at the venue. They will let guest speakers know where they need to be, where exit routes are, and will communicate directly with and escort guests during an emergency.
    - **Peer Support:** Someone available to provide help, guidance, and emotional support in the event of a crisis.
    - **Medic/First Aid Liaison:** Someone equipped for emergency physical care and/or the first person to contact ambulances and other emergency health services. This is important to assign to avoid multiple or delayed calls to emergency services in the event of a crisis.
- Special Considerations for In-Person Events
    - Create registration for the event.
    - Limit disclosure of the time and location of the event (registrants only, days before event, etc).
    - Screen audience questions and participation through mediation, submitted written questions/Slido/QR code, etc.

    - Take a headcount at the beginning and occasionally to be aware of changes. If there is a registration list can confirm with the number registered.
    - Maintain communications in event organizers group messaging so that the team is all aware of potential threats and we have documentation.
- Special Considerations for Online Events
    - Create registration for the event.
    - Create a passcode, waiting room, or other form of authorization to control event access.
    - Limit disclosure of the time and location of the event (registrants only, passcode day of event or days before event, etc).
    - Limit video and audio controls for participants when appropriate.
    - Turn off general chat.
    - Screen audience questions and participation through mediation, submitted written questions/Slido/QR code, etc.
    - Maintain communications in event organizers' group messaging so that the team is all aware of potential threats and we have documentation.

When to Cancel the Event

Throughout the event planning process, should the likelihood of threats to physical or emotional safety appear extremely high, cancel the event before an incident occurs. It is never too late to cancel or adjust logistics of an event in the interest of safety.

Detection and Assessment

All lab members involved in an event will be on the lookout for any possible incident. In addition, we may assign additional Safety Monitors to the job of keeping an eye out for safety incidents. In many cases, it will be obvious when an incident has started. Review the Common Types of Attacks to be aware of common suspicious behaviours.

Response

Our main priority with any incident is to de-escalate the situation and to keep organizers, guests, and attendees safe from harm. After the incident, we recommend that all affected people consult our Care Plan.

The first step is always to **assess the severity of the disruption/threat.**

For In-Person Events

If the incident is something that the event organizers CAN handle, we will proceed into the De-Escalation Protocol:

- Calmly announce we are going to use a security protocol and begin.
- Lock the venue so no new people can enter.
- Begin de-escalation:
    - Stage Area: If the disruption is near the stage, the Facilitator may initiate de-escalation.
    - Other Areas: In other cases, the Security Monitor will begin de-escalation. If backup is needed, Peer Support or another designated person will assist with de-escalation. The remaining event organizers should monitor the situation without overlapping voices to avoid distracting the disruptor from the de-escalation process.
    - De-escalation: calmly enforce event rules and code of conduct (disruptors will be asked to leave).
    - Security Monitor or Facilitator (whichever is not engaged), Co-Host, Peer Support and Medic on standby to engage Emergency Contact Protocol.
    - If a minor interruption, offer options to the disruptor(s): participate in the event calmly, talk to event organizers calmly after the event, leave written feedback, or leave peacefully.
    - If uncooperative, offer to escort disruptors out of the venue peacefully. Avoid touching to prioritize safety.
    - If a major interruption or situation becomes hostile, signal/announce and initiate Emergency Contact Protocol.
- Proceed to Remediation and Recovery Step 1.

If the incident is something that the event organizers CANNOT handle or regain control from, we will proceed to the Event Ending Protocol:

- Calmly announce the event will be ended to prioritize everyone's safety and comfort.
- Announce emergency protocols have been engaged: initiate Emergency Contact Protocol.
- Depending on the situation, Facilitator asks everyone to remain seated or guides attendees toward the exits in a safe and orderly fashion. Guest Liaison relays the emergency to guests and directs guests to remain seated or exit safely. Encourage everyone to remain calm and avoid rush or panic. Ensure vulnerable individuals are taken care of by the Co-Host, Security Monitor, or Peer Support.

- Take headcount before and after evacuating to see if everyone has been safely evacuated.
- Proceed to Remediation and Recovery Step 3.

For Online Events

If the incident is something that the event organizers CAN handle…

- Calmly announce we are going to use a security protocol and begin.
- Host/Co-host: Go to Host tools -> Suspend participant activities. This turns off and locks all mics & videos and also automatically locks the meeting so no new people can join.
- Begin De-escalation:
    - Calmly enforce event rules and code of conduct (disruptors will be asked to leave)..
    - If a minor interruption, offer options to the disruptor(s): participate in the event calmly, talk to event organizers calmly after the event, leave written feedback, or leave peacefully.
    - If a major interruption, remove/kick the disruptor(s).
- Proceed to Remediation and Recovery Step 1.

If the incident is something that the event organizers CANNOT handle or regain control from…

- Calmly announce the event will be shut down to prioritize everyone's safety and comfort and then end the meeting for all.
- Proceed to Remediation and Recovery Step 3.
- Lab director to formulate a plan to release an update on the situation, or respond accordingly.

For Online Lab Meetings

If the incident is something that the event organizers CANNOT handle or regain control from…

- Immediately shut down the Zoom meeting and regroup on our communication platform.
- Proceed to Remediation and Recovery Step 1.

Emergency Contact Protocol

Establish clear procedures for determining who will contact emergency services, when to do so, who will make the call, and in what order.

