

Digital Financial Abuse and Phishing

Scam Resources



Phishing scams are when criminals use deceptive tactics to trick individuals into revealing personal or financial information or clicking malicious links. Scams are commonly received through text, email, and phone calls.

Common tactics include:

- Sending an email pretending to be a person or website.

- Telling someone they need to send money or provide financial information right away or else someone they love will be hurt, they may lose all their money, or their account will be closed.
- Offering refunds or money to be paid to you with cryptocurrency.
- Making seemingly harmless requests to click links, scan QR codes, download attachments, or fill out online forms.

Phishing messages often appear to come from legitimate institutions, such as banks, subscription services, businesses, or government agencies, and typically prompt the recipient to take immediate action under false pretenses, such as updating account information or claiming a refund.

Variations of phishing scams may involve minimal text and appear as receipts, delivery notifications, or urgent notices; these are designed to infect a device with malware or viruses when links or attachments are clicked.

It can be challenging to identify these kinds of scams. Here are some additional resources that may be helpful for survivors experiencing other forms of digital financial abuse.

Rental Scams

Due to the lack of affordable housing, scams of fake rental properties are common. See the RCMP's [Rental Scam webpage](#) for more information and tips to help.

Scams via Email

We all get emails claiming we inherited money, someone has tried to access our accounts, or that a third party has intimate images of us. Here are some resources on identifying scams and what to do if you receive them:

- [How to Spot Email Fraud and Scams](#)
- [What to do if a scammer has your email address - 8 tips](#)
- [Don't take the bait: Recognize and avoid phishing attacks](#)

Scams via Text

Phishing scams through text messages and messages through apps like WhatsApp usually start with trying to engage you in conversation.

You might see texts from an unknown number saying:

- "Is this a good time?"
- "Your bill payment didn't go through."
- "We could not deliver your parcel."
- "CRA needs more info."

Scammers may also pretend to be from a company or government office, asking you to follow up on a package or document.

The following resources share how to identify scams and what to do if you receive them.

- [What to do if you receive a spam text](#)
- [How to stop spam texts: An easy 4-step guide](#)
- [Hung up on mobile spam?](#)

Scams via Phone Call (Robo Call)

Scams through phone calls try to trick you into thinking that an urgent matter needs to be discussed to keep you on the phone. Common scams via

phone calls often involve stories about kidnapping and the need for banking information.

- [How to protect yourself from scammers and how to avoid unwanted calls](#)
- [Protecting yourself from telemarketing and retail scams over the phone](#)
- [Register with the National Do Not Call List](#)
- [Blocking and filtering unwanted calls](#)

Scams Posing as the Canadian Government

Here is a link to a document by the Government of Canada on recognizing scams from services and what to do if you receive them.

- [Identify scams related to government services](#)

For more tech safety tips, check out our resources:

- [What to Do if You're a Victim of Fraud](#)
- [6 Tips for Securing Your Online Financial Information](#)

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 project was funded by TD Bank Group, through its corporate citizenship platform, the TD Ready Commitment.