Start Here: Use These First

Companion Workbook for *Is This Message Real?* — the three tools that matter most, then the full index.

If you only have **30 minutes**, do these three things in this order.

Step	Tool	Do this
1	FRG1-01 STOP. LEAVE. CHECK. Wallet Card	Print one for every family member. Learn the three words.
2	FRG1-02 Family Verification Plan (and FRG1-03 Safe-Word Sheet)	Agree who to call, how to verify, and a safe word — in person.
3	FRG1-05 Before You Send Money Checklist	Keep it next to the device you bank with. Use it for any unusual payment.

Then, when you need them

- **Suspicious call?** FRG1-08 (exit scripts), FRG1-09 (family emergency), FRG1-10 (bank).
- **Suspicious text or email?** FRG1-06 and FRG1-07.
- **Clicked or shared something?** FRG1-13. **Sent money?** FRG1-14, then FRG1-15 and FRG1-18.

Security

Do not record passwords, PINs, one-time codes or your safe word on any worksheet. Files with personal details (FRG1-15) should be stored securely.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Resource Index

Code	Resource	Format	Use it when…
FRG1-01	STOP. LEAVE. CHECK. Wallet Card	Printable PDF, 2-up card	Always carry
FRG1-02	Family Verification Plan	Fillable PDF + DOCX	Family meeting
FRG1-03	Family Safe-Word Setup Sheet	Fillable PDF	Family meeting
FRG1-04	Two-Channel Verification Matrix	Printable PDF	Any unexpected request
FRG1-05	Before You Send Money Checklist	Printable PDF	Before any unusual payment
FRG1-06	Text Message Decision Tree	Printable PDF	Suspicious text, link or QR code
FRG1-07	Email Verification Checklist	Fillable PDF	Invoices, alerts, shared documents
FRG1-08	Phone Call Exit Scripts	Printable PDF	Unwanted or pressuring call
FRG1-09	Family Emergency Callback Script	Printable PDF	“Family member in trouble” call
FRG1-10	Bank Fraud Call Verification Script	Printable PDF	Caller claims to be your bank
FRG1-11	Payment Method Red-Flag Chart	Printable PDF	Asked to pay in an unusual way
FRG1-12	Investment Offer Verification Checklist	Fillable PDF	Online investment offer
FRG1-13	Post-Click Decision Tree	Printable PDF	After clicking or sharing details
FRG1-14	Money-Loss Response Checklist	Printable PDF	After sending money
FRG1-15	Scam Evidence Log	Fillable PDF + DOCX	After any scam attempt
FRG1-16	One-Hour Family Scam-Proofing Agenda	Fillable PDF	Family session
FRG1-17	Two-Page Fraud Firewall Quick Guide	Printable PDF	Refrigerator / desk reference
FRG1-18	Canada / U.S. Reporting Links Sheet	Web page + PDF	Reporting a scam

Last updated November 2026. Individual files use the naming pattern FRG1-NN_Name_v1.0. Printer-friendly: every PDF is black-and-white friendly; colored boxes are also labeled in words.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

STOP. LEAVE. CHECK. Wallet Card

Pocket reference for the core verification protocol. Contains no personal data.

How to use: Print at 100% (no “fit to page”) on card stock or plain paper. Cut along the outer edge of each row, then **fold on the dashed line** so the front and back face outward. Each row makes one folded card (3⅜ × 2⅛ in, standard wallet size). Make one for every family member and keep one in your phone case, wallet or purse.

FAMILY READY GUIDES · IS THIS MESSAGE REAL?

STOP. Pause. Don’t click, reply, pay or share a code.

LEAVE. Leave the call, text, email or link. Hang up.

CHECK. Verify on a second channel you already trust.

Saved number · official app · a person you know, in person

RED FLAGS = STOP

- **Urgent** or threatening: “act now”, “last chance”
- **Secret**: “don’t tell your family or the bank”
- **Unusual payment**: gift cards, crypto, wire, cash courier
- Asks for a **code, PIN or password**
- Won’t let you **hang up and call back**

Report: Canada: Canadian Anti-Fraud Centre, 1-888-495-8501, antifraudcentre-centreantifraude.ca. U.S.: reportfraud.ftc.gov. Forward scam texts to **7726**.