For example:

Initiating Emergency Contact Protocol: Use a distinct non-verbal, verbal, or written signal to activate the emergency protocol, separate from regular incident procedures. The Facilitator will signal to the event organizers and announce the activation of emergency protocols. They should maintain a calm demeanor to help keep the room orderly, continuing to facilitate or act as a point of contact for questions.

Contacting Emergency Services:

- If de-escalation by Facilitator or Security Monitor fails or the situation escalates into a greater safety threat, the Security Monitor (1), Co-Host (2), Peer Support (3), or First Aid/Medical Liaison (4) —whichever is least preoccupied, in the safest position, and least vulnerable to police violence—will contact the designated security contact or law enforcement and relay messages.
- For health emergencies, the Medic/First Aid Liaison will call 911 and relay messages. If no Medic/First Aid is available, the Peer Support, Security Monitor, or Co-Host —whichever is least preoccupied, in the safest position, and least vulnerable to police violence—will cover this role.
- For mental health emergencies, Peer Support will be on-site in a known location, clearly identified by a tag or sign. They will decide whether to call the appropriate emergency service or 911 and will have themselves or someone in the best position make the call and relay messages. If no Peer Support is available, the Medic, Security Monitor, or Co-Host —whichever is least preoccupied, in the safest position, and least vulnerable to police violence— will cover this role.

Communication:

- Always notify the group if someone has contacted emergency services, especially if the call was made by someone outside of the event organizers.

Remediation and Recovery

Once the incident has been de-escalated and order restored:

Step 1: Check in with the remaining participants and discuss whether the event can continue.

Step 2: Inform and direct participants to the appropriate channels if they need or want support following the incident.

Outcome #1: Continue the event.

Outcome #2: End the event in a calm and organized fashion.

Step 3: The event organizers regroup as soon and safely as possible in order to document the Incident Report accurately and to begin facilitating support for the team/affected individuals.

Step 4: Lab Director determines the appropriate public communication and formulates a plan to engage with University Communications, release an update on the situation, or respond accordingly.

Documentation

After the incident has been addressed and the event has concluded, the event organizers will gather all available information to create a comprehensive and accurate summary using the Incident Report Template. During this reporting process, we prioritize minimizing further harm and ensuring the care and wellbeing of those affected. This report serves as a record for the protection of those impacted, and we recommend including a witness to attest to the account.

Report Contents

The Incident Report Template will include all pertinent information to the incident, but at minimum we will document the following:

- Date, time, location of incident
- Description of the incident
- Description of actions taken
- Involved parties
- Witness information
- Reflection and follow up (to be completed in the next Review step)

Post-Incident Report and Review

Once the threat has been mitigated and normal operation is restored, the Safety Working Group will compile all available information to produce an accurate and in-depth summary of the incident in an **Incident Summary Report (ISR)**. Throughout the incident, the Safety Working Group will have kept Incident Logs that contain detailed records wherever possible, and these shall serve as the basis of the report. Interviews will also be conducted with appropriate members of the Safety Working Group to obtain any additional information that may be available to augment the logs and records kept throughout the process.

Report Contents

The Incident Summary Report (ISR) will include all pertinent information to the incident, but at minimum:

- Dates and times of milestones throughout the process (e.g. incident detection, verification, notifications, remediation steps, completion, etc.)
- List of symptoms or events leading to discovery of the incident
- Scope of impact
- Mitigation and preventative measures
- Restoration logs
- Stakeholder communications (including copies of memos, emails, etc. where possible)

Timeframe

The ISR should be prepared as expeditiously as possible following the incident so future preventative measures may be taken as quickly as possible. Information to prepare the ISR and interviews with the Safety Working Group should be conducted immediately to ensure the greatest possible accuracy of information.

Post-Incident Review Meeting

After the conclusion of the incident, the Director and possibly select members from the Safety Working Group will meet with management to discuss the event in detail, review response procedures and construct a Process Improvement Plan (PIP) to prevent a recurrence of that or similar incidents. The compiled Incident Report constructed by the Director will serve as a guide for this meeting.

In the meeting, a full debrief of the incident will be presented and findings discussed. The Director will share the full scope of the breach (as comprehensively as possible), causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication

gaps, technical and procedural recommendations, and the overall effectiveness of the response plan.

As a whole, the group will review the information presented and will determine any weakness in the process and determine all the appropriate actions moving forward to modify the plan, address any vulnerabilities and what communication is required to various stakeholders.

Process Improvement Plan

The Director will draft a **Process Improvement Plan (PIP)** based on the results of this meeting. The plan should discuss any applicable items necessary to prevent future incidents to the extent practicable, including cost and time frame requirements where possible. The PIP will also include a review strategy to ensure all recommendations made in the PIP are met in a timely fashion and functioning appropriately.

Areas of focus may include, but are not limited to:

- New hardware or software required
- Patch or upgrade plans
- Training plans (Technical, end users, etc.)
- Policy or procedural change recommendations
- Recommendations for changes to the Incident Response Plan
- Regional communications recommendations

Additionally, the PIP must be kept strictly confidential for security purposes. Any communication required to clients or to the public must be drafted separately and include only information required to prevent future incidents.

Further Reading

Dunn, Suzie, Julia Falco, Chanel Grenaway, et al. Challenging Gendered Digital Harm: Research Report on Impacts and Solutions to Digital Harm Facing Women, Gender-Diverse People, and Gender Equality Organizations. Canadian Women's Foundation, 2025. https://canadianwomen.org/wp-content/uploads/2025/05/25-18_CWF_GenderedDigitalHarm_ENG_Mainreport_v14.pdf

Marwick, Alice, Dafna Kaufman, Jacob Smith, et al. *An AoIR Guide to Researcher Protection and Safety*. 2025. https://aoir.org/riskyresearchguide/.

