

Think Smarter About Scams

A practical North American family guide

By Kit Harlow



Pause. Check independently. Get help together.

For teens, parents, grandparents and anyone they trust. Younger children can read the examples with an adult.

Review edition v02 | 19 September 2026

For families across North America, with country-specific reporting resources. Scenarios and messages are fictional teaching examples. Brand names identify organizations being impersonated; this guide is independent and not endorsed by them.

1. Give yourself room to check

A convincing call can arrive while you are cooking, working or worrying about someone. You do not need to solve the whole mystery on the spot. Start by creating a pause.

"I don't make decisions on unexpected calls. I'll check and contact you myself."

Three moves to practise

PAUSE: Stop before paying, sharing a code, installing an app or following instructions.

DISCONNECT: End the call or leave the message unanswered. You do not need the caller's permission.

VERIFY: Use a saved contact, the number on your bill or card, or an official app you open yourself. A transfer to the caller's "supervisor" is still part of the same call. [1, 4]

A familiar name on the screen is not proof: caller ID can be falsified. A convincing voice is not proof either. Some impostors use AI-generated audio; others use ordinary acting, stolen details or a believable story. [1, 2]

Family practice: One person reads, "You must do this right now." Another practises ending the conversation. Swap roles. Make the habit easy to use before anyone is frightened.

2. "It's me. I need help."

"Grandma, I've had an accident. Please send money. Don't tell Mum."

Evelyn hears a voice that sounds like her grandson. Then another person takes over, claiming to be a lawyer. Her first impulse is to help. She puts her hand on the family contact list beside the phone.

What might be happening

AI can imitate a voice using recorded audio. The caller may also know names and family details. Urgency and secrecy make it harder to check. You do not have to detect an audio glitch to protect yourself. [2]

Try this: "I'm checking that you're safe. I'm calling you on your usual number."

Call the person through an established contact. If they do not answer, try another trusted person who can help locate them. Silence does not prove the story. [2]

The text-message version

"Hi Dad. My phone broke. Save this new number. Can you pay a bill for me?"

Do not treat the new number as verified. Contact your family member through the old number or another established route before sending anything. This is a documented impersonation pattern. [1]

If someone may be in immediate danger: contact emergency services independently. Do not let a demand for secrecy prevent you from getting help. [7]

3. "Rogers Mobility: save 40%"

"You're eligible for 40% off your cellphone bill. Read me the code we just sent so I can apply it."

Sam would welcome a lower bill. The caller sounds professional and offers a new phone too. Sam decides to check the offer through the provider before doing anything.

What to watch for

Cellphone-provider impersonators use discounts and device offers to obtain account information or codes. Another version ends with a delivered phone: the caller says it is the wrong model and supplies a return address. That can send the device to criminals while leaving the customer with the account charges. [3]

Your move: End the call. Open MyRogers yourself or use the contact number on your bill. Ask the real provider to verify the exact offer, any order and any return instructions. Do not share a password or one-time code with the unexpected caller, or sign in while they guide you. [3]

If a phone arrives: verify the return directly with the provider before using a label supplied by the caller. [3]

The 40% discount is an illustrative offer. The percentage alone does not establish fraud; independent verification matters.

Rogers Customer Care: 1-888-764-3771. If you shared account information or see an unexpected order, contact them promptly. [9]

4. "Read me the Apple code"

"This is Apple Support. Someone is accessing your account. Read me the confirmation number we just sent so I can stop them."

A code arrives on Maya's phone. That seems to support the caller's story. But a genuine Apple verification code does not prove that the person calling works for Apple. Someone else may have triggered an account sign-in attempt. [13, 14]

The code protects your account

Sharing a sign-in code can help an attacker complete access. Apple says its support staff do not ask for your Apple Account password or verification codes. Do not read the code aloud, send a screenshot or enter it on a page the caller supplies. Reject sign-in approval requests you did not initiate. [13]

Try this: "I don't share verification codes. I'll contact Apple myself."

