Tech Safety Planning Checklist

A Note on Language

In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

Technology safety planning should always be done in tandem with more traditional safety planning. Online violence and offline violence are interconnected and it is important to consider the non-technology-related risks that may be associated with technology safety planning. This tech safety planning checklist is meant to be an addition to a broader safety plan and not a standalone checklist.

Whenever you are safety planning with someone who has experienced technology-facilitated violence, it is important to note that the perpetrator may have access to their devices or accounts and may be monitoring their communication and movements via these devices and accounts. Making changes to any device, social media account, email, or other technology may alert the perpetrator that your client is seeking help and can trigger additional abuse. Extra safety planning precautions may need to be taken in these situations.

In some cases, you may need the support of an IT specialist or law enforcement, such as when detecting stalkerware or other spyware.

Passwords

- [ ] Make a list of all devices (e.g. laptop, cell phone, Fitbit, AirTags, home security system, smart car, Internet-connected devices, Siri/Alexa, Bluetooth-connected sound systems, etc.) and accounts (e.g. social media, email, online shopping, online food services, transportation apps, cloud accounts, fitness trackers, games, etc.). See appendix A for a list of potential accounts.
- [ ] Note which of these the perpetrator has access to, knows the passwords to, or may know the passwords to.
- [ ] Think about what information is included on those accounts (e.g. home address, phone number, email address, credit card information, personal messages, Internet search history, communication about safety planning, etc.).
- [ ] Change all passwords to unique passphrases that the perpetrator would not be able to guess. Avoid using things like the names of children or pets, important dates, old addresses, or old phone numbers. A passphrase is a sentence that is easy to remember but would not be easy to guess. Adding symbols of numbers for letters can make it even more difficult to guess (e.g. L1tTl3R3dC0rV3Tt3).
- [ ] Do not use the same password for multiple accounts.
- [ ] Use a unique passphrase for each account or use a password manager.
- [ ] Change the password to your home Wi-Fi.
- [ ] For security questions on accounts, make up fake answers or do not use questions that the perpetrator would be able to guess; otherwise, they may be able to access the account (e.g. instead of using your mother's maiden name, make up an answer when they ask for your mother's maiden name and answer with something different. Just make sure you will remember your fake answer).
- [ ] Turn off all automatically saved passwords on all devices and accounts.
- [ ] Sign out of all accounts and devices when not using them.
- [ ] Use two-factor authentication on any app or account that allows for it. Two-factor authentication requires you to enter a password that is sent to your phone or email to confirm that it is actually you accessing the account.
    - [ ] For general information on two-factor authentication, see HackBlossom.
    - [ ] Use this website to see which common apps use two-factor authentication.
- [ ] Do not use social media accounts to sign in to other accounts (e.g. "Sign in with Facebook" or "Sign in with Google" options).
- [ ] Remove the perpetrator's email addresses or devices from shared accounts and as Trusted Devices on your accounts.

Blocking, Deleting, and Unfriending

- Consider blocking or unfriending the perpetrator's email address, phone number, or social media contact. Ensure that you have collected all the evidence needed from those accounts before doing this. Certain programs will delete or not allow you to access conversations and information from the other person's account once they have been unfriended, blocked, or deleted from your account.

- When deciding to block, delete, or unfriend someone, consider whether this may escalate the abuse. There may be benefits to having access to the perpetrator's social media (such as knowing their location) that are worth considering.
- Consider which of your friends and family may have your perpetrator as a "friend" on their accounts. Ask friends and family not to post information about you or photos of you online and not to share information with the perpetrator.

