01 / HELP WITHOUT BLAME

PINDAB SCAM RECOVERY GUIDE

Being scammed does not mean you are stupid.



Someone chose to deceive you. You deserve help and respect - not a lecture.

Stop the contact. Protect your money and accounts. Get support. This Canadian youth guide helps you take the next step, even if you are unsure what happened.

If money or banking access is at risk, contact your provider immediately through its official app, website, card number or branch. Do not wait to finish this booklet.

02 / START HERE

You do not have to fix everything at once.

Start with what is at risk now. You can ask a trusted person to work through these steps with you.

01 STOP replying

End the call or chat. Do not argue, negotiate or warn the suspected scammer.

02 DO NOT send more

No extra fees, gift cards, crypto, passwords, codes or identity photos.

03 CONTACT the provider now

If money or access is affected, call the bank, card issuer or payment service through an independently verified channel.

04 SECURE affected accounts

Use a trusted device. Change exposed passwords and reused ones; follow the provider’s recovery steps.

05 SAVE what you can safely

Keep messages, usernames, receipts and transaction references. Do not delay urgent bank contact to collect everything.

06 REPORT, then block

After preserving accessible evidence, report the profile, ad or listing using the platform’s own tools. Block further contact.

07 TELL a safe, trusted adult

Choose someone who can help calmly: a caregiver, youth worker, teacher or counsellor.

08 REPORT in Canada

Victims should contact local police and report to the Canadian Anti-Fraud Centre. Page 7 gives verified routes.

If someone is in immediate danger, call 911. For non-emergency fraud reporting, use the local police service’s official reporting route.

03 / MONEY OR BANKING ACCESS AFFECTED

Call the bank or payment provider now.

Use an official route

Open the genuine app, use the number on your card, or independently find the institution’s website. Do not use a number or link supplied by the suspected scammer.



Tell them exactly what happened

Explain the payment type, date, amount and whether you sent it yourself, shared access or saw activity you did not authorize. Being precise helps them choose the right process.

Ask about immediate options

Can they stop a pending payment, secure access, replace a card or start an investigation? Ask for the next step, applicable deadline and case number.

E-TRANSFER / ACT QUICKLY

You may be able to cancel before the money is deposited. Once deposited, an Interac e-Transfer cannot be cancelled by the sender. Contact your own institution about suspected fraud regardless; do not assume a report guarantees a refund.

WORDS YOU CAN USE

“I think I have been scammed. I [sent a payment / shared access / noticed an unauthorized transaction] on [date]. Please help secure my account and explain what can be done about the payment.”

Card, e-transfer, gift-card and other payment routes differ. Contact the relevant issuer or service promptly. Keep the answer and follow-up date; no refund is promised.

04 / PASSWORDS, CODES OR DEVICE ACCESS

Secure access from a trusted device.

Use the real recovery process

If locked out, go directly to the provider’s official account-recovery page. Do not pay someone in a message to unlock it.



Change exposed and reused passwords

Secure affected email as well, especially if it can reset other accounts. Choose strong, unique replacements that meet the service’s rules.

Check who still has access

Review signed-in devices, recovery email and phone details. Sign out unfamiliar sessions and revoke suspicious access where offered. Enable multi-factor authentication.

SHARED A CODE OR BANK LOGIN?

Contact the bank immediately, even if nothing seems missing yet. A new password alone may not secure every session, card or recovery setting. Tell support what you shared; never write the secret itself here.

ALLOWED REMOTE ACCESS TO A DEVICE?

Stop the session and disconnect that device from the internet. Use another trusted device or phone to contact your bank and legitimate technical support. Do not enter replacement credentials on a device that may still be compromised.

A trusted adult or youth worker can help you follow the official instructions without needing your PIN, password or one-time code.

05 / KEEP THE RECORD SAFELY

Save evidence without staying in contact.

CAPTURE WHAT IS ALREADY ACCESSIBLE

Screenshots of messages, profile or ad, username, website address, dates, receipts, payment amount and transaction reference. Keep original messages or files when safe; names and profiles can change.