End the call and open the Apple Support app or type **support.apple.com** yourself. Do not disable security features because a caller tells you to. [13]

Already shared it? Change your Apple Account password promptly through trusted settings, review account details and remove unfamiliar devices. If locked out, start recovery at **iforgot.apple.com**. [14]

Family practice: Ask, "Who started this sign-in?" A code used for your own sign-in is different from a code requested by a stranger.

5. "Your money isn't safe"

"This is your bank's fraud team. Move your savings to a safe account. We'll stay on the line."

An official-sounding caller describes a suspicious transaction. They may know some card digits. Then they ask for a transfer, a login code or access to your screen.

The request is the warning

A real-looking number and partial account information do not authenticate the caller. The Canadian Anti-Fraud Centre warns about fake investigators who seek account codes, remote access, money transfers or collection of bank cards. [4]

Try this: "I'll call the number on my card and ask the bank to check."

Do not transfer money to an external account to "protect" it. Do not read out a login or payment-approval code to an unexpected caller. Do not approve a sign-in prompt you did not initiate. [4]

Call back safely: use a different phone if possible. CAFC advises using a different phone or waiting 10 minutes before calling back; this helps avoid a connection that has not cleared. Use the number on your card, not a callback number supplied during the call. [4]

Family question: "What is this person asking us to do?" is often more useful than "Do they sound trustworthy?"

6. An invitation worth checking



Leah gets a party invitation apparently from a friend. It asks her to sign in with her email password to see the location. She shows her dad. Together, they message the host using an existing conversation.

What the caller or message wants

Your credentials or reset code.

“I’ll check with the host before signing in.”

Contact the host through a saved number before opening the link. Do not give an invitation page your email account password. [17]

Family practice: Ask which contact route you already trust. Use that route before paying, sharing a code or granting access.

7. A sticker on the parking meter



Noah is about to scan a parking-payment code when he notices a sticker edge. He pauses and opens the parking operator's verified app instead. A code being in a public place does not authenticate it.

What the caller or message wants

Card details or money through a fake payment site.

"I'll use the parking operator's official payment method."

Use the operator's independently verified app or another official payment method. Inspect the sign and destination; placement on a meter does not prove authenticity. [18]

Family practice: Ask which contact route you already trust. Use that route before paying, sharing a code or granting access.

8. A frightening call about a pet



A caller tells Ana that a clinic has her injured dog and needs payment immediately. Ana asks her partner for help, ends the call and contacts the real clinic through its published number.

What the caller or message wants

An immediate payment before you verify the claim.

“I’m calling the clinic directly to check.”

Call the actual clinic independently. Details from a missing-pet post and convincing images are not proof. [20]

Family practice: Ask which contact route you already trust. Use that route before paying, sharing a code or granting access.

9. The small fee in a text

"Delivery held. Pay a small redelivery fee to release your parcel."

"Unpaid toll: settle today to avoid penalties."

"Traffic hearing notice. Scan the QR code to pay your balance."

A small amount can make a request feel harmless. The real target may be the card details or password you enter on a copied website. Fake delivery and account messages are established scams; U.S. authorities also warned about toll texts in 2025 and traffic-notice QR texts in 2026. [5, 10, 11]

Take another route

For a parcel, open the retailer's or courier's official app yourself. For a bill or fine, find the organization's official contact details independently. Check whether the claim exists before paying. Do not use the message's link, QR code or phone number to verify the message. [5, 10, 11]

A QR code is another way to open a link. An official-looking seal or case number does not establish who sent it. [11]

Try this: "I'll check my account directly."

For kids and teens: If a message says you owe money, your account will close or you must keep a secret, show a trusted adult before responding. You do not need to handle the problem alone.

10. Three more traps to recognize

Easy online work that asks you to pay

"Complete these tasks. Deposit \$100 to unlock your earnings."