Stalking, Tracking, and Monitoring

- Use a camera cover on all your devices' cameras when you are not using them.
- If the perpetrator is tracking your device or accounts, consider using a different device (e.g. a friend's computer, a work device, or a computer at a library) to look up information and begin planning how to make changes to your devices or accounts.
- Consider what personal information is posted online (e.g. home address on a birthday event invitation, phone number in a Facebook post, or a new workplace on LinkedIn) and decide whether to delete that information or make it private. Remember that other people could share that information with your perpetrator even if you have blocked them from your accounts.
- Turn off or limit the location functions on your devices when not in use.
- Turn off location functions like Find My Phone or Find My Friends.
- Delete previously-stored location history, especially before and after arriving at domestic violence shelters or other safe spaces.
- Do not "check-in" to locations on social media.
- Change privacy settings on apps and social media to more private settings.
- Do not post photos on social media containing metadata or background information that could alert the user to your location. One way to remove location-based metadata on a photo is to take a screenshot of the photo and post the screenshot rather than the original photo that contains the metadata.
- Remove the perpetrator's email addresses or devices from shared accounts and remove their device from Trusted Devices on all your accounts. See Appendix A for potential accounts.
- Check accounts for Last Account Activity or Account Activity to see if any unusual IP addresses are accessing the account.
- If there is concern that the perpetrator has access to your accounts, consider using a P.O. Box for an address on online accounts and deliveries. Consider the risk of the perpetrator accessing credit card information or misusing the account if they have access.
- Untether your phone or other devices from the perpetrator's devices (e.g. Bluetooth stereo in their car or home, fitness notifications to their smartwatch, etc.).
- Search belongings (e.g. purses, cars, jackets) for GPS tracking devices or other recording devices.
- Examine any gifts or unusual items in the home, including children's items, for hidden cameras or recording devices.
- Consider what information is on your children's devices and accounts (e.g. phones, video game systems, social media accounts) and what may be shared with the perpetrator.
- Consider whether the perpetrator may have access to any home security system information, such as access to the cameras or information when people are leaving or entering the home.
- Consider using a device or program (e.g. network scanners, port scanners, RF signal detectors) that can detect certain hidden cameras to scan your Wi-Fi or home.
- Look through apps on your phone and delete any unfamiliar ones.
- If you are concerned that the perpetrator may have installed spyware on your devices, you may want to have an IT specialist or law enforcement check the device for spyware. Remember that if spyware is installed on the device, the perpetrator may be able to see whatever is being done on the device, which may escalate the abuse.
  - The Clinic To End Tech Abuse also has resources to help identify spyware on a device.
  - Signs that a device may have spyware on it:
    - Device running slowly
    - Battery draining
    - Data being used up
    - Device getting hot
    - Device lighting up when not in use
    - Clicks or odd sounds on calls
    - Takes a long time to shut down
- Keep your devices' operating systems up to date. These updates often patch any insecurities found on the software that hackers could misuse and spyware. Double-check your privacy settings after an update to make sure the update did not change any of them.
- Consider replacing devices entirely. If you decide to do this, you should not back up your devices from previous devices. This may transfer any spyware installed on the previous device.
- Look for unusual hardware attached to desktop computers (e.g. key loggers are often attached between the keyboard and the desktop).
- It should be noted that experienced hackers and IT engineers may be able to access the location of a device, even when it is turned off in the settings. If your perpetrator has an IT background, there can be additional challenges to tech safety depending on their skill. You may want to speak with an IT specialist or law enforcement if this is the case.

Alternate Accounts

- If the perpetrator has access to your accounts and there is no safe way to stop this at this moment (e.g. if they require you to share your passwords by threatening to hurt you otherwise), create an alternate email account or social media account that the perpetrator does not know about or have access to for sensitive communication.
- Do not sign into this account on your personal or shared devices. Use a work computer, library computer, or friend's computer to access it.

Cloud Storage, Shared Accounts, Unauthorized Access

- Remove the perpetrator from any shared accounts, devices, or plans if it is safe to do so.
- Remove Bluetooth connections from the perpetrator's devices (e.g. connected to their home stereo, car, etc.).
- Consider what content is being automatically uploaded or connected (e.g. calendars, iCloud storage for photos and texts, Fitbit, smart watches) and whether the perpetrator could gain access to these accounts or information.

