



CANADIAN ANTI-FRAUD CENTRE CENTRE ANTIFRAUDE DU CANADA

Cryptocurrency Wallet Fraud

2026-08-05

FRAUD: RECOGNIZE, REJECT, REPORT IT LA FRAUDE: IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

The Canadian Anti-Fraud Centre (CAFC) wants to warn Canadians about frauds targeting people who own or use cryptocurrency wallets. Fraudsters may try to gain access to a wallet, steal cryptocurrency, or trick victims into sharing private information.

Cryptocurrency transactions are difficult to reverse. Once cryptocurrency is sent or stolen, it may be difficult or impossible to recover. People who have already lost cryptocurrency may also be targeted again by fraudsters who claim they can recover the funds.

Cryptocurrency wallet fraud and recovery phrases

A cryptocurrency wallet is used to access and manage cryptocurrency. Some wallets are applications on a phone or computer. Others are physical devices.

Many cryptocurrency wallets use a list of 12 or 24 secret words. This is called a **recovery phrase** or **seed phrase**. It works like a master key and can be used to restore the wallet and control the cryptocurrency inside. Anyone who gets the recovery phrase may be able to access the wallet and transfer the cryptocurrency. They may not need the victim's phone, computer or physical wallet device.

Fraudsters may try to get this information through fake websites, emails, text messages, telephone calls, letters, QR codes or harmful software. They may claim there is a problem with the wallet and that immediate action is needed.

A recovery phrase should never be shared. A police service, government agency, financial institution, wallet provider or legitimate support service will not ask you to send it by email, text message, social media, online form or letter.

Recovery fraud

People who have lost cryptocurrency may be targeted again through recovery fraud.

In this type of fraud, a fraudster claims they can find, unlock or return stolen cryptocurrency. They may pretend to be a:

- Police officer or government employee
- Lawyer or investigator
- Cryptocurrency expert
- Wallet or exchange employee
- Representative of a recovery company
- Victim who claims to know how to recover the funds

Fraudsters may contact victims by telephone, email, text message, social media or a letter in the mail.



Royal Canadian Mounted Police
Gendarmerie royale du Canada



Competition Bureau
Canada

Bureau de la concurrence
Canada



Ontario Provincial Police

Canada

They may already know some information about the victim, such as the amount lost, the type of cryptocurrency involved or a public wallet address. They may use these details to appear legitimate and ask the victim for information they are missing.

They may request personal information, identification, financial details, wallet information or an upfront payment. Knowing some correct information does not prove that the person or organization is legitimate.

Warning signs

Beware of anyone who:

- Contacts you without being asked about your cryptocurrency or wallet
- Claims your wallet has been hacked, frozen or placed at risk
- Says they have found your stolen cryptocurrency
- Promises or guarantees that lost funds can be recovered
- Asks for your recovery phrase, private key, password, PIN or security code
- Asks you to confirm personal or financial information
- Sends a link or QR code and asks you to connect or verify your wallet
- Tells you to transfer cryptocurrency to a “safe,” “secure” or “protected” wallet
- Asks you to install software or provide remote access to your device
- Requests an upfront recovery, legal, tax, insurance or processing fee
- Pressures you to act quickly or keep the matter secret
- Tells you not to contact police, your financial institution or family members

How to protect yourself

- Never share your recovery phrase or private key.
- Keep your recovery phrase in a private and secure place.
- Do not store it in an email, cloud account, online document or photograph.
- Use strong and unique passwords.
- Turn on multi-factor authentication when available.
- Keep wallet devices, applications, phones and computers up to date.
- Download software and updates only from official sources.
- Check website addresses before entering information.
- Do not click links, open attachments or scan QR codes in unexpected messages.
- Do not allow an unknown person to remotely access your device.
- Never transfer cryptocurrency to a wallet provided by someone who contacts you.
- Do not pay anyone who promises to recover lost cryptocurrency.
- Do not provide personal, financial or wallet information through unexpected correspondence.
- Find an organization’s official contact information yourself and contact it directly.
- Slow down and verify all requests before taking action.

Anyone who suspects they have been the target of cybercrime or fraud should report it to their local police. Also visit the [Report Cybercrime and Fraud](#) website to report online or by phone at 1-888-495-8501.