

Preserving Emails as Digital Evidence

Compiled by Tech Safe BC



Last Updated: February 5, 2026

Email is a common way people communicate, including in family law matters where courts often ask parties to use email because it creates a written record.

But current/former partners can misuse email by:

- Sending harassing or threatening messages.
- Accessing your email without permission.
- Creating fake email accounts to impersonate or monitor you.
- Sending harmful attachments, spyware, or viruses.

Saving copies of abusive emails can help show a pattern of behaviour and support your case in criminal or civil court. **If something in this guide is no longer up to date, or you have any questions, please reach out to techsafe@bcsth.ca with your concerns.**

Safety Check

Before saving emails, think about whether it is safe to do so.

Saving emails may alert your current/former partner if they are monitoring your device or accounts. This could happen if they:

- Have physical access to your phone or computer.
- Know your passwords.
- Can access your cloud storage ([iCloud](#), [Google Drive](#), [Dropbox](#)).
- Have installed spyware or Stalkerware.

If you think your device or accounts may be monitored, make a plan to collect evidence safely. This helps prevent further harm and reduces the chance the abusive person could delete important evidence.

See [Safely Preserving Digital Evidence of Technology-Facilitated Violence](#) and consider reaching out to an [anti-violence worker](#) for support.

Understanding Email Evidence

Courts generally require that email evidence:

1. Is relevant, and
2. Can be connected to the person who sent it.

Emails can be deleted or altered, and sometimes printed emails look different than what appears on your screen. The tips below help you save a clear, complete record.

What to Include When Saving Emails

1. The Email Message

You can save an email by:

- Printing it on paper, or
- Using “Print to PDF” to save a digital copy.

A printed or PDF email usually shows:

- To
- From
- Date and time
- Subject line
- Attached file names

If printing changes how the email looks or cuts off information, take a [screenshot](#) of the email and print the screenshot instead.

2. The Email Header

An email header contains hidden technical information, including when and where the email travelled across the internet. This can sometimes help show who sent it.

To save a header:

1. Look for an option like “View original,” “Show details,” or “View full header.”
2. Print or save the header as a readable file like .txt, .doc, or .pdf.

How to print a header depends on the email provider.

Try searching online for: “How to print email header in [Gmail/Outlook/Yahoo/etc.]”

3. The IP Address (Optional)

Inside the header you may see a “Received” line with an Internet Protocol (IP) address. An IP address can sometimes show the general location where an email was sent (usually a city, not a home address).

Important notes:

- This will not work for all emails.
- IP addresses can be easily hidden or masked.
- You cannot find an exact address without a warrant.

IP information is optional and may or may not help your case.

4. Evidence Showing Who Sent the Email

If someone is using a fake email address:

- Save every message they send.
- Look for patterns such as writing style, spelling, phrases, or tone.
- Save examples of past messages from the person you believe is responsible, if they show similar patterns.

These similarities can help show that the same person is behind the messages.

5. Keep the Original Email in Your Account

If you want police to investigate, do not delete the original email. Law enforcement needs to see the email as it originally appeared.

6. Save the Entire Thread

Courts often want to see the whole conversation, not just one reply.

Try to:

- Print or save the full thread.
- Start a new Subject line when conversations change, so threads stay organized.

Safeguarding Email Evidence

Once you save your emails:

- Keep copies in a safe location.
- Consider storing a backup on a USB stick, external hard drive, or another secure device.
- Choose a storage option that fits your situation and safety needs.

For more guidance, see [Safely Preserving Digital Evidence of Technology-Facilitated Violence](#).

If you are experiencing tech abuse, you are not alone. Find support in your community by connecting with a [BC Society of Transition Houses Member Program](#) or check out our other safety resources at techsafebc.bcsth.ca.

©BC Society of Transition Houses, Tech Safe BC Project, 2026. We encourage others to share this material, provided BC Society of Transition Houses is acknowledged.