Digital Breakup Checklist: Online Safety After Separation

This checklist is designed for frontline workers supporting survivors of tech-enabled abuse. It covers some of the main steps a survivor can take after leaving their partner to ensure their online accounts and apps are protected.

Before getting started, remind yourself of the foundational principles of survivor centered tech safety support, see The 4 Core Principles of Tech Safety.

Step 1: Identify Online Accounts and Apps

To get a complete picture of digital risks, start by working with the survivor to make a list of their online accounts. Survivors may have accounts they don't regularly use or even think about, but these can still store personal data that can be accessed by their current or former partner for abuse. Going through the list below with the survivor can help generate a complete list.

Common Account Types to Check:

- **Email accounts** (e.g., Gmail, Outlook)
    - Email accounts can be accessed to monitor a survivor's activities.
    - Check whether a survivor has multiple email accounts that they may not think of immediately. For example, do they have an old personal email that they don't use any more, or a work email?
- **Social media** (e.g., Facebook, Instagram, TikTok, Discord)
    - Social media accounts can be used to track someone's location, send harassing threats and messages, impersonate a survivor, post humiliating content, and/or monitor a survivor's activities.
    - Prompt the survivor to think about all the social media platforms they use or have used within the past few years, not just the major ones. Do they have accounts on platforms like Pinterest, Snapchat, Reddit, WeChat, etc.?
- **Banking and financial accounts** (e.g., online banking, PayPal, online shopping profiles)
    - Banking and other financial accounts can be accessed to spend a survivor's funds and open credit under their name.
- **Streaming and gaming services** (e.g., Netflix, Spotify, Xbox, Twitch, Discord)
    - These accounts can be used to make purchases with the survivor's payment methods, or an abuser could impersonate another player to get close to the survivor.
- **Health and fitness apps** (e.g., Apple Health, Fitbit)
    - These apps can be used to track a survivor's location and health data.
- **Travel and ride-share apps** (e.g., Uber, Lyft)

    - These apps can be used to track a survivor's location and when they are away from home.
- **Food delivery services** (e.g., DoorDash, UberEats)
    - These apps/accounts can be used to make purchases with the survivor's payment method or to show up at their address impersonating a delivery driver.
- **Cloud storage services** (e.g., Google Drive, iCloud, Dropbox)
    - These services can be used to monitor emails, text messages, access photos, or download suspicious apps.

Important Safety Notes

- Making sudden changes, like blocking someone, may alert them that the survivor knows they are accessing their accounts. This could escalate the risk of violence or allow them to destroy evidence.
- Consider taking steps gradually, developing a safety plan or seeking guidance before acting.
- If in immediate danger, advise the survivor to contact a support organization or emergency services.

Step 2: Secure Each Account and Device

Once accounts have been identified, guide the survivor through the steps below. Go through these steps for each account/app on their list.

1. Change Passwords Securely

- Use a strong, unique password that the abuser can't guess like "$pringIsH3r3!".
- Avoid passwords related to birthdays, pets, or other personal details.
- Use a password manager if remembering passwords is difficult.
- Don't use the same password for multiple accounts.

2. Check Password Recovery and Security Settings

Most accounts ask for a recovery email or phone number in case you forget your password. Make sure this recovery info is something only the survivor can access. If an abuser has access, they could reset the password and get into the survivor's account.

- Go to **Account Settings > Security > Recovery Options** (this varies by platform).
- Update the recovery email and phone number to one the abuser doesn't have access to.
- Update app security questions or disable security questions if the abuser may know the answers to current ones. Security questions are the pre-set questions that platforms use to verify your identity if you forget your password. Answers to security questions do not have to be real.

3. Enable Two-Factor Authentication (2FA)

Two-Factor Authentication is a way to make accounts safer. It means two steps are needed to log in—like typing in one's password and then entering a code sent to your phone or email.

- Some devices allow users to turn this feature on under **Settings > Security > Two-Factor Authentication**.
- If possible, set up a backup method like an authenticator app.
- Options include text messages, an authentication app (ex. Google Authenticator, Microsoft Authenticator), or a security key.
- If the survivor chooses to use text message or an alternate email for authentication, make sure they use a phone number or email the abuser does not have access to.

