BC Society of Transition Houses

# How to Back Up and Store Your Digital Evidence

Once you have captured all of the evidence you wish to preserve, it is important to keep the saved files in a safe place. File storage options will depend on what storage methods you and your perpetrator can access. When considering where to store your evidence, it is important to assess any risks to your safety. For example, your safety may be at risk if the perpetrator still lives with you and is able to access your smartphone, uncovers saved recording, or has your login ID and password to an email address or cloud storage account where you were planning to store the evidence.

If you would like to learn more about creating a technology safety plan, connect with your local anti-violence organization (more information below) or see BCSTH's "A guide for Canadian women experiencing technology-facilitated violence: Strategies for Enhancing Safety."

## Safety Check

Before you back up and store evidence, always think through any potential risks to your safety. This is especially important if there is a risk that the perpetrator is monitoring the activities on your device.

This could be happening in several ways

- Your devices could be monitored if the perpetrator has access to your device, such as if you share a home or they have made you share your passwords with them.
- If the perpetrator knows your cloud storage ID (i.e., iCloud, Google Drive, or Dropbox) and password, they will have access to some of your files, photos and videos.
- It is also possible for the perpetrator to be monitoring your smartphone or computer via mobile spyware, such as stalkerware. If the perpetrator is monitoring your device these ways, it could alert them to you collecting evidence.

If you suspect that the perpetrator has access to your devices, accounts, or files, you will need to make a plan on how to avoid detection when collecting evidence. This is both to protect you from additional abuse and to avoid the risk of the perpetrator deleting important evidence.

Look at your account settings on your email, social media and other accounts to see what devices are connected and disconnect them from the account if it is safe to do so. You can also check to see what IP addresses are being used to look at your account. If you see an unusual IP address accessing your accounts, this may be important evidence that the perpetrator is accessing your accounts without consent.

Consider password safety and the importance of changing passwords on all relevant platforms and devices. If you have any concern that your device(s) may be infected with spyware, plan how to change

passwords without alerting the perpetrator. Anti-violence advocates will assist you with safety planning and technology use.

You may also need to consider alternative ways to preserve evidence, some of which can be found in this toolkit.

## How to Store Digital Evidence

Depending on the device you are using, video screen recordings, videos, photos, screenshots and audio recordings will automatically be saved in your photo album, gallery, hard drive or audio files.

Once you have preserved all of the information you need, keep the saved digital files in a safe place. File storage options will depend on your circumstances. For example, your safety may be at risk if the perpetrator still lives with you and is able to access your smartphone and uncovers the saved recording.

### Storing digital evidence on a device

If you cannot keep the digital evidence on your device for safety or other reasons, transfer the file elsewhere (see below) and delete the file from the device. Once deleted, remove any "recycle bin" copies made. Some devices like Apple iOS store deleted photos and videos in a "Recently Deleted" album for 30 days, or until actually removed from the device. Navigating to this album and overriding it to delete photos and videos can be an important part of a safety plan.

### External storage options

Storing digital evidence on an external storage device like a USB memory stick or external hard drive can be a good alternative to storing it on your device. This process involves transferring the recordings off of your smartphone and onto another device. This process might require specific chords and adapters to transfer the files from one device, such as a smartphone, to another, such as a computer or USB. Check your device to see what is needed to transfer files from your smartphone to an external hard drive or USB memory stick. iPhones, for example, may need specific apps and adapters to transfer files from the smartphone to the USB memory stick. Most Android devices require the same connectors as your phone uses.

> #TechSafetyTip: It is best to transfer the audio file as few times as possible in order to minimize questions about the authenticity or copying of your recording.

> #TechSafetyTip: Keep a record of the times and ways you transferred the recording from one device to another.

## Cloud storage

Storing digital evidence in an online cloud storage solution like Dropbox, Google Drive, iCloud or others can be a good option if having a physically saved copy is too high a safety risk. Even if you have a hard copy of the evidence, it is worth saving a second backup copy. This option can also be simpler than external storage options and would remove the need to purchase any other devices or adapters.

Many cloud storage providers offer free trial plans that are limited in storage. Despite being limited in size, in most cases, these services offer enough storage to preserve digital evidence.