An unexpected recruiter offers simple online work. An app displays growing earnings and may even pay a small amount first. Then it demands your money, often crypto, before you can continue or withdraw. That initial payment does not prove the job is real. Do not deposit money to release supposed wages. [8]

Fake technical support

"Your computer is infected. Install this support app now."

An unsolicited call or alarming pop-up directs you to a supposed technician. Do not grant remote access or call the number in the warning. Seek help through the device maker or a support company you already know. [12]

Someone offering to recover lost money

"We found your stolen funds. Pay a recovery fee and we'll release them."

People who have already been scammed may be approached again. Do not pay a stranger who promises to recover the loss. Contact your bank or payment provider through its official channels. [7]

Notice the shared pattern: Each story offers a reason to keep following instructions. Practise saying, "I'm stopping here and checking with someone I trust."

11. If you already clicked or paid

You deserve help, not a lecture. Tell a trusted person what happened so you can work through the next steps together.

Clicked but entered nothing? Close the page. Do not return to investigate. If you downloaded software, gave device permissions or notice suspicious behaviour, seek trusted technical help. [6, 12]

Shared a password or code? Contact the affected service through its official channel. From a trusted device, change exposed passwords, including reused ones, and enable multi-factor authentication. Use official account recovery if locked out. [6]

Paid or shared card details? Contact the bank, card issuer or payment provider immediately. Explain what happened; ask about blocking further charges and reversing or recalling the payment. Recovery is not guaranteed. Keep receipts and transaction details. [6, 7]

Installed remote-access software? Stop using that device for sensitive activity and get trusted help removing unwanted access and checking it. Use a different trusted device to contact your bank and secure accounts. [6, 12]

Shared identity documents? Contact the issuer and follow your country's identity-theft guidance. In Canada, identity-fraud victims should also contact both credit bureaus. [7]

Granted an app account access? Revoke unfamiliar app permissions in account security settings. A password change alone may not remove that access. [16]

Keep relevant messages, dates and receipts for reporting. Do not keep talking to the scammer to gather more evidence. Country-specific help is on page 18.

Scam directory 1 of 4

20 additional warnings to recognize. Source dates identify the advisory, not when the scam began.

01. The “prove you’re human” trap

A familiar-looking CAPTCHA asks you to paste or run commands for a security check.

Check: Close the page. A genuine CAPTCHA does not require running commands on your computer. If you ran them, disconnect and get trusted technical help. [15]

02. A real permission screen, a malicious app

A shared file or invitation opens a legitimate account permission screen, but the app requesting access belongs to an attacker.

Check: Verify the sender and review permissions. If granted, revoke the unfamiliar app in account security settings; changing a password alone may not remove access. [16]

03. The invitation that steals your account

A message resembling a known invitation service asks for your email password or an account code to reveal party details. It may name a friend.

Check: Contact the host through a saved number before opening the link. Do not give an invitation page your email account password. [17]

04. A sticker over the parking code

A fraudulent QR sticker covers the legitimate payment code on a parking meter.

Check: Use the operator’s independently verified app or another official payment method. Inspect the sign and destination; placement on a meter does not prove authenticity. [18]

05. An unexpected gift with a QR code

An unsolicited package includes a code to reveal the sender or arrange a return. Some deliveries also support fake reviews made in your name.

Check: Do not scan to investigate. Check your shopping accounts directly and report suspicious deliveries to the marketplace. [19]

Scam directory 2 of 4

20 additional warnings to recognize. Source dates identify the advisory, not when the scam began.

06. “We have your injured pet.”

A supposed animal hospital demands urgent treatment money. Stolen or AI-generated pictures may appear to show your pet in distress.

Check: Call the actual clinic independently. Details from a missing-pet post and convincing images are not proof. [20]

07. The new client who overpays

A supposed parent urgently books childcare, sends a cheque for too much and asks you to refund the difference.