FAMILY READY GUIDES · IS THIS MESSAGE REAL?

STOP. Pause. Don’t click, reply, pay or share a code.

LEAVE. Leave the call, text, email or link. Hang up.

CHECK. Verify on a second channel you already trust.

Saved number · official app · a person you know, in person

RED FLAGS = STOP

- **Urgent** or threatening: “act now”, “last chance”
- **Secret**: “don’t tell your family or the bank”
- **Unusual payment**: gift cards, crypto, wire, cash courier
- Asks for a **code, PIN or password**
- Won’t let you **hang up and call back**

Report: Canada: Canadian Anti-Fraud Centre, 1-888-495-8501, antifraudcentre-centreantifraude.ca. U.S.: reportfraud.ftc.gov. Forward scam texts to **7726**.

Print note: the phone numbers and addresses on the back are current as of November 2026. Check Resource FRG1-18 (Reporting Links Sheet) for updates.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Family Verification Plan

Our household rules for urgent requests, callbacks and second checks. Fill in on screen or print and write by hand.

Security note

Do **not** write passwords, PINs, one-time codes, full account numbers or your safe word on this page. Keep this plan with your household documents, not on a shared drive or in an email.

1. Our household

Household / family name	
Plan date	
Plan owner (keeps this updated)	
Next review date	

2. Our golden rule

No money, gift cards, crypto, bank details or codes go out on the strength of one call, text, email or message — even if it looks, sounds or says it is someone we know. We Stop, Leave, and Check on a second channel first.

3. Second-check people

Anyone asked to send money or share information checks with at least one of these people first, using a number we already had saved.

Name	Relationship	How we reach them (saved number / in person)

4. Our rules for urgent requests

Pause time before any unusual payment	
Amount that always needs a second person	
Who must approve payments in our household	
Our callback rule (where the number comes from)	

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Our rule for “family emergency” calls	
Who we call at the bank (use card / app number)	
Who handles our mail, e-transfers and cards if one of us is away	

5. Everyone agrees

Family member	Initials	Date

Next: set up your safe word using FRG1-03 and rehearse the plan at your family session (FRG1-16).

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Family Safe-Word Setup Sheet

A shared secret that proves it is really us when someone asks for urgent help or money.

Never write the word here

Do not write the safe word on this sheet or in a text, email, chat or cloud note. Share it in person or by voice and memorize it. If it is written anywhere, keep that copy separate from this sheet.

Step 1 – Choose it

- Pick a word or short phrase that is **easy to remember but impossible to guess**: two or three unrelated words work well.
- Avoid names of people or pets, birthdays, addresses, teams, and anything posted on social media.
- Choose one that everyone in the family, including children and grandparents, can say without difficulty.

Step 2 – Share it safely

- Tell each person **in person**, or by phone only if you are certain who you are speaking to. Never by text, email or direct message.
- Keep the circle small: only people who may need to verify an urgent request.

Step 3 – Use it

- Ask for it whenever someone claiming to be family asks for **money, gift cards, a code, or a favour** by phone, voice message, video call or text.
- Voices and faces can now be copied convincingly. A real family member can give the word; a scammer cannot.
- If the caller cannot give it, stop, hang up, and call back on the saved number (see FRG1-09).
- Never offer the word first, and never give hints.

Step 4 – Replace it

- Replace it every 6–12 months and **immediately** if it may have been overheard, written down, or said to someone suspicious.
- Tell everyone the new word in person and record the date below.

Our record (no words, only facts)

Date safe word was set	
Who knows it (first names)	
We store a backup: where? (not on this sheet)	
Replace by (date)	

Replacement log

Date replaced	Reason (e.g., scheduled, suspected exposure)	Everyone told?