National Institute of Standards and Technology. "Cybersecurity Framework," November 12, 2013. https://www.nist.gov/cyberframework.

National Institute of Standards and Technology. "CSF 2.0 Profiles," February 20, 2024. https://www.nist.gov/cyberframework/profiles.

National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." Gaithersburg, MD: National Institute of Standards and Technology, February 26, 2024. https://doi.org/10.6028/NIST.CSWP.29.

References

Bhargava, Isha. 2023. “Trans Twitch Star Files Human Rights Complaint Against London, Ont., Police After Swatting Arrest.” CBC News, April 24, 2023. https://www.cbc.ca/news/canada/london/trans-twitch-star-files-human-rights-complaint-against-london-ont-police-after-swatting-arrest-1.6819941.

Communications Security Establishment Canada. “Best Practices for Passphrases and Passwords (ITSAP.30.032).” Canadian Centre for Cyber Security, September 17, 2019. https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032.

Cervini, Eric. Spying Before Stonewall: How the FBI Secretly Tracked Gay Activists in the 60s. June 8, 2020. https://www.vice.com/en/article/the-fbi-secretly-tracked-gay-activists-in-the-60s/.

Cineas, Fabiola. 2023. “Ron Desantis’s War on ‘Woke’ in Florida Schools, Explained.” Vox, February 15, 2023. https://www.vox.com/policy-and-politics/23593369/ron-desantis-florida-schools-higher-education-woke.

“Ghetto Informant Program,” Wikipedia, July 5, 2025, https://en.wikipedia.org/w/index.php?title=Ghetto_Informant_Program&oldid=1298852561.

Jankowicz, Nina. 2022. How to Be a Woman Online. New York: Bloomsbury Academic.

JusticeTrans. 2024. “Understanding & Fighting Back against the Anti-Trans Movement in ‘Canada.’” Toronto, ON: JusticeTrans and Women and Gender Equality Canada. https://justicetrans.org/wp-content/uploads/JT-REPORT-2024-FINAL-ENG.pdf.

Lang, Nolan. 2024. “Saskatchewan’s Pronoun Law and Canadian Anti-Trans Sentiment - Spring.” Spring: A Magazine of Socialist Ideas in Action, February 7, 2024. https://springmag.ca/saskatchewans-pronoun-law-and-canadian-anti-trans-sentiment.

Luneau, Delphine. 2022. “ICYMI: Leading Medical Organizations Call for Action to Counter Threats, Abusive Behavior Targeting Health Care Facilities, Workers and Families.” Human Rights Campaign. October 3, 2022. https://www.hrc.org/press-releases/icymi-leading-medical-organizations-call-for-action-to-counter-threats-abusive-behavior-targeting-health-care-facilities-workers-and-families.

Massanari, Adrienne. 2017. "#Gamergate and the Fappening: How Reddit's Algorithm, Governance, and Culture Support Toxic Technocultures." New Media & Society 19 (3): 329–46. https://doi.org/10.1177/1461444815608807.

Mortensen, Torill Elvira. 2018. "Anger, Fear, and Games: The Long Event of #GamerGate." Games and Culture 13 (8): 787–806. https://doi.org/10.1177/1555412016640408.

Rothchild, Alice. 2020. "Cyber Bullies at Canary Mission Muzzle Free Speech." Washington Report on Middle East Affairs, January/February, 12–13. https://www.wrmea.org/2020-january-february/cyber-bullies-at-canary-mission-muzzle-free-speech.html.

Ruf, Cory. 2024. "Amnesty International Canada Condemns 'Appalling' Anti-Trans Policy Changes in Alberta." Amnesty International Canada. February 2, 2024. https://amnesty.ca/human-rights-news/appalling-anti-trans-policy-changes-in-alberta/.

Shrier, Abigail. 2020. *Irreversible Damage: The Transgender Craze Seducing Our Daughters*. Washington, DC: Regnery Publishing.

Appendices

Appendix A. Incident Log Template

Column titles:

- # (ID number)
- TLP (Traffic Light Protocol): clear, green, yellow, or red
- Has Report: yes, no
- Date
- Status: new, open, closed
- Task # (NA, Planio #, GitHub #)
- Type: email, Bluesky, Facebook, Instagram, other online platform, physical, verbal, threats, theft, vandalism, medical, fire, hazard, other
- Reported By (reporter name)
- Username (of threat actor)
- Short Description
- Response
- Notes
- Screenshot File Name
- Link (to webpage with suspicious activity)

Appendix B. Incident Report Template (IRT)

Date and Time

Date of Incident:

Time and Duration of Incident:

Location

Venue Name and Address:

Specific Area of Incident:

Date and Time

People involved:

Contact info:

Description of Incident

Brief Summary:

Detailed Description of Incident and Actions Taken (Immediate response, Emergency services contacted, How was the incident resolved)**:**

Description of Equipment, Property, Damage or Loss Incurred and Estimated Value:

Additional Info:

Supporting Documentation:

Incident Type

- ☐ Physical
- ☐ Verbal
- ☐ Property Theft or Vandalism
- ☐ Medical Emergency

- ☐ Fire or Hazard
- ☐ Other:

Incident Severity

- ☐ Low
- ☐ Moderate
- ☐ High
- ☐ Critical

Involved Parties

Names and Roles of Individuals Involved:

