BC Society of Transition Houses

How to Preserve Evidence Posted on a Website

Perpetrators can misuse websites to post non-consensual images and videos, harassing, intimidating and threatening comments and messages and create fake profiles and accounts. When technology-facilitated violence occurs, maintaining a record of events is important for criminal and civil proceedings. Posting and removing content online can occur as quickly as pressing a button or two, so it is important to be able to preserve online evidence as soon as possible.

This information sheet outlines the most common ways to preserve evidence located on a website.

It is important to collect evidence from a website immediately as it is always possible for the content of the website to be changed at any time. If you do not collect the evidence as soon as possible, it may be lost or changed.

Safety Check

Before you capture online 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 mobile device. This could be happening in several ways:

- Your smartphone 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 that you are 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 the account. An unusual IP address may indicate someone is 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 can support you to create a safety plan when using technology.

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

Options to Capture Evidence on a Website

Video Screen Recording

One of the easiest methods of preserving digital evidence on a website is to record a video of the website on your smartphone.

How to enable video screen recording on your smartphone is outlined in BCSTH's Preserving Digital Evidence for Court Using Video Screen Recording information sheet. That sheet shows you how to video screen record on an Apple iOS and an Android smartphone.

If you do use video screen recording to capture evidence found on a website, you will have to make sure that you can play the recording in court. You will first have to save your recordings onto a USB memory stick, CD or DVD, depending on the equipment available to you or the court you are presenting the evidence in. Equipment that can play your recordings is also necessary.

You should ask the court ahead of time what equipment they have available for you to use to play your recording. You may be able to request certain equipment (for example, large screen monitors) from the court using an Equipment Request Form. However, courts may not always have the equipment you need so you may have to bring your own equipment to court (i.e., a laptop). If you know that you will not have access to the equipment needed to play a video screen recording, you should also consider using a printout of a screenshot or PDF file instead and present that to the court.

Screenshots

If your smartphone doesn't have the capacity to record video by screen recording you can take a screenshot or series of screenshots of the website and the pages you would like to preserve. BCSTH information sheet, How to Save and Print a Screen Shot for Evidence, applies to both smartphones and computers.

