SPARK
TEEN DIGITAL DATING VIOLENCE

TECHNOLOGY SAFETY PLANNING

CHECKLIST

Technology safety planning should always be done in tandem with a 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. Abusive partners often utilize technology-facilitated violence as part of a larger pattern of abuse. This tech-safety planning checklist is meant to be an addition to a broader safety plan and a resource for support workers and not a standalone checklist.

Whenever you are safety planning with a woman or youth who has experienced technology-facilitated violence it is important to note that the abuser 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 abuser 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 (i.e. laptop, cell phone, Fitbit, home security system, smart car, internet connected devices, Siri/Alexa, Bluetooth connected sound systems, etc.) and accounts (i.e. social media, email, online shopping, online food services, transportation apps, cloud accounts, fitness trackers, games, etc. See appendix A for list of potential accounts.)
- ☐ Note which of these the abuser has access to, knows the passwords to, or may know the passwords to.
- ☐ Think about what information is included on those accounts (i.e. personal address, phone number, home address, credit card information, personal messages, internet search history, communication about safety planning, etc.).
- ☐ Change all passwords to unique passphrases that the abuser would not be able to guess. Avoid using things like the names of children or animals, 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. For example: P@$$phra$$e$@reH@rdT00Gue$$
- ☐ Do not use the same password for every account.

- ☐ 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 abuser would be able to guess, otherwise they may be able to access the account (i.e. 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, but 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 them accessing the account.
  For general information on two-factor authentication see HackBlossom:
  https://hackblossom.org/domestic-violence/defense/two-step-verification.html
- ☐ See this website to see which common apps use two-factor authentication:
  https://twofactorauth.org/#communication
- ☐ Print out or write down several two-factor authentication one-time use codes in case you lose your phone. Store them somewhere the abuser will not find them.
- ☐ Do not use social media accounts to sign in to other accounts (i.e. "Sign in with Facebook" or "Sign in with Google" options).
- ☐ Remove abuser's emails or devices from shared accounts and as "Trusted devices" on your accounts.

Blocking, deleting, and unfriending

- ☐ Consider blocking or unfriending the abuser'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 abuser's social media (such as knowing their location) that are worth considering.
- ☐ Consider which of your friends and family may have your abuser 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 abuser.

SPARK
TEEN DIGITAL DATING VIOLENCE

Stalking, tracking and monitoring

- ☐ Use a camera cover on all your devices' cameras when you are not using them.
- ☐ If the abuser is tracking your device or accounts, consider using a different device (i.e., a friend's computer, a work device, or a computer at a library) to look up information and to begin planning how to make changes to your devices or accounts.
- ☐ Consider what personal information is posted online (i.e., home address on a birthday event invitation, phone number was shared on a Facebook post, or a new work place was announced on LinkedIn) and decide whether to delete that information or make it private. Remember that other people could share that information with your abuser 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 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 containing metadata or background information that could alter the user to your location on social media.
- ☐ 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 abuser's emails 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 abuser has access to your accounts, consider using a P.O. Box for an address on online accounts and deliveries. Consider the risk of the abuser accessing credit card information or misusing the account if they have access.
- ☐ Untether your phone or other devices from the abuser's devices (i.e., Bluetooth stereo in their car or home, fitness notifications to their smartwatch, etc.).
- ☐ Search belongings (i.e., 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 (i.e., phones, video game systems, social media accounts) and what may be shared with your abuser.

- ☐ Consider whether the abuser may have access to 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 (i.e., network scanners, port scanners, RF signal detectors) that can detect certain hidden cameras to scan your Wi-Fi or homes.
- ☐ Look through apps on the phone and delete any unfamiliar ones.
- ☐ If you are concerned that your abuser 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 abuser may be able to see whatever is being done on the device, which may escalate abuse.
- ☐ The Clinic To End Tech Abuse also has resources to help identify spyware on a device: https://www.ceta.tech.cornell.edu/resources

  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, 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 abuser has an IT background, there can be additional challenges to tech-safety.

Alternate accounts

- ☐ If the abuser has access to your accounts and there is no safe way to stop this at this moment (i.e., 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 abuser does not 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.

Cloud storage, shared accounts, unauthorized access

- ☐ Remove abuser from any shared accounts, devices, or plans.
- ☐ Remove Bluetooth connections from the abuser's devices (i.e., connected to their home stereo, smart car, etc.).
- ☐ Consider what content is being automatically being uploaded or connected (i.e., calendars, iCloud storage for photos and texts, Fitbit, smart watches) and whether the abuser could gain access to these accounts or information.
- ☐ Remove all devices except your 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 abuser has access to the device or account, they can check your search history.
- ☐ If looking for help or resources, use a computer not in the home (i.e., 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 (i.e. "Revenge Porn")

- ☐ Make a list of images and videos that may exists.
- ☐ 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 in order for the images to be recognized and removed from Facebook and Instagram.
- ☐ If safe to do, ask the ex-partner to delete the images after the relationship ends and tell them that there is no consent to share them. Document this communication.

- ☐ Consider whether the abuser may have been able to capture images without consent (i.e., 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, this can help alert a person 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 Cyber Civil Rights Initiative guide to getting content taken off the internet: https://www.cybercivilrights.org/online-removal/
- ☐ Report to social media companies or porn companies, 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 (tattoos, birthmarks)
- ☐ Avoid images in places that are identifiable (is the room recognizable?)
- ☐ Use programs like Signal that allow for disappearing messages
- ☐ If images have been released, consider using a reputation services to help get the content removed.