Some example services are:

- Dropbox
- Google
- Amazon
- Pcloud
- iCloud

## Safety planning around cloud storage

Storing digital evidence in a cloud storage service can be beneficial for women[1] who are still residing with their abuser; however, there are safety risks when accessing cloud storage services that necessitate developing a safety plan for the use of this storage method.

The following are cloud storage safety planning considerations:

a. Consider whether the perpetrator has access to your cloud storage via access on his own devices or by knowing the password. If safe to do so, consider removing the abuser's devices and changing your password.

b. Do not download a video screen recording app for your cloud storage provider that connects directly to your account and/or indicates you have used such an app. The exception would be if you normally use the app for other personal reasons for example, using one for work purposes. This may alert the perpetrator that you are collecting evidence.

[1] In this toolkit we will be using the term "woman", "violence against women" and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. Women and girls face higher rates of most forms of technology-facilitated violence. They also experience some of the most serious consequences as a result of this violence. However, technology-facilitated violence impacts transgender, non-binary, male and female people. We hope that all people impacted by this violence will find these documents useful.

#TechSafetyTip: if you are using a cloud storage app for personal reasons, create a different account that the perpetrator will not know about when uploading digital evidence. Use a safe device that the perpetrator does not have access to when creating this new account.

c. Sign up for these services with an email account that the perpetrator does not have access to in order to avoid the safety risks below:

- If you share an email account with the perpetrator or they know your email password, they may be able to reset the password to the cloud storage account associated with that email to gain access to it.
- Updates from your cloud storage provider likely will be communicated via the shared email account and can signal to the perpetrator that you have another storage account.

d. Create a new email specifically for uploading your digital evidence to the cloud. There are a lot of free email account services, below is a sample of some services. As a bonus, some free email providers also offer free limited cloud storage.
   - Mail.com
   - Gmail.com
   - Outlook.com
   - Protonmail.com

e. Be cautious when accessing an email or cloud storage website with a web browser. By default, web browsers keep a browsing history. In order to safeguard your web browsing history from the perpetrator, delete your history after visiting any sources you are gathering evidence from.

f. When apps are downloaded from an app store, the history of what apps you have currently and previously installed will be assigned to your app store account. If they have access to this account, the perpetrator can login to this account and see your download history.

g. Typically, most online storage options are based in the United States and therefore, governed by US law. Despite how private you may think your cloud storage account is, there is also a possibility that US law enforcement may have access to it. Generally, this poses low risk to users, but this still must be considered.

## Decoy Apps

In many app stores, there are apps commonly referred to as “decoy apps.” These are file storage apps designed to avoid suspicion by pretending to be different apps completely.


A common example is a calculator decoy app. This app works exactly like a traditional calculator. But, type in a special code like "36x%29=", and it will open a file folder within the app to save pictures or videos.

It is important to note that files stored in the decoy app are still stored on the device, although hidden. There are ways to determine if a device contains a decoy app and if a device is being monitored by stalkerware, the perpetrator will have access to everything on your phone and will be able to see that you have a decoy app.

For more information about technology safety planning, see BCSTH's A Guide for Canadian Women Experiencing Technology-Facilitated Violence: Strategies for Enhancing Safety.

For more information about stalkerware, see BCSTH's information sheet on Mobile Spyware.

## Connect to an Anti-Violence Worker or Legal Advocate for Support

If you are unsure how to preserve evidence of technology-facilitated violence, contact an anti-violence program in your area for support and to develop a safety plan that includes technology safety considerations. Legal advocates available in BC communities may be able to assist.

BC anti-violence programs and legal advocates:

- VictimLink BC
- 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

*Technology Safety Project*

*This document is a part of a series that details how to preserve evidence related to the misuse of technology in experiences of domestic violence, sexual assault, and stalking. The series is part of the Preserving Digital Evidence of Technology-Facilitated Violence Toolkit. This document, or any portion thereof, may be reproduced or used in any manner whatsoever as long as acknowledgment to the BC Society of Transition Houses is included in the product.*

*This document was published March 2021.*

BC Society of Transition Houses

THE LAW FOUNDATION OF BRITISH COLUMBIA