KEEP CONTEXT, NOT JUST ONE LINE

A short timeline helps: what was offered, what you were asked to do, what you sent or shared, and when you noticed the problem. You can write “not sure” rather than guess.

DO NOT TAKE EXTRA RISKS FOR PROOF

Do not reply to get a confession, reopen a suspicious link or download an attachment. Do not publish private screenshots. Give originals to verified services through their secure process.

A quick evidence list

- ☐ Message / profile / advertisement saved safely
- ☐ Transaction details and receipt saved privately
- ☐ Short timeline started / unknown details marked
- ☐ Bank, platform and police reference numbers kept

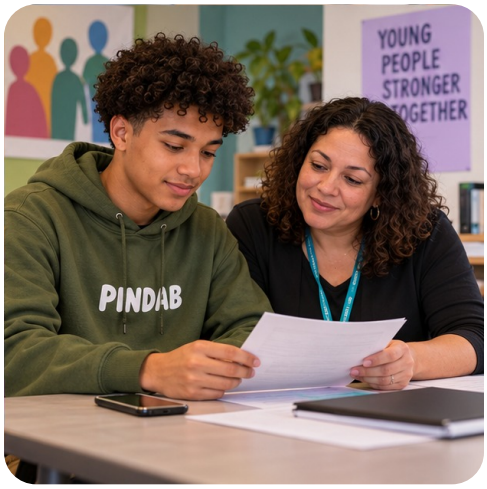
Never record PINs, passwords, one-time codes, SINs or full account/card numbers on these worksheets. Evidence collection must not delay urgent bank contact.

06 / REPORT THE ACCOUNT OR AD

Report on the platform. Then block.

Save accessible identifiers first

Keep the profile handle, listing or ad link and relevant messages if safe. Reporting or blocking can make some material harder to find later.



Use built-in reporting tools

In the genuine app or website, choose Report profile, Report ad, Scam/Fraud or the closest option. Describe the conduct briefly and keep any confirmation.

Block and stop checking the thread

Do not negotiate a refund with the suspected scammer. If they return from another account, do not re-engage; preserve new threats safely and report them.

A PLATFORM REPORT IS ONE PART

It may help the platform review or remove content, but it does not replace contacting the payment provider, local police or the Canadian Anti-Fraud Centre. Removal, investigation and repayment are different outcomes.

WORDS YOU CAN USE

“This account or advertisement appears to be involved in a scam. It requested [payment or information] for [claim]. The relevant date is [date]. I have kept the messages and transaction reference.”

Report through official tools, not a “support agent” who messages you privately. You do not need to keep talking to the account to complete a report.

07 / WHERE TO REPORT IN CANADA

Different contacts do different jobs.

BANK / CARD ISSUER / PAYMENT PROVIDER

For money sent, unauthorized activity or exposed banking access, contact the relevant provider immediately using a verified official channel. Ask about security, payment status, disputes and follow-up.

LOCAL POLICE / report a crime

If you were a victim, contact your local police service through its official non-emergency reporting route. Ask how to submit evidence and keep the occurrence or report number. Call 911 for immediate danger.

CANADIAN ANTI-FRAUD CENTRE / national reporting

1-888-495-8501
Online: reportcyberandfraud.canada.ca

Victims and witnesses can report. The CAFC collects reports to assist law enforcement; local police investigate. Reporting does not automatically recover money.

IF IDENTITY INFORMATION WAS EXPOSED

Contact affected organizations and the issuer of compromised ID through official channels. If identity fraud is suspected, ask Equifax and TransUnion about fraud alerts and checking your file. For youth, ask how their process applies at your age.

Not sure it was a scam? You can still contact the bank for guidance and report a suspected attempt. Do not wait for a complete evidence package.

08 / YOU DESERVE SUPPORT

Tell someone who can help without blame.



Being scammed does not mean someone is stupid.

Scams use pressure, impersonation and trust. Responsibility for deception belongs to the scammer. Feeling embarrassed does not mean you did anything to deserve it.