4. Review and Remove Unauthorized Devices

- For cloud accounts (iCloud, google drive), you can log out of all devices connected to cloud accounts remotely from account security settings. The survivor should log into

their iCloud or Google account and go to settings > Security > Devices or Active Sessions. Remove any unfamiliar or shared devices.

- Most social media apps allow you to see where your account is logged in. This can be found under **Settings > Security > Devices or Active Sessions**.
- Look for email forwarding rules that could send copies of messages to the abuser within email account settings. This can usually be done through **Settings > Forwarding & Filters** in email accounts.
- For accounts that can have multiple users or be shared (e.g. Netflix, Google Drive, family-sharing setups), ensure no additional users are linked to accounts.
- Check family plans for mobile carriers, Apple Family Sharing, and Google Play Family to see if there are any unfamiliar devices or accounts that are accessing accounts .

5. Turn Off Location Sharing

- On a phone: Go to the phone's **Settings > Location** and check if location tracking is enabled and turn it off if it is not needed. A survivor can also select which apps can access their location.
- For Google Users: Go to **Google Maps > Location Sharing** and disable any shared access.
- For Apple Users: Open **Find My iPhone > People > Remove Shared Contacts**.
- Social Media: Survivors can check location settings in Snapchat, Facebook, and Instagram by going to their profile and looking through account settings.
- Disable real-time tracking in fitness and ride-share apps.

6. Adjust Privacy Settings on Social Media

- Survivors should go to their account settings and set their profiles to **private** to control who sees posts and personal information.
- Remove any contacts who might share information with the abuser, even if they were once trusted. This includes mutual friends, family members, or anyone who may still be

in contact with the abuser and could give them access to the survivor's account, either directly or by sharing screenshots or updates.

- Review app permissions that allow third-party logins.
- Consider downloading social media history if it's needed for evidence through privacy settings.

For more information see Conversation Guide: Harassing and Threatening Messages.

7. Remove Saved Payment Methods in Apps.

- This can be done on most devices by going to **Settings > Payment Methods** and deleting saved credit cards or PayPal Do the same for each app such as ride-share apps, food delivery apps, and online stores.

Step 3: Plan for Ongoing Safety

After a survivor secures their accounts, encourage them to continue to monitor their digital presence:

- Regularly check for suspicious activity or login attempts through account and privacy settings.
- Set up a backup recovery method by being notified of any suspicious activity through a second email or phone number.
- Store files securely using a USB drive, password-protected folder, or trusted email account.

Survivors might not be sure if they want to go to the police or they may know they don't want to involve law enforcement right now. Encourage them to preserve evidence of any unfamiliar devices accessing their accounts, devices and apps so they have proof if they ever need it later. Here are some suggestions:

- Take screenshots or video screen record any unfamiliar devices accessing accounts, devices and apps before removal.
- Include the person's profile including phone number and any details that show who they are in evidence.
- Save and print any transactions that were made with the survivor's account without their knowledge and consent.
- Store the evidence in a safe place (a device or account that the abuser does not have access to). Back it up somewhere else, too, just in case.

Every survivor's situation is unique, and their choices should guide the response. By providing information, options, and support, frontline workers can help survivors regain financial control while prioritizing their safety.

Suggested Resources

- What is Tech-Facilitated Gender-Based Violence?
- Is Tech Abuse Hapening to You (Poster)
- Tech Safety Planning Conversation Starters
- Tech Safety Planning Conversation Starters for Anti-Violence Workers Supporting Indigenous Survivors
- Your Safety, Your Voice: Steps for a Digital Breakup
- Safety Planning Check List
- Preserving Digital Evidence Toolkit
- Digital Breakup Tool

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a larger pattern of violence that can happen both online and in person. As a support worker, it's important to let survivors know they are not alone. For guidance on addressing TFGBV, you can refer to our comprehensive techsafety.ca website.

This project was supported by a grant from CIRA's Net Good Program.