Check: Do not send the excess payment. Contact your bank: money appearing in your balance does not establish that a cheque is genuine. [21]

08. Deepfake officials offering recovery

A video impersonating an FBI official sends previous scam victims to a counterfeit complaint site. A supposed investigator may then offer to recover losses.

Check: Use ic3.gov directly for U.S. internet-crime reports. IC3 does not recover money through social-media accounts or ask for recovery payments. [22]

09. The official threatening arrest

An alleged official claims you missed court or are linked to a crime. Fake credentials and AI-supported video calls can add credibility.

Check: End contact and call the agency independently. Do not pay a caller by gift card, crypto or courier. [23]

10. An investment courier at your door

An online investment contact says cash collection is needed to fund an account or release profits. A courier arrives with an agreed password.

Check: Do not hand over cash. The matching password only connects the courier to the person who supplied it; it does not verify the investment. [24]

Scam directory 3 of 4

20 additional warnings to recognize. Source dates identify the advisory, not when the scam began.

11. The copied car dealership

A cloned dealership website copies real branding, photographs and vehicle listings, sometimes using AI.

Check: Contact the real dealership independently and arrange an inspection. Reviews of the genuine business do not authenticate a copied site. [25]

12. The unofficial bill-payment portal

A paid search result looks like your utility or service provider's official payment page but belongs to an unrelated intermediary.

Check: Use the website printed on your bill or the company's own app. This can be deceptive payment routing rather than outright theft of the whole payment. [26]

13. The rental with a different landlord

Photos of a real property appear in a new listing with a different contact, attractive rent and pressure to send a deposit.

Check: Search the address and verify who manages it. Conflicting listings and excuses preventing a viewing need investigation before payment. [27]

14. A stranger selling your land

Criminals impersonate vacant-land owners using stolen information and forged identification, then try to sell the property.

Check: Have ownership and identity independently checked. Ask the local land-records office about available change alerts. Remote-only communication and pressure to close are warnings. [28]

15. A permit invoice with real details

A municipal-looking invoice quotes your real permit number, project address and officials' names obtained from public records.

Check: Call the municipality using its published number. Accurate project details and an official-looking PDF do not authenticate the invoice. [29]

Scam directory 4 of 4

20 additional warnings to recognize. Source dates identify the advisory, not when the scam began.

16. The course promising trading wealth

Lifestyle videos promise financial freedom through paid investment coaching or trading education.

Check: Treat guaranteed success and low-risk riches as warning signs. Research the provider and instructor, and seek an independent opinion before paying. [30]

17. A fortune from someone with your name

A supposed lawyer offers to split an unclaimed life-insurance policy belonging to someone who shares your surname.

Check: Do not send money or personal information to claim a stranger's supposed fortune. Independently verify any genuine estate matter. [31]

18. The relief fund that appeared overnight

A donation appeal follows a fire, flood or other disaster. It impersonates a charity or invents one, using urgent emotional messages.

Check: Find an established charity independently and verify its donation channel. A friend reposting the appeal is not verification. [32]

19. The brand sale in your social feed

A personalized ad offers a desirable product at a steep discount and leads to an impersonated store or counterfeit seller.

Check: Check the seller independently. An advertisement appearing on a familiar platform does not mean the seller has been verified. [33]

20. The fake airline help number

A paid search ad places a scammer's phone number or website beside a familiar airline or hotel name.

Check: Use the official app, existing booking confirmation or independently verified company website to contact the business. [34]

Our family check-first card

Print this page and keep it somewhere easy to reach.

When a call or text asks for money, codes or access

1. **PAUSE.** No payment, code, download or account change while someone is pressuring us.
2. **DISCONNECT.** "I'm going to check this independently."
3. **VERIFY.** Use a saved number, the number on a bill or card, or an official app opened separately. Ask a trusted person for help.

Our household plan

Trusted person 1: _____

Phone: _____

Trusted person 2: _____

Phone: _____

Where we keep verified bank/provider numbers: _____

Optional: agree privately on a family phrase. Keep it off this displayed sheet. Treat it as one extra check, not permission to send money without verification.

