

Preventing Harassment and Threats through E-Transfers



An e-Transfer is a way for people in Canada to send money to someone with a bank account at a participating bank, using online or mobile banking.

This service, offered by Interac, is quick and convenient—but it can also be misused by abusers to harass or threaten a current or former partner.

This resource provides tech safety strategies for survivors experiencing harassment and threats through Interac e-Transfers.

How Interac e-Transfer Services are Misused to Abuse

Survivors have shared <u>how abusers misuse Interac e-Transfers</u> to harass, threaten, and withhold court-ordered support payments.

Common tactics include:



Withholding the security password or using a harmful security question and password to receive funds.

For example, an abuser may create a threatening security question like "Who am I watching 24/7?" or "Who is the worst mother in the world?" then setting the answer to the survivor's or their child's name to instil fear. An abuser may also withhold the security password or give the survivor the wrong password, so they are forced to keep contacting her abuser.



Setting the recipient's name to something harmful.

An abuser may change the survivor's name within their account settings to something inappropriate like "worstmomever" to intimidate or cause emotional harm to the survivor every time she gets an e-Transfer notification.



Sending abusive messages in the "Optional Message" text box.

When setting up an e-Transfer, the sender can include an optional message. Abusers are misusing this function to send harassing and threatening messages to survivors, such as: "This is the last support payment you're ever getting from me. I don't care what the court says. You just wait; I'm coming for you."

This example may be particularly harmful and likely if the survivor has blocked their abuser from other platforms but still receives e-Transfers related to support payments.



Sending repetitive e-Transfers for as little as \$0.01.

Abusers may also send repetitive e-Transfers for as little as \$0.01 to take advantage of the "Optional Message" feature and send a series of harassing and threatening messages.

This is common with abusers who have been blocked from contacting the survivor through other technology and online platforms as they only need to know a survivor's e-mail address to do this.

Securing Your Account

If you are experiencing harassment through Interac e-Transfers, know that there are steps you can take to protect yourself. Taking the time to secure your e-Transfer account can help minimize the abuse enacted through Interac's e-Transfer platform.

Here are some options:

- Enable auto deposit to avoid being forced to answer security questions.
 This prevents an abuser from using this feature to harass you or force contact. Set it up in your online or mobile banking under Interac e-Transfer settings.
- Change your e-Transfer email if you no longer need to receive funds from the abuser. Use a new, private email and create it on a safe device.
- Opt-Out feature:

As of March 6, 2025, <u>Interac will allow all users to set</u>
 <u>communication preferences for each sender</u>. Survivors can use this feature to avoid receiving abusive messages.

What to do After Receiving a Harassing or Threatening Message through e-Transfer

- <u>Preserve</u> and <u>document evidence</u> by taking a <u>screen shot</u>, <u>video screen</u> <u>recording</u> or printing the page.
 - This will ensure that you have proof of the harassment or threat. Banks do not usually have access to this information, so it's important to save your own records in case they are needed for court or police reports
- Contact a <u>local shelter or anti-violence organization</u> to discuss options and develop a <u>safety plan</u>.
- Call your bank and let them know that you are experiencing
 harassment and threats through e-Transfers. Ask them to add the
 specific dates and times to your file. The abuser may be violating the
 bank's terms of service around the use of e-Transfers and could be held
 accountable by the bank.
- Report the harassing messages and threats to the police and share
 your evidence. The abuse and harassment you are experiencing is a
 crime. Be sure to ask for a file number for your reference.

Abusers should not be able to misuse financial tools to cause harm. Securing your account, preserving evidence, and seeking support from local antiviolence organizations or law enforcement can help you navigate this situation safely. Financial abuse is a serious issue, and you are not alone—support is available to help you regain control and security.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support. For more information about digital financial abuse, see our full Digital Financial Abuse Toolkit.

This resource was funded by Interac.