Contact Info (optional based on safety and privacy concerns, useful for recordkeeping):

Witness Information

Name of Witness:

Contact Information:

Statement/Testimony:

Reflection and Follow-Up

Lessons Learned:

Preventive Measures Implemented:

Follow-up Tasks:

Reporter Information

Name:

Date:

Appendix C. Care Plan: A Victim-Centered and Trauma-Informed Guide to Evaluating Options in Times of Crisis

Immediate Actions

If you feel physically unsafe, remove yourself from the environment and contact emergency services or a trusted ally. Ensure you have access to basic necessities like water, food, and a safe space during the crisis. If you are concerned about being followed, watched, or stalked when removing yourself (e.g. someone is waiting outside), you might call a campus or community walk-and-talk service, contact a trusted ally, call a taxi, or have someone in the area escort you out. For immediate anxiety, grounding techniques, like deep breathing exercises, can help.

Introduction

It can be incredibly overwhelming and stressful to take action in a time of crisis. While it is important to centre the targets and/or victims of an incident, it can be painful and upsetting to be centred and to have to make big decisions in times of crisis. To even see yourself as the victim of a targeted attack can take a long and challenging process of reframing – for some, this just isn't a useful position.

In writing this policy, we want to recognize that the systems that exist to respond to these threats, attacks, and incidents are often not designed with the wellbeing of people targeted in mind. Often, when faced with potentially upsetting, stressful, and even traumatic incidents, we are left with what feels like no good options. This very real experience can be isolating and alienating. We hope that this plan will be one step toward a victim-centric safety planning process that does not rely on structures of securitization to make support and community accessible. We write this plan with an understanding that incidents are not always reported due to the same challenges that can also block access to community, support, and care.

This plan is written with two perspectives in mind: providing a basis and structure for community-based care and providing resources directly to victims of different types of attacks. A central point of focus is the options you have when dealing with an attack or crisis. We are often pressured to take immediate action and this plan aims to instead provide an overview of what each option provides and might look like.

Dealing with Shame and Blame

Above all else, we want to stress that a personal or cybersecurity incident is not your fault. As many steps as we take to protect ourselves, we can still become victimized or harmed by an

incident out of our control. Sometimes this is a result of a direct, targeted attack and other times you may be collateral damage. Challenges faced by victims of a personal or cybersecurity incident include emotional stresses such as guilt, shame, embarrassment, or fear. Compromising a shared computer system can result in guilt and shame that will silence timely reporting. Professional embarrassment or fear of career consequences may hinder the project safety. Personal, often physical, challenges associated with public scholarship and activism may require rapid responses such as calling the police or security, which may also be a source of risk and further stress.

Challenging Decisions

As we are faced with challenging decisions to protect ourselves and others, we do not become responsible for the harm that is done to us. The challenges associated with the experience do not become less real as a result of our planning processes. Planning does not make us responsible for the everyday violences and sources of harm that come out of repressive political-economic structures, nor the actions of individuals who want to cause us harm. Whether you have a minimal online presence or a large public following, you are not to blame for the harm that is directed at you. The standard, and often systemic, response to these kinds of incidents often falls back on victim blaming: you were “too loud,” “too public,” “too private,” and even “too trans” to be protected. Regardless of your actions, you can still be the target of cyber- and personal security threats and we are here to support you through it.

While disclosing that you have been targeted can help us to support you through an incident, it can also present additional threats to personal and social safety, especially when an incident involves the weaponization of personal information and/or false accusations. We want to have open conversations about what disclosure means to you, what kind of and how much information is shared, and how documentation is stored. We must be ready to identify an incident and determine our safety both in person and online. We view this process as complex, imperfect, and nonlinear and are ready to support your process of responding to and recovering from an incident.

Finding support and self care during distressing times

Fear, anxiety, and depressive symptoms are common responses to cyberstalking and online attacks (Worsley et al. 2017). Victims report feeling helpless and feeling that the support available to them, particularly from police, is inadequate (Worsley et al. 2017). Being stalked, attacked, and/or threatened can feel embarrassing and isolating – often by design. Whether personalized or politicized, shame is a key part of violence.

It is important that you access networks of support to whatever extent you are comfortable. Share your experiences with friends, colleagues, family, join online or in person support

groups, reach out to professionals and survivors. Share as little or as much as you are ready to. Take your time to layer coping strategies and responses that feel right for you and your situation whilst prioritizing your safety.

We want to ensure that you have options in this process of personal safety planning and, above all, that you are not dealing with it alone. If it is overwhelming to document an incident, make space for yourself to feel that and find support around it. The following strategies can provide support during difficult times:

Practice Self-Compassion: Remind yourself that being targeted is not your fault, and you are not alone in this experience.

Acknowledge Your Feelings: It's normal to feel anger, fear, or helplessness. Allow yourself to process the impact of the crisis and your emotions without judgement.

Lean on Trusted People: Reach out to friends, family, or colleagues who can offer emotional and practical support.

Focus on What You Can Control: Prioritize actions that help you feel safer, such as enhancing digital security or temporarily stepping away from online platforms.

Delegate tasks: Ask trusted allies to help with monitoring online activity, reporting abuse, or managing your social media accounts.

Professional Help: Consider consulting a therapist, counselor, or support group experienced in handling harassment-related stress.

Advocate for Yourself: Clearly express what type of support or assistance you need from your network. Block or mute harassers and adjust privacy settings to protect yourself.