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Two-Channel Verification Matrix

If a request arrives on one channel, confirm it on a different one that **you** start, using contact details you already had.

The request arrives by…	Do NOT use	Safer second channel (you start it)	Tips
Text message / chat app (SMS, WhatsApp, iMessage)	Replying to the message; links, buttons, QR codes in it; the number it came from	Call the person or company on a number saved in your contacts, on the back of your card, or in the official app	Real contacts can be reached on the second channel too. If they can't be, that is information.
Incoming phone call	Caller ID (it can be faked); "press 1"; a number they give you; staying on the line	Hang up, wait, and call back using the number on your card, statement, bill or official website. Use another phone if you can.	Scammers can keep a landline open. Listen for a dial tone before you call back.
Voicemail or voice message	Calling the number left in the message	Look up the organization's number yourself, or call the family member on their saved number	A voice can be cloned. Ask for the safe word on the callback.
Email	Links, attachments, "reply" address, phone number in the email	Open the company's app or type its address yourself; or phone using a number from a past statement	Check the sender's actual address, not just the display name.
Social media message / friend request	Replying; clicking links; moving to a private chat app	Phone or video the person using a number you already had; ask the safe word	A hacked account can send messages that look genuine.
Video call	Trusting the face or voice alone	Hang up and call back on a saved number; ask the safe word or a question only they can answer	Video can be faked or replayed.
Letter, flyer or QR code in public	Scanning the QR code; calling the number printed on it	Search for the organization yourself or use its official app; ask a person you trust	Stickers can be placed over genuine QR codes (parking, menus, notices).
At the door or a courier pick-up	Handing over cash, cards, PINs or devices	Close the door; phone the organization on its official number; contact family	Real agencies do not send couriers to collect money.
Pop-up or browser alert ("virus", "support")	The number or button in the alert; allowing remote access	Close the browser; restart the device; contact support through the company's official site or app	No genuine alert asks you to phone a number.

The rule: A second channel counts only if you start it with contact information you already trusted **before** this request arrived.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Before You Send Money Checklist

A five-minute pause for any unusual, urgent or unexpected payment. Keep it by the device you bank with.

If any box in sections A–C is ticked, do not send the money yet. Go to section D.

A. The request

- ☐ Someone contacted me first, and I did not expect this request.
- ☐ I am being rushed, threatened, or told “now”, “today” or “last chance”.
- ☐ I have been asked to keep it secret from family, my bank, or the police.
- ☐ I have been told to lie to a bank teller or staff about why I am sending money.

B. The payment

- ☐ They want gift cards, cryptocurrency, a wire transfer, cash, or a courier pick-up.
- ☐ I am being asked to move money to a “safe account”, or to “test” or “reverse” a payment.
- ☐ The recipient’s name, account or business does not match what I was told.
- ☐ I am asked to share a one-time code, PIN or password to complete it.

C. The person

- ☐ I have not spoken to them on a number or channel I already trusted.
- ☐ I have never met them in person, but they ask for money or investment.
- ☐ They ask me to leave the app or platform and use a private chat.
- ☐ They say I will lose a benefit, be arrested, or harm a family member if I don’t pay.

D. Pause and check

- ☐ **Stop.** Take at least one hour; for large amounts, sleep on it (24 hours).
- ☐ Call the person or company on a number from my contacts, card, bill or official app — not the one in the message.
- ☐ Tell a second person from our Family Verification Plan (FRG1-02) and listen to their reaction.
- ☐ Call my bank using the number on my card and ask if the request is genuine.
- ☐ Ask: could I get this money back if it is wrong? Many payment types cannot be reversed (see FRG1-11).