- Remove all devices except your own devices from Trusted Devices on all accounts.
- Check Last Account Activity on all accounts to see if an unusual IP address or device has been accessing the account.

Search History

- If the perpetrator has access to the device or account, they can check your search history.
- If looking for help or resources, use a computer that is not in the home (e.g. a public computer, a friend's computer, or a work computer).
- Selectively delete Internet search history.
- Use "private" or "incognito" options so the search history is not being recorded.
- Turn off cookies in the browser setting.

Intimate Images or "Revenge Porn"

- Make a list of images and videos that may exist.
- Consider using Facebook's program that prevents other people from uploading sexual images that have been registered and "hashed" with the company. However, you would need to send those photos to Facebook for the program to be able to recognize and remove the images from Facebook and Instagram.
- If safe to do, ask your former partners to delete any intimate images after the relationship ends and tell them that there is no consent to share them. Document this communication.
- Consider whether the perpetrator may have been able to capture images without consent (e.g. hidden camera, screen capturing sex via Zoom or Skype).
- Do a reverse image search on Google for images.
- Search common pornography sites for your name. People are often doxed and named when their images are shared.
- Set up a Google alert for your name, as this can help alert you when your name is mentioned online if it is posted along with your images.
- Consider alerting family, friends, and co-workers who may receive the images to reduce the harm.
- If the image has been shared without consent, see the Cyber Civil Rights Initiative guide to getting content taken off the Internet.
- Report to social media companies or porn companies, as most have policies that forbid non-consensually shared nude images.
- If sharing intimate images, consider harm reduction strategies:
  - Avoid images with your face or identifying marks (e.g. tattoos, birthmarks)
  - Avoid images in places that are identifiable (e.g. a recognizable room)
  - Use programs like Signal that allow for disappearing messages
- If images have been released, consider using a reputation service to help get the content removed.

Google Alerts

- Set a Google alert for your name so you are notified when your name appears online. This will not find all places where your name is posted, but can alert you to some instances.
- Make a Google alert for all versions of your name (e.g. Victoria Chan, Vickie Chan, Vicky Chan)

Reporting Harmful Content to Social Media Companies

- Gather evidence (e.g. screenshots) of the harmful content before reporting, as it may be deleted by the social media company if it violates their policies.
- See HeartMob's Media Safety Guides for tips on social media companies' policies and reporting mechanisms.

Software Updates, Firewalls, and Anti-Virus Software

- Update your software regularly. This includes your mobile phones. These updates often patch any insecurities found on the software that hackers could misuse.
- Enable firewalls and anti-virus software on all devices.

Evidence Collection

- Create a log of all experiences of technology-facilitated violence and include information such as the time, date, perpetrator, evidence gathered, and other useful information. See WSC's Sample Technology-Facilitated Violence Log here.
- Take screenshots or make recordings of abuse.
- Consider whether the app alerts the other person if someone else takes a screenshot. If it does, it may not be safe to screenshot and it may be better to take a photo or video of it with a second device.
- Ensure you include the profile and other identifying information about the perpetrator in the evidence.
- Ensure it shows the date of the abuse.
- If the abuse is happening via email, keep the original email as it contains metadata such as the IP address of the sender.
- If the abuse was posted by someone else, capture it before they have a chance to delete it.
- Store copies of the evidence in a secure location. Back up the information in at least one other location.
- If the perpetrator has access to the device or cloud storage where the evidence is stored, they could delete the evidence.
- Have both printed copies and electronic copies of the evidence.

Download Appendix A: Devices and Accounts to Consider

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you or call/text the Kids Help Phone to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

We gratefully acknowledge Suzie Dunn, PhD Candidate at the University of Ottawa, for the creation of this information sheet.

Adapted from BCSTH's Technology Safety project, based on their resource Technology Safety Planning Checklist.

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

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