Engage in Calming Activities: Practice mindfulness, breathing exercises, or activities that help you ground in the present moment.

Stick to a Routine: Re-establishing daily habits can create a sense of stability and normalcy.

Digital Detox: Limit screen time and social media exposure to avoid retraumatization from online interactions.

Stay Connected and Combat Isolation: Reach out to others, even if it's just to vent how you're feeling. Staying connected can reduce overwhelming feelings and loneliness.

We also recommend this advice from psychologist Lisa Feldman Barrett (*How Emotions Are Made: The Secret Life of the Brain*) on dealing with online harassment and distressing times.

Evaluating Options: Reporting & Documenting an Incident

Document the Incident

Alongside the direct experience of the incident and decision-making, the process of capturing, documenting, and storing information about an incident can bring on complex and potentially mixed emotions. In some cases, it can be easy, cathartic, and relieving to document an incident. In other cases, it can be upsetting, triggering, and overwhelming to do so. It is normal to move through these emotions whilst processing the incident. Neither response speaks to the nature or the severity of the incident nor you as a person.

Documenting an incident is often associated with potentially exposing or arresting its persecutor. Sometimes this will be and immediately feel like the best option. Sometimes you might feel confused or unsure. Sometimes you will be completely opposed to this approach. For this reason, it can help to focus on this particular task at a speed and at times that make sense for you. You do not have to make a police report, go to security with, publicize, or even review this documentation. However, it is often useful to ensure that you have it prepared so you can put it away and revisit when you have a better sense of what your next steps might be. It can take some of the pressure off of a decision when its immediacy is stripped away.

Types of Evidence

Document evidence such as screenshots, emails, or messages to use if you decide to report the harassment. Keep a record of the incident in a place where it is secure but out of sight in everyday life. Store screenshots out of your main camera roll on your cell phone and in a private, password protected Drive or Locker. The idea is to have these files safe, secure,and available to you when you might need them, without turning them into a trigger or a disruption. If documenting feels overwhelming, ask a trusted friend or ally to assist.

Reporting the Incident

See the Contact Info section for who to contact to first report an incident. For more information about reporting, see the relevant section, either Personal Safety, Cybersecurity, or Event Safety.

If you immediately know that you need support or need help finding support, you can bring this up while reporting. If you do not immediately know, that is perfectly normal and okay. The door to support will not close. You can let us know when reporting if you need someone to check in with you regularly, how, when and how long you might need this.

If you decide to report a potentially compromised phone to police, it is likely that they will take your phone for a period of time to scan or evaluate its contents. For example, they can

retrieve messages, locate spyware or stalkerware, and gather other kinds of evidence against your attacker. While this may preserve evidence, giving your phone to police can be uncomfortable and even risky. If this is a concern, you may be able to get help from your local victim service program or from a free legal clinic. If you need help finding these services, reach out to a contact on the safety team or trusted friend.

Resources and tools

For Carleton Students

Carleton Health and Counselling Services

Equity and Inclusive Communities

For all lab employees:

Employee & Family Assistance Program: Carleton's Employee & Family Assistance Program (EFAP) is a free comprehensive program that is available to support faculty, staff and their families.

Ottawa and Canada-based Resources and Tools

Ottawa Victim Services (OVS) is a not-for-profit organization based in Ottawa, ON, Canada. Since 1998, OVS has been providing emotional and practical support to people in our community who've been affected by crime or tragedy

The Crisis Line's professionally trained volunteer crisis line specialists are there to answer your call 24 hours a day, seven days a week. They will provide you support in a crisis and can transfer your call to the Local Crisis Team if needed.

Good2Talk is a free, confidential and anonymous helpline providing professional counselling and information and referrals for mental health, addictions and well-being to post-secondary students (18-30) in Ontario, 24/7/365.

Walk-In Counselling Clinic: No referral is required for the Walk-In Counselling Clinic. You will be assisted, with no appointment, on a first-come, first-serve basis during our Walk-In Counselling Clinic hours. The Walk-In Counselling Clinic is open to Ontario residents within the greater Champlain region. The Walk-in Counselling Clinic offers counselling services in English, French, Arabic, Somali, Spanish, Cantonese and Mandarin at a variety of different locations.

VictimLink BC (1-800-563-0808) is a 24-hour, B.C. toll-free information, support and referral service for victims. You will find a safe and confidential service where you can discuss your experience and decide what you want to do. They will not discuss your situation with anyone else without your knowledge and permission, except as required by law (such as in cases of child abuse or neglect or a crime that is about to be committed).

Free Legal Clinics of Ottawa, with three locations across the city, can give you legal advice, help you fill out forms related to your case, represent you at some tribunals and courts, refer you to other agencies when they can't help

Canada-Wide Resources and Tools

Canadian Centre for Occupational Health and Safety offers a guide for dealing with internet harassment in the workplace.

eMentalHealth.ca: a community navigation tool concentrated on resources in Eastern Ontario, organized according to catchment area and type of service. This searchable online tool makes community resources and referral information accessible.

NeedHelpNow.ca offers support to minors affected by online sextortion and online sexual violence.

Techsafety.ca compiles a list of Canada-wide and provincially-specific resources for victims of online harassment, abuse, and stalking.

Victim Services Directory can be used to locate and connect to local victim service providers.

International Resources and Tools

Coalition Against Stalkerware – Resources and tools for detecting and removing spyware.