Google alerts

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

Reporting Harmful Content to Social Media Companies

- ☐ Gather evidence (i.e., screenshots) of the harmful content before reporting, as it may be deleted by the social media company if it violates their policies.
- ☐ See HeartMob “Media Safety Guides” for tips on how to report to social media companies’ policies and reporting mechanisms: https://iheartmob.org/resources/safety_guides

Software updates, firewall, 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, include information such as the time, date, abuser, evidence gathered, and other useful information. See the BCSTH Sample Technology-Facilitated Violence Log here: https://bcsth.ca/techsafetytoolkit/sample-technology-facilitated-violence-log/
- ☐ 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 screen shot 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 abuser 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 the information up in at least one other location.
- ☐ If the abuser 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.

Connect to an Anti-violence Work or Legal Advocate for Support

If you would like more information about how to incorporate technology into a safety plan, see the BC Society of Transition Houses Technology Safety Resources or a legal advocate in your community.

- VictimLink BC
- KUU-US Crisis Line Society
- Legal Aid BC
- Rise Women's Legal Centre
- Shelter Safe Map
- BCSTH technology safety planning and A Guide for Canadian Women Experiencing Technology-Facilitated Violence: Strategies for Enhancing Safety

Spark Teen Digital Dating Violence Project

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

This document was published March 2021.

SPARK
TEEN DIGITAL DATING VIOLENCE

APPENDIX A:

Devices and Accounts to Consider

Social Media Accounts

- ☐ Facebook
- ☐ Twitter
- ☐ Instagram
- ☐ Snapchat
- ☐ TikTok
- ☐ Pinterest
- ☐ WeChat
- ☐ YouTube
- ☐ Tumblr
- ☐ Reddit
- ☐ LinkedIn

Communication

- ☐ Smart Phone
- ☐ Computer
- ☐ Gmail
- ☐ Personal and work email
- ☐ Messenger
- ☐ WhatsApp
- ☐ Signal
- ☐ Slack
- ☐ QQ
- ☐ Viber
- ☐ Telegram
- ☐ Instant, DM's or Private Messages on online platforms

Video Conference

- ☐ Zoom
- ☐ MS Teams
- ☐ Skype
- ☐ FaceTime
- ☐ Video Calls on online platforms

Cloud Storage

- ☐ iCloud
- ☐ Dropbox
- ☐ Google Drive
- ☐ Amazon Drive

SPARK
TEEN DIGITAL DATING VIOLENCE

Childcare and pets

- ☐ Shared calendars
- ☐ Child tracking apps
- ☐ Baby monitor
- ☐ Photo sharing
- ☐ Scheduling apps
- ☐ Animal camera
- ☐ Animal tracker (i.e. GPS device in collar)

Bills and Utilities

- ☐ Phone plans
- ☐ Electricity
- ☐ Gas
- ☐ Internet/Cable

Food Delivery Services

- ☐ SkipTheDishes
- ☐ Uber Eats
- ☐ DoorDash
- ☐ Foodora
- ☐ Other restaurant accounts

Finances

- ☐ Bank accounts (including credit cards)
- ☐ Investment accounts (i.e., stocks, investments, retirement, education, etc.)
- ☐ PayPal
- ☐ Apple wallet
- ☐ Bitcoin Wallet
- ☐ OXF

Government Accounts

- ☐ Canada Revenue Agency
- ☐ Appointment booking apps
- ☐ Student Loan Account
- ☐ My Account
- ☐ BC Services Account

Transportation apps

- ☐ Uber
- ☐ Lyft
- ☐ Taxi apps
- ☐ Waze
- ☐ Google maps
- ☐ Public transit apps

SPARK
TEEN DIGITAL DATING VIOLENCE

Shopping Apps

- ☐ Amazon
- ☐ Grocery points card
- ☐ PC Optimum
- ☐ Coffee points card
- ☐ Real Estate apps
- ☐ Account/reward apps at stores you shop at or online

Entertainment

- ☐ Spotify
- ☐ Netflix
- ☐ Crave
- ☐ Disney+
- ☐ Amazon Prime Video
- ☐ Apple Music and TV
- ☐ iTunes
- ☐ Podcast apps
- ☐ Audible
- ☐ PornHub

Gaming

- ☐ Discord
- ☐ Twitch
- ☐ Switch
- ☐ Steam
- ☐ Xbox Live
- ☐ PlayStation Network
- ☐ Origin
- ☐ Smart phone games

Health and Fitness

- ☐ Fitbit
- ☐ Apple Watch
- ☐ Distance tracking (i.e., Strava, MapMyRun)
- ☐ GPS devices (i.e., Garmin, hiking apps)
- ☐ Period or fertility apps
- ☐ Diet or calorie counters
- ☐ Medical tracking apps
- ☐ Therapy apps

Travel

- ☐ Travel points cards (i.e., Aeroplan, Air Miles)
- ☐ Airbnb
- ☐ Expedia
- ☐ TripAdvisor
- ☐ HostelInternational
- ☐ Airlines
- ☐ Trains

Smart Home Devices

- ☐ Amazon Echo
- ☐ Google Nest
- ☐ Alexa
- ☐ Siri
- ☐ Sonos One
- ☐ The Ring
- ☐ Home security systems
- ☐ Smart thermostat
- ☐ Smart lighting
- ☐ Smart lock

Smart Portable Devices

- ☐ Smart car
- ☐ GPS in car
- ☐ Bluetooth in car
- ☐ Tracking app for bike
- ☐ Tiles
- ☐ Find my phone

Education and Learning Accounts

- ☐ School email
- ☐ School online assignment platform
- ☐ Library card
- ☐ Language apps