Date and time I paused _____

Amount and what it was for _____

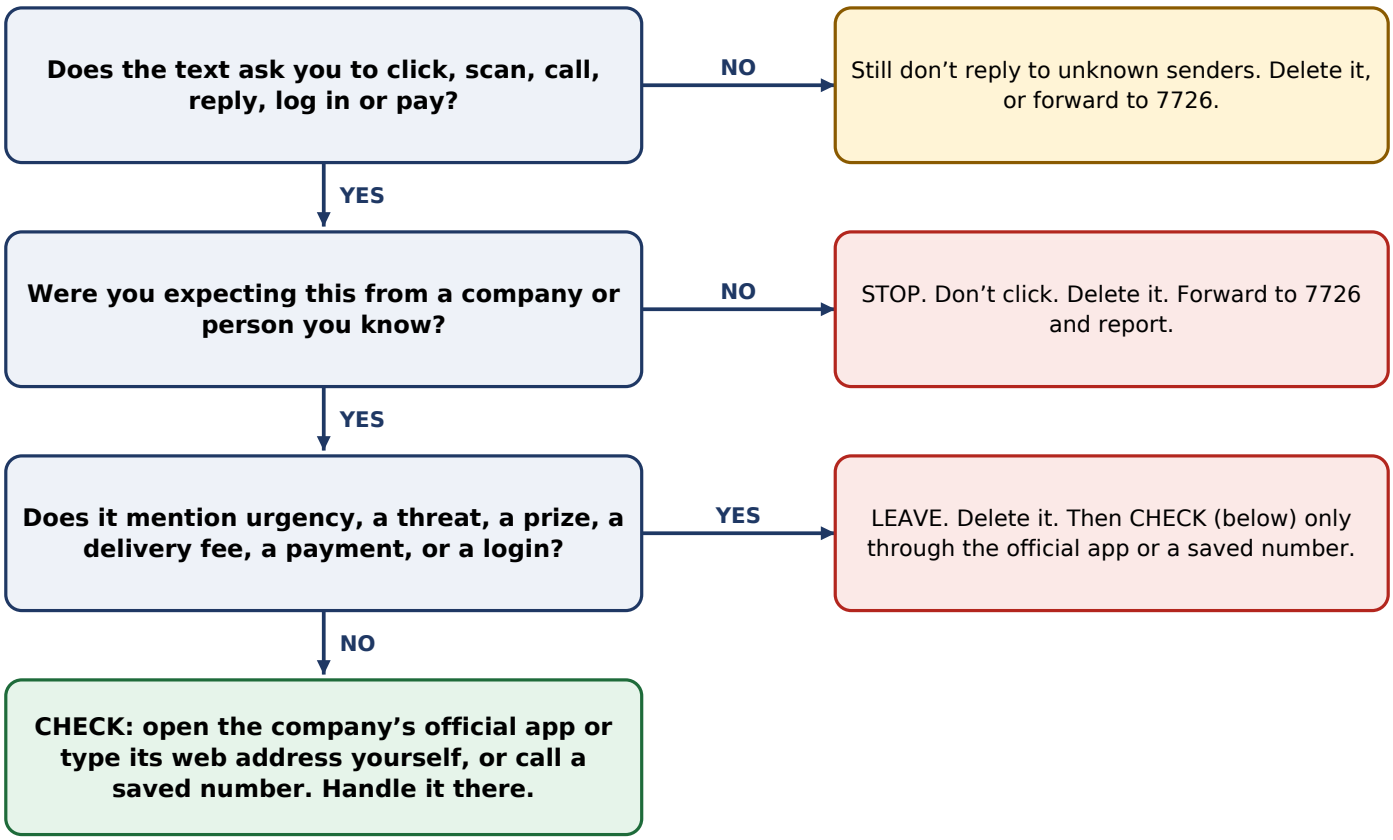
Who I checked with _____

Decision: ☐ Don’t send ☐ Send after verified ☐ Not sure — ask a second person

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Text Message Decision Tree

What to do with a suspicious text, link or QR code. Start at the top and follow the arrows.



Tips

- **QR codes are links.** Treat any QR code like a link — especially on parking meters, posters, menus and packages.
- Real organizations do not ask you to confirm a PIN, password or one-time code by text.
- Family "new number" texts ("Hi Mum, I lost my phone…"): call the old number or ask the safe word before anything else.
- If you clicked or replied, go to FRG1-13 (Post-Click Decision Tree).