Access Now: if you're an activist, a journalist, a human rights defender, or a member of a civil society group currently experiencing an urgent digital security incident, you can contact Access Now, a nonprofit organization that can provide emergency assistance, recommendations and referrals, technical support, and educational resources through its Digital Security Helpline.

Crash Override Network operates a crisis phone line and online resources for people who are experiencing online abuse.

Dangerous Speech Project's guide on counterspeech.

CCRI Crisis Helpline: if you are a victim of nonconsensual pornography, defined as the distribution of sexually graphic images without your consent, and you are living in the U.S.,

contact the Cyber Civil Rights Initiative, a nonprofit organization combating online abuse. It offers resources, legal referrals, and a 24/7 Crisis Helpline.

Vita Activa: If you are a Spanish speaker, Vita Activa has a helpline providing online support for women, LGBTIQ+ people, journalists and activists experiencing stress, trauma, gender violence or other crises.

Coalition Against Stalkerware can help you find support through a resource list it maintains if you are concerned about potential spying, monitoring, or stalking.

Online Harassment Field Manual, by the nonprofit organization PEN America, offers strategies and resources for those facing online abuse.

Tall Poppy helps organizations protect their employees against online harassment and abuse. They offer an online digital safety management platform which helps people lock down their accounts and protect their privacy. Should an employee come under attack, their expert incident response team provides compassionate support to reduce the harm of harassment.

Emotionally Demanding Research Network Scotland is a group of researchers (including students, research support staff, and practitioners involved in research) with experience of conducting emotionally demanding/challenging research. Our aim is to connect people involved in this kind of work in order to better support each other in doing this research.

Right To Be provides resources for self-care for victims of cyber harassment. Their guide is available in English, French, Arabic, Burmese, Indonesian, and Spanish.

References

Barrett, Lisa Feldman. “Advice from a Psychologist.” *Online Harassment Field Manual*, PEN America, April 9, 2018. https://onlineharassmentfieldmanual.pen.org/advice-from-a-psychologist/.

Worsley, Joanne D., Jacqueline M. Wheatcroft, Emma Short, and Rhiannon Corcoran. 2017. “Victims’ Voices: Understanding the Emotional Impact of Cyberstalking and Individuals’ Coping Responses.” Sage Open 7 (2): 2158244017710292. https://doi.org/10.1177/2158244017710292.

Appendix D. Event Planning Checklist

In Advance of Event:

What is the level or perceived risk and concern, and how can you increase safety accordingly?

- ☐ Content: Are the guests or topic considered 'controversial'?
- ☐ Location: Are there anti- rallies happening in the locale?
- ☐ Environment: Have there been incidents at other similar events locally or currently? What safety lessons can we implement from them?
- ☐ Have explicit discussions prior to an event on the role and need for law enforcement services: understand what actions various law enforcement services are authorized to take that the event organizers would be unable to act on their own (e.g. escorting people out of the venue)
    - ☐ If you decide that security/police have a role, have a clear plan to keep people who are typically targeted by security/police feeling safe and comfortable.
    - ☐ Familiarize yourself with your rights as well as the rights and limits of law enforcement services chosen (Campus Security, Police/911, venue security, trained personnel).
- ☐ If the event is expected to garner publicity for the project, brief the chair, dean, Coms, and the office of risk management to explain why we are at risk and to prepare them for any complaints.
    - ☐ Work with University Communications to prepare press statements designed to counter disinformation. Create a simple key message, written for those who care about the topic and are interested.

Venue, Date and Time Selection:

- ☐ Choose venues with multiple exit routes and accessible exit plans and safety plans.
- ☐ Confirm if you have the right to ask people to leave. Can anyone come in? Is there open access to the building or room?
- ☐ Is there service or wifi? How will the event organizers communicate on the day of?
- ☐ Consider the safety of people arriving and leaving the event, whether it is an evening or day and how far is parking/public transportation.

Planning with Guest Speakers and Co-Organizers:

- ☐ Ask guests about their security and safety concerns, needs, past experiences, and what we can generally do to make them feel safe.
- ☐ What are the guests' comfort levels in Q&A panels? Are there questions they will not respond to? Do they want a facilitator to respond to those questions and to disruptors?
- ☐ Have your questions, speeches, or facilitation notes peer-reviewed.

Leading Up to Event:

- ☐ Create registration for the event.
- ☐ Limit disclosure of the time and location of the event (registrants only, days before event, etc.)
- ☐ For online events: Create a passcode, waiting room, or other form of authorization to control event access

Day of Event:

- ☐ Identify security options and introduce yourselves to on-site security.
- ☐ Go over your Emergency Contact procedure, assign and review roles:
  - ☐ Know what authorities or support will be called and when, by whom, and in what order, to avoid multiple calls or confusion.
  - ☐ Identify people with de-escalation training, First Aid, knowledge of local mental health resources.
  - ☐ Roles: Facilitator/Host, Co-Host, Guest Liaison, Security Monitor, Medic, Peer support
- ☐ Inform co-presenters and guests of safety plans, exit routes and points of contact so they are not panicked or lost if an incident occurs.
- ☐ Take a headcount at the beginning and occasionally to be aware of changes. If there is a registration list, confirm with the number registered.
- ☐ Screen audience questions and participation through mediation, submitted written questions/Slido/QR code/etc.
- ☐ Maintain communications in a group chat so that the team is all aware of potential threats or actions taken and so that you have documentation.

For Online Events:

- ☐ Limit video and audio controls for participants when appropriate.
- ☐ Turn off general chat.