Our promise

"You can tell me if something happened. We will deal with it together."

Practise with the emergency call, the 40% discount, the Apple code and the parcel text. Everyone takes a turn asking for help. Review the contact list when numbers change.

Help across North America

Contact the affected bank, card issuer or account provider promptly. A fraud report does not block a card or recover an account for you.

Canada

Report to the Canadian Anti-Fraud Centre at **1-888-495-8501** or **reportcyberandfraud.canada.ca**. Contact local police and keep the file number. For identity fraud, contact both Canadian credit bureaus. [7]

United States

Use **ReportFraud.ftc.gov** for consumer scam reports, **IC3.gov** for internet crime, and **IdentityTheft.gov** for an identity-theft recovery plan. Contact your bank or payment provider separately. [6, 22]

Mexico

For cybercrime guidance, contact Guardia Nacional at **088**. Contact your bank directly about transactions. For financial-service advice or complaints, CONDUSEF lists **55 53 400 999** and **condusef.gob.mx**. These channels serve different purposes. [35, 36]

Immediate danger

Call **911** in Canada, the United States or Mexico. Reporting websites are not emergency services.

A second scam can follow the first

Do not pay an unsolicited “recovery expert” who guarantees the return of your money. Preserve messages and receipts, stop contact, and get help from someone you trust. [7, 22]

Rogers customers can call **1-888-764-3771** about account concerns. Rogers and Fido customers can forward spam texts to **7726**. [9]

Sources and editorial notes

Checked 19 September 2026. Sources are clickable in this PDF.

[1] CAFC: emergency impersonation

[2] FTC: fake emergencies

[3] CAFC: cellphone-provider fraud

[4] CAFC: bank investigator fraud

[5] FTC: spam texts

[6] FTC: what to do if scammed

[7] CAFC: victim help

[8] FTC: task scams

[9] Rogers: fraud and scams

[10] FTC: unpaid tolls

[11] FTC: traffic-violation text

[12] FTC: tech support

[13] Apple: social engineering

[14] Apple: compromised account

[15] FTC: The “prove you’re human” trap

[16] FBI / IC3: A real permission screen, a malicious app

[17] FTC: The invitation that steals your account

[18] FTC: A sticker over the parking code

This guide covers current warnings and established scams. A recent warning is not proof that the underlying scam is new. Country labels in the online directory describe the source jurisdiction; similar tactics may appear elsewhere.

Sources continued

Checked 19 September 2026. Sources are clickable in this PDF.

[19] [FTC: An unexpected gift with a QR code](#)

[20] [FTC: “We have your injured pet.”](#)

[21] [FTC: The new client who overpays](#)

[22] [FBI / IC3: Deepfake officials offering recovery](#)

[23] [FBI / IC3: The official threatening arrest](#)

[24] [FBI / IC3: An investment courier at your door](#)

[25] [FTC: The copied car dealership](#)

[26] [FTC: The unofficial bill-payment portal](#)

[27] [FTC: The rental with a different landlord](#)

[28] [FBI / IC3: A stranger selling your land](#)

[29] [FBI / IC3: A permit invoice with real details](#)

[30] [FTC: The course promising trading wealth](#)

[31] [FTC: A fortune from someone with your name](#)

[32] [FTC: The relief fund that appeared overnight](#)

[33] [FTC: The brand sale in your social feed](#)

[34] [FTC: The fake airline help number](#)

[35] [Guardia Nacional: cybercrime guidance \(088\)](#)

[36] [CONDUSEF: contact details](#)

Stories are fictional teaching examples. Illustrations were generated with AI. Brand names identify organizations being impersonated; this independent resource is not endorsed by them. The English-language first edition draws primarily on U.S. and Canadian warnings, with Mexican reporting guidance. Coverage will expand through verified sources.