CHOOSE A SAFE ADULT

A parent or caregiver, relative, teacher, counsellor, coach or youth worker can help. If one person is unsafe or dismissive, choose another. You do not have to disclose private household finances to ask for support.

WORDS YOU CAN USE

“Something happened online and I think it was a scam. I am worried about being judged. Can you help me contact the bank, save what matters and work through the next steps calmly?”

A supportive response sounds like this:

“Thank you for telling me. You are not stupid. Let’s focus on what we can do next. Would you like me to sit with you while you call?”

09 / PRACTISE THE NEXT MOVE

Three situations. No blame. Clear actions.

These fictional Canadian examples are about responding, not testing who should have known better.

A / THE $85 MARKETPLACE DEPOSIT

An item never arrives and the seller demands another $25 “release fee.”
Next move: stop contact and do not pay more. Contact the payment provider now, preserve the listing and receipt safely, then report the account and block. If victimized, report to police and the CAFC.

B / THE FAKE BANK TEXT

You entered a banking password and one-time code into a linked page.
Next move: contact the real bank immediately using a verified channel. From a trusted device follow its security instructions, secure exposed email and reused passwords, and save the text without reopening its link.

C / THE “RECOVERY EXPERT”

After a scam, someone promises to return your money if you first pay $120.
Next move: do not pay or share access. Verify any claimed agency independently. Save the message safely and report it. Even official-looking accounts can impersonate a real organization.

What would make asking for help easier?

You can use a fictional answer. You never have to share a personal scam experience to use this guide.

10 / PRIVATE RECOVERY RECORD

One place for the next step.

Use short notes and account nicknames. Keep sensitive evidence separately and share it only through verified secure channels.

What happened / when I noticed / what is still uncertain

Payment type / date / amount / reference nickname

Information or access exposed - type only, never the secret

Who I contacted / date / case or occurrence number

Action agreed / deadline / follow-up date

Platform and CAFC report status / trusted support person

Do not put passwords, PINs, one-time codes, SINs or full account/card numbers here. Avoid including someone else’s private information. Keep this record somewhere safe.

11 / CHECK BACK, WITHOUT BLAMING YOURSELF

Recovery can take more than one step.

Money and access

Check recent transactions using the genuine app. Report new suspicious activity promptly. Confirm the provider’s follow-up date and ask whether further security steps are needed.

Accounts and identity

Review recovery contacts, signed-in devices and any affected email. If identity information was involved, follow the relevant issuer’s and credit bureau’s guidance.

Evidence and reports

Keep reference numbers and new replies together. Send updates through verified channels. Ask the bank or police what else they need; no outcome is guaranteed.

Support and breathing room

Ask someone you trust to help with calls or forms. Take breaks from messages. You can feel upset and still take one useful step at a time.

WATCH FOR A SECOND SCAM

Do not send “recovery money.” Independently verify anyone claiming to be a bank, police officer, CAFC employee or investigator. The CAFC does not ask individuals to send money.

12 / VERIFIED CANADIAN RESOURCES

Use the official route, not a message link.

CAFC / What to do after fraud

https://antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-eng.htm

CAFC / How to report fraud and cybercrime

https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm

National online reporting portal

https://reportcyberandfraud.canada.ca

Get Cyber Safe / Recovering a hacked account

https://www.getcybersafe.gc.ca/en/blogs/recovering-hacked-account

FCAC / Protect financial information after a breach

https://www.canada.ca/en/financial-consumer-agency/services/protect-financial-information-data-breach.html

Interac / Consumer frequently asked questions

https://www.interac.ca/en/resources/personal-resources/personal-faq/

CRTC / Scam response and remote-access concerns

https://crtc.gc.ca/eng/phone/telemarketing/fraud.htm

CAFC / Recovery-pitch scams

https://centreantifraude.ca/scams-fraudes/recovery-recuperation-eng.htm

Checked October 24, 2026. Reporting routes and service procedures can change. The right process depends on the payment, account and circumstances. This guide does not promise a refund or an investigation outcome.

PINDAB provides educational resources and is not affiliated with these organizations. The people and practice situations are fictional. Reprint the checklists whenever helpful.