- ☐ Assign trusted co-hosts.

Appendix E. Carleton's Social Media Privacy and Security Guidelines

The Transgender Media Lab's Social Media Policy is available on our public website. This policy helps ensure our social media content reflects our lab's values. This policy also describes the actions we will take to ensure that people commenting on our social media posts are not causing harm to BIPOC and disabled trans people.

Below are the guidelines that Carleton University Communications has shared with us:

Basic Security

- Consider having a professional and personal profile. Your personal profile should be used for close friends and family, while you share your professional profile on your website, employment bio, etc. This allows you to continue using social media on your personal account without having to interact with distractions or harassment that may come to your professional account. Personal accounts have limited connections (only people you know), are listed as private, and do not have identifiers to your real name or profession. This allows you to have a safe space to interact with friends on social, should your professional account come under any issues.
- Link a private phone number and email address to your accounts, separate from your normal or everyday email account. You may consider using an email address created specifically for social media management. If your account is accessed or your email is viewable from the social profile, you can ensure that your normal private email is not visible to the public.
- Regularly check the security settings on your profiles (ex. quarterly). Platforms often change features and settings, and you may have your settings overridden or new settings enabled as default.
- Narrow your connections on your personal profiles. Be wary of the types of entities and individuals who you connect with and do not know on a personal level.

Usernames, Biographies, Profile Pictures

- It is strongly recommended that you avoid using a profile or username which indicates or relates to your real name.
- Avoid profile pictures which can indicate your location (street signs, home number, license plates, etc). When possible, choose photos with a neutral background and show limited objects.
- Keep personal information off the platform. Birthdates, addresses, additional modes of contact, these are items that do not need to be shared on social media.

Passwords and Logins

- When possible, you should always use multi-factor-authentication (MFA).
- Do not reuse passwords between sites.
- Do not use departmental or shared mailbox accounts, only use work emails to manage CU owned accounts (exampledepartment@carleton.ca vs janesmith@carleton.ca)

Managing X (Twitter)

Restricting Commentary

- Click on your post
- Click "..." in the upper right of the post
- Click "Change who can reply"
- Click "Only accounts you mention"

Privacy Settings

- To find your privacy settings click the "..." icon; sometimes labelled as "More".
    - Click "Privacy and Safety".
    - From this area you can determine the information you share, who can see what you share, along with what you can see.
- To prevent others from accessing your Tweets, click "Audience and tagging".
    - Click "Protect your Posts". This makes it so individuals who follow you are the only ones who can see your posts.
    - Change 'Photo tagging' from "anyone can tag you" to "only people you follow can tag you".
- Turn off your location by Clicking "Your posts".
    - Click "add location information to your posts".
    - Deselect "Add location information to your posts".
- To mute or block individuals click on "Mute and Block"
    - You can mute notifications from people you don't follow or don't follow you, as well as new accounts/accounts with default profile pictures/accounts with unverified emails and phones numbers – this is recommended as these accounts are most likely to be troll accounts.
    - o mute or block individuals you must do so from one of their posts or profile pages. Navigate to a post or profile page and click "...". From that menu select mute or block.
- To control direct messages, return to "Privacy and safety," click "Direct Messages"
    - Click "Allow messages only from people you follow". This will prevent strangers from DMing you.

    - Disable read receipts.
- Turn off “Spaces” listening activity under the Spaces section.
- Discoverability, consider disabling letting people find you with your email or phone number, especially if your account is created with a publicly available email or phone number (e.g. your Carleton University account).

Managing Instagram

Restricting Commentary

- Click “More” or the icon.
- Click “Settings”.
- Scroll to “How others can interact with you”
- Click “Hidden Words”
    - Click “Manage custom words and phrases”
    - Enter the words that are causing issues. All words entered will automatically trigger comments to be hidden should they contain them. (ex: murder, terrorism, etc.)
- To restrict users, and automatically hide all their previous commentary on your account and posts:
    - Click the username on the comment o Click the ‘...’ on the user profile
    - Click ‘restrict’
- On an individual post:
    - Click on your post
    - Click “...” in the upper right of the post o Click “Turn off commenting”

Privacy Settings

- Click “More” or the icon.
- Click “Settings”.
- You will be taken to the embedded Meta Accounts Center. You can choose to edit your information in the Instagram version or go directly to the Meta Account Center. Both options have similar tools sets, but the Meta Accounts Center will allow you to view all your Meta profiles at the same time.
- Click “Who can see your content”
    - Click “Private Account”. Now people need to request access to see your content.
- • Click “How others can interact with you”
    - Disable “Show Activity Status”
    - Change “Allow @mentions from” from ‘everyone’ to ‘people you follow’ o Disable “Allow others to use your posts”

    - Change “who can tag you” from ‘everyone’ to ‘people you follow’
    - Consider the “Hidden Words” section of the settings.
- You may choose to add advanced filtering to hide comments with key words you find offensive or triggering
- Enable “hide message requests” which will take the keyword filter and apply it to DM’s.
    - Click “Comments”
- Change “allow comments from” ‘everyone’ to ‘people you follow and your followers’
- Consider adding keyword filters which will automatically hide any comments you don’t appreciate.

Managing Facebook

Restricting Commentary

- Click Settings
- Click “Followers and public content”
- Click ‘Hide posts with profanity’
- Click ‘Hide Comments containing certain words’
    - Enter the words, separated by commas, that you wish to be comments and posts to have to be automatically hidden.