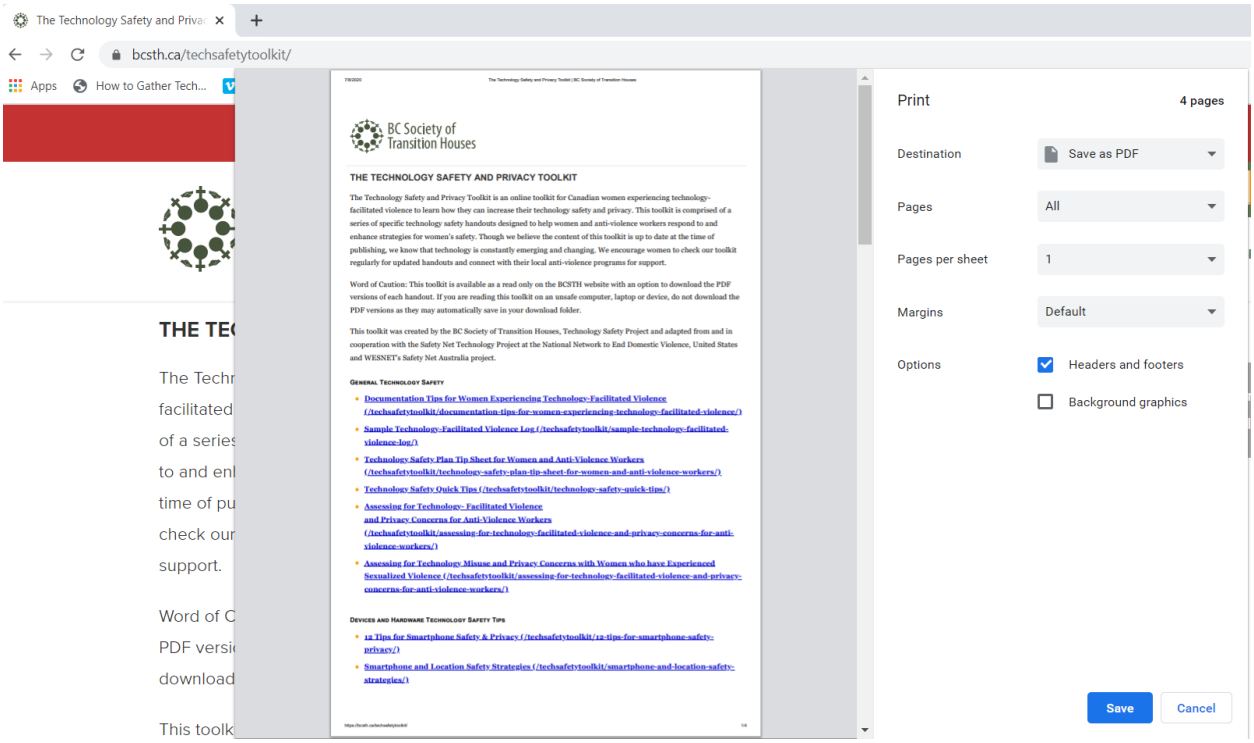
Print To PDF

It is possible to save a copy of a website and the webpages you want to preserve as a PDF file. From your laptop or computer, open the page of the website you want to save as a PDF. Depending on the browser you are using, select the "Print" option that works for your browser. This can be done by either:

- Selecting the Print option on your web browser, or
- Right click on the webpage and select Print, or

- Hold down the “Ctrl” and “P” keys at the same time until the print screen appears.

Once your print screen appears, select the option to “Save as a PDF” in the printer or destination box.



Make sure you select the “Headers and Footers” option if it’s available so the PDF file will include the website link and date on the document you want to save.

Once the website has been converted to a PDF, you can choose to save the file in a safe location and/or print the document for your records. You will want to double check the PDF to make sure it properly saved the information from the website. Saving a PDF through the print function does not always capture the entire website.

Other options:

a. Built-in software in iOS Safari: using “Markup” saves your entire loaded page as PDF
b. Firefox on Android has a save to PDF option

Printing

If you are preserving evidence on a website, it is best to save a copy for your records in case the printed copy gets lost or stolen or the information on the website is deleted. To print a copy of the website you can:

- Print the screenshot
- Print the webpage
- Print the PDF

HTML (HyperText Markup Language)

It is recommended that you capture the HTML of a webpage with a screenshot. This is because the HTML language contains the source files which shows that someone uploaded a file to the website. A screenshot of the HTML of the website (before downloading) is a good backup - as the HTML file could have broken parts when saved locally. Incomplete screenshots of the HTML webpage may cause issues presenting the evidence in court.

Generally, from a desktop or laptop computer, you can retrieve the HTML of a website from File or right click directly on the webpage -> Save As -> Webpage -> Complete.

Tips for Preserving Website Information

1. Capture the Entire Website

Many self-representing litigants will capture an offending message, comment or photo rather than the entire web page. As some courts will not accept just a portion of the webpage, it is always best to capture the entire webpage. To do this, you may need to take multiple screenshots or print multiple pages to capture an entire post with comments and identifying information. You may need to expand comments to ensure you are capturing all of the information.

Make sure to include the URL of the website and the time and date the capture of the webpage was taken.

2. Get Supporting Evidence

Screenshots of a webpage may be adequate for some courts. However, this type of evidence may not always be sufficient. Consider if there is any accessible supporting evidence available to you. For example, if you are trying to capture a post on Facebook, supporting evidence might be found in your Facebook data which can be accessed through their Download Your Data Feature.

3. Include Perpetrator Information

Social Media Sites:

On a social media platform like Instagram, Facebook, SnapChat or Twitter, capture the following:

- photo(s) of the account of the person who wrote, sent or posted the harassing photo, image or comment,
- the profile of the person who sent wrote, sent or posted the harassing photo, image or comment,
- the person's profile URL,
- image or message that is harassing,
- any comment(s) that are harassing or threatening, and
- the date and time of post.

Websites:

Websites can come in many different forms. They can also have less identifying data if they are not a social network with profiles. Anonymous posting websites can be particularly challenging to collect information about people uploading content. In these cases, legal action against the site to disclose their data or data on their users might be necessary. Collect all information you can see from pages that concern you, using screenshots, videos, and other tools discussed in these resources.

Authentication

Since you will be presenting printouts or screen recordings of websites and not a live version of the website itself, the authenticity of your printouts or screen recordings may be contested. If this is the case, you will have to authenticate your printouts. BCSTH has more information about authentication in our Authentication of Digital Evidence for Protection Order Matters in BC Family Court or BC Civil Courts information sheet.

Safety Reminder

Your safety is important. If you think the perpetrator may become more abusive if your preserved evidence is discovered, consider asking a friend to capture the website on their own phone or computer and save it for you for court. However, make sure the friend knows that capturing the evidence could mean that they may have to go to court to testify as a witness for your case as to the steps they took to preserve your evidence.

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

Adapted with permission from the National Network to End Domestic Violence's Safety Net project, based on their Legal Systems Toolkit.