BC Society of Transition Houses

Preserving Emails as Digital Evidence

Email messages, whether accessed through a computer or a mobile device, are a common form of communication. In many family law agreements, courts routinely order email communications as a means of "safe" communication between parties, as it leaves a written record. However an abusive (ex) partner can misuse email by sending harassing messages, gaining unauthorized access to your email, creating fake email addresses in order to monitor or impersonate you, or sending computer viruses or spyware via emails. Email evidence can be used to strengthen contested cases by providing proof of abuse and to present a picture of the abusive relationship and domestic violence.

Safety Check

Before you capture email 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 be able to assist you to create a safety plan while using technology.

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

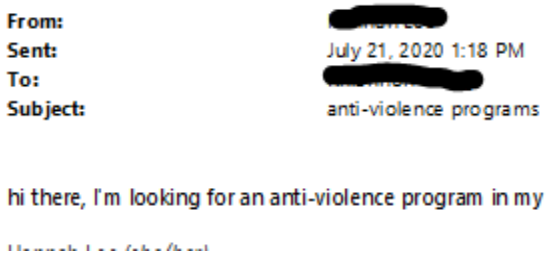
©2021 BC Society of Transition Houses, Technology Safety Project

Email Evidence: The Digital Trail

While email evidence can be extremely useful, it is not always properly preserved, and it can get accidentally deleted or have its authenticity questioned. Admitting email evidence generally requires showing that an email is relevant to your case and that a specific person authored and/or sent it.

What to Include in Email Evidence

1. **The email message**. You can print out the email, which will show the *To, From, Date, and Subject* information. A printed email will also show the file name of any attachments. When printing an email, it can change how the email looks which can make it harder to admit in the email in court. If the email changes when you print it, you might want to take a screenshot and then print the screenshot instead.



2. **The header**. What you see in an email is often not all of the information available in that email. A lot of information is hidden in what is called the "header." Specifically, the header has information about the IP address (an individualized code that can help to show who sent an email). When printing emails for court, make sure to print the email with the email header. To find how to print emails with headers do an online search for "*How to print email header in [name of email provider (e.g. Outlook, Gmail, etc.)]"* and follow the instructions.

   Email headers might open in a text editor or browser window. Saving the digital file to a readable file format (such as .txt, .doc, or .pdf) is recommended for preservation of data. Below is an example of an email header from a Microsoft Outlook email address.

```
Received: from QB1PR01MB4020.CANPRD01.PROD.OUTLOOK.COM (2603:10b6:b01:2f::19)
 by YTBPR01MB2544.CANPRD01.PROD.OUTLOOK.COM with HTTPS via
 YT1PR01CA0140.CANPRD01.PROD.OUTLOOK.COM; Tue, 21 Jul 2020 20:18:08 +0000
Authentication-Results: bcsth.ca; dkim=none (message not signed)
 header.d=none;bcsth.ca; dmarc=none action=none header.from=bcsth.ca;
Received: from QB1PR01MB2817.CANPRD01.PROD.OUTLOOK.COM (2603:10b6:c00:39::29)
 by QB1PR01MB4020.CANPRD01.PROD.OUTLOOK.COM (2603:10b6:c00:3d::13) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3195.17; Tue, 21 Jul
 2020 20:18:07 +0000
Received: from QB1PR01MB2817.CANPRD01.PROD.OUTLOOK.COM
 ([fe80::6046:b41d:8028:777d]) by QB1PR01MB2817.CANPRD01.PROD.OUTLOOK.COM
 ([fe80::6046:b41d:8028:777d%5]) with mapi id 15.20.3216.020; Tue, 21 Jul 2020
 20:18:07 +0000
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Hannah Lee <hannah@bcsth.ca>
To: Rhiannon Wong <rhiannon@bcsth.ca>
Subject: anti-violence programs
Thread-Topic: anti-violence programs
Thread-Index: AdZfnATTjP+9LXXtRZmYozy2FTU48Q==
Date: Tue, 21 Jul 2020 20:18:07 +0000
Message-ID:
<QB1PR01MB2817A5C3F3A5CBA771B65BF1B8780@QB1PR01MB2817.CANPRD01.PROD.OUTLOOK.CO
M>
Accept-Language: en-CA, en-US
Content-Language: en-US
X-MS-Has-Attach:
```

3. **The IP address.** Once you have the printed email header, look for the "received" IP address. It will be a long code. You can take that code and enter it into an IP address search on an online search service. Generally, it will provide you a map that shows where an email was sent from. This will not work with all emails, but it will work for many emails.

   Note: Tracking an IP location will only narrow the location down to a specific city, not an exact address, (a warrant is needed for exact locations). Additionally, IP addresses can be easily masked so it might not actually help you identify who sent the email.

4. If you are receiving email from someone using a fake email address, what is written in the email may help indicate who sent it. If you have multiple emails from one fake email address, you can print all of them to help show that the different emails are from one person by establishing a common pattern, theme or word/sentence/phrase choice in the communication.

5. If you want law enforcement to investigate your emails as evidence in a criminal case, it is important that you don't delete or forward the emails. You should keep the original email messages in the email account for clarity.

Printing and Submitting Email Evidence to Court

You can print out the email, showing the:

- To
- From
- Date
- Subject information.
- File name of any attachments

You can also include the header if you're able to.

Print all the emails of the same conversation or "Subject." Most courts will want to see the entire conversation thread, not just one "reply" to a larger conversation. It may be helpful to start new email conversations or "Subjects" for separate conversations instead of replying to the same email thread for long periods of time.

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.

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

BC Society of Transition Houses

THE LAW FOUNDATION OF BRITISH COLUMBIA