Managing LinkedIn

Restricting Commentary

- Click on your post
- Click “...” in the upper right of the post
- Click “who can comment on this post”
- Click “no one”

Privacy Settings

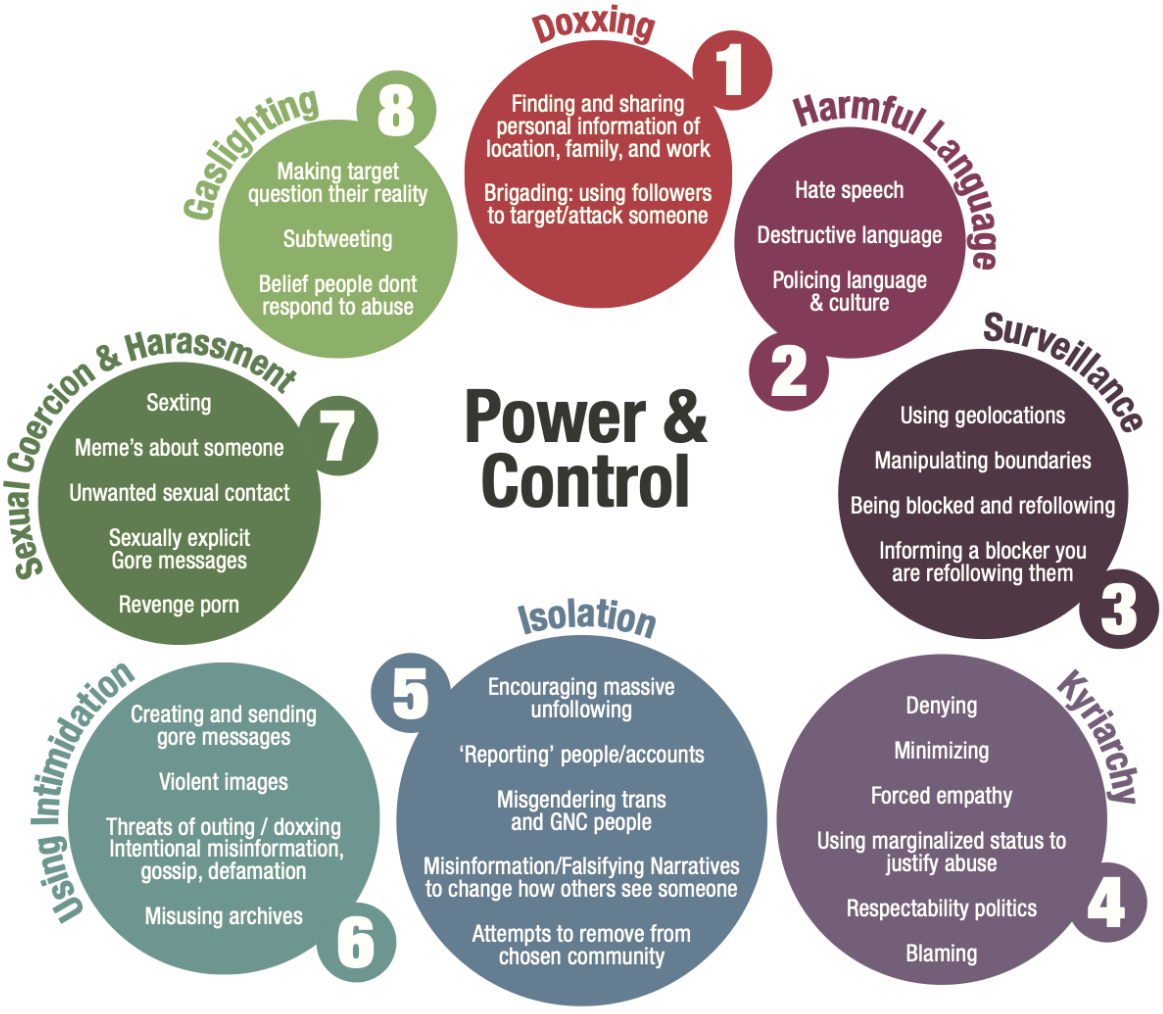
- Click “Me” on the top right of the LinkedIn menu
- Click “Setting & Privacy” Under “Account”
- On the next page, the right-hand menu will have a tab “Visibility”.
- Click the “Visibility” tab
    - Under ‘profile discoverability using email’, change from anyone to connections
    - Under ‘profile discoverability using phone number’, change from anyone to connections
    - Click “Who can see your last name”, change to connections
    - Click “Notify connections when you are in the news” – turn to off.

Appendix F. Power & Control Online

Power & Control

1 Doxxing
2 Harmful Language
3 Surveillance
4 Kyriarchy
5 Isolation
6 Using Intimidation
7 Sexual Coercion & Harassment
8 Gaslighting

Modeled from the popular Power & Control Wheels that have been created for discussing domestic and intimate partner violence, we extend those conversations to the violence we have experienced and survived online. We have described the violence we have experienced and seen online.



Created by The Alchemists: Bianca Laureno, I'Nasah Crockett, Maegan Ortiz, Jessica Marie Johnson, Sydette Harry, Izetta Mobley, and Danielle Cole for the Center for Solutions to Online Violence. | **Design by:** Liz Andrade

Appendix G. Understanding & Fighting Back against the Anti-Trans Movement in ‘Canada.’

PDF available here:
https://justicetrans.org/wp-content/uploads/JT-REPORT-2024-FINAL-ENG.pdf