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Email Verification Checklist

Use for invoices, account alerts, “shared document” messages and anything that asks for action.

Keep it safe

Do not paste suspicious links or attachments into this form. Describe them in your own words. Never type passwords or full account numbers here.

Date and time received	
Who it claims to be from	
Sender’s actual email address (as shown when you open details)	
What it asks me to do	

Quick checks (tick each one you have done)

- ☐ The **actual sender address** matches the real organization (watch for look-alikes: rnicrosoft, paypa1, extra words, odd endings).
- ☐ I was **expecting** this invoice, document or alert.
- ☐ The greeting and writing look normal for this sender (no odd wording, generic “Dear customer”).
- ☐ I have **not clicked** anything. On a computer I hovered over the link and the address matches the company; on a phone I did not tap it.
- ☐ The attachment is a type I expected (be cautious with zip, html, macro-enabled Office files, or unexpected PDFs).
- ☐ The message does **not** pressure me with a deadline, a threat or a “secret”.
- ☐ Payment details (bank, e-transfer address) are **unchanged** from past invoices — or I have confirmed the change by phone.

Second-channel check

- ☐ I contacted the sender by phone or app using details I already had.
- ☐ They confirmed they sent it.

Result

- ☐ Verified as genuine
- ☐ Suspicious — deleted and reported (mark as phishing in your email app; forward to your provider or employer’s security team)
- ☐ Not sure — asked a second family member

Notes

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Phone Call Exit Scripts

Short, polite-but-firm phrases for ending the call. You never owe a caller your time, your answers or your money.

You can always hang up. A real bank, agency or hospital will still be there when you call back on their official number.

If the caller says…	Say this, then hang up
“This is your bank’s fraud department. Your account is compromised.”	“I’ll hang up and call the number on the back of my card.”
“This is the tax agency / immigration / social security. You owe money or face arrest.”	“Agencies send letters. I’ll contact the agency directly. Goodbye.”
“This is the police. We’re holding your grandson / you have a warrant.”	“I’ll call the police on their public number and the family on theirs.”
“Grandma/Dad, it’s me. I’m in trouble. Don’t tell anyone.”	“What’s our safe word?” (No word? “I’ll call you back on your number.”)
“Tech support: your computer has a virus.”	“I don’t take support calls. Goodbye.”
“You’ve won / your package is stuck / pay a small fee.”	“Not interested. Don’t call again.”
“Don’t hang up or the account will be frozen!”	“Hanging up is exactly what I’m going to do.”
“You must pay with gift cards / crypto / cash today.”	“No legitimate organization asks for that. Goodbye.”
“Confirm the code we just texted you.”	“I never share codes.”

After the call

- Wait at least 10 minutes, or use a different phone, before calling back. Some scammers keep a line open.
- Don’t call back a number the caller gave you. Use a saved or official one.
- Write down the date, number and what they said (FRG1-15) and tell a family member.
- Report it — see FRG1-18.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Family Emergency Callback Script

For any call, message or video saying a family member is hurt, arrested, stranded or in trouble and needs money now.

Stay calm. Slow it down. Real emergencies can wait two minutes for a callback. Scammers depend on you not taking them.

Step 1 – Don't give information

- Don't say the family member's name first. Ask, "**Who is this?**" and let them say it.
- Don't confirm details like where someone lives, who else is in the family, or whether they are travelling.

Step 2 – Ask for the safe word

- "What is our safe word?" (see FRG1-03). If they can't say it, treat it as a scam.
- Or ask a question only the real person would know — not something on social media.

Step 3 – Hang up and call back

1. Say: "I'm going to call you back right now." Hang up even if they plead or say "don't hang up".
2. Call the person on the number **already saved** in your phone.
3. No answer? Call their spouse, partner, parent, friend, workplace or school. Try a second family member.
4. If someone says they are a lawyer, police or hospital: look up the organization yourself and call its main number.

Remember

- Real police, courts and lawyers do not demand bail or fees in gift cards, crypto, cash, couriers or transfers to strangers.
- Never withdraw cash or buy gift cards because someone on the phone told you to.
- Don't let the caller stay on the line or choose who you call.

People to call (fill in by hand)

Name	Phone	Name	Phone

Pair with your trusted contact list from the book and your Family Verification Plan (FRG1-02).

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Bank Fraud Call Verification Script

Safe steps when someone calls, texts or emails claiming to be your bank, card company or payment provider.

Never trust caller ID, a name or a "verification" by the caller. Numbers can be faked, and callers can sound professional. Use the number on the back of your card, your statement, or inside your official banking app.

Script

1. **Say:** "Thank you. For my security I'm going to hang up and call my bank on the number on my card."
2. **Hang up.** Wait at least 10 minutes, or use a different phone, before calling.
3. **Dial** the number on the back of your card, a recent statement, or in your banking app — never a number from the message or search ads.
4. **Say:** "I received a call or message claiming to be from you about possible fraud. Can you check my accounts and tell me if it was genuine?"
5. Ask for the fraud department and a **reference number**. Note the date, time and name.
6. If the bank wants to discuss anything, **they will say so on their own call**. You don't need to complete anything the first caller wanted.

A real bank will never…

- Ask you to move money to a "safe account", a "secure wallet" or to "test" a transfer.
- Ask for your full PIN, online banking password, or a **one-time code** that was texted to you.
- Ask you to install remote-access software, or to "confirm" your identity by letting them see your screen.
- Send a courier to collect your card, cash or devices.
- Pressure you to keep the call secret from family or bank staff.

If you already shared something

- Call your bank **now** on the official number and say exactly what you shared. Ask to freeze or replace cards and secure online access.
- Go to FRG1-13 (Post-Click Decision Tree) and FRG1-14 (Money-Loss Response Checklist).

Bank / card name I called _____

Date and time _____

Reference number _____

Notes _____

Official-contact tip: write the real fraud line for each of your banks on the back of this page or inside your Family Verification Plan (FRG1-02).

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Payment Method Red-Flag Chart

Why certain payment requests deserve extra verification. Educational only — protections vary by bank, provider and country.

If they ask you to pay by…	Why scammers like it	How hard is it to get money back?	What a scam looks like
Gift cards	Instant, anonymous, spent by whoever holds the numbers	Very hard. Contact the card company at once, but recovery is rare.	“Pay the tax / bail / fee with gift cards.”
Cryptocurrency (ATM or app)	Fast, irreversible, hard to trace to a person	Very hard. Transfers generally cannot be reversed.	“Deposit cash into this Bitcoin machine to secure your account.”
Wire transfer / international transfer	Large amounts move quickly; recipient may be abroad	Hard. Ask the bank to recall it immediately — hours matter.	Fake invoice; “safe account”; romance or investment “platform”.
Cash, courier or in-person pick-up	No paper trail; scammer may send a driver or “agent”	Very hard once handed over.	“A courier will collect the cash to keep it safe.”
Person-to-person apps and e-transfers (Interac e-Transfer, Zelle, Venmo, Cash App)	Instant and often irreversible when you send willingly	Often hard. Provider support varies — report immediately.	“Send it to me and I’ll refund the overpayment.”
Cheque / bank draft / “overpayment”	Funds can show as available before the cheque is found to be fake	Not recoverable from the bank if you spent real money.	“I paid too much — please send back the difference.”
Credit card (to a business you chose)	Not preferred by scammers — more protections	Often better. Dispute rights apply to unauthorized or defective charges.	Fake sites can still steal card details — type the address yourself.
Anything they chose, with pressure to hurry	Pressure and secrecy are the tactics, not the payment type	Varies	Urgent + secret + unusual = STOP.

Rule of thumb: If a stranger or an unexpected caller tells you *how* to pay, that is a red flag by itself.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Investment Offer Verification Checklist

Prompts independent checks **before** sending funds to any online opportunity. Not investment advice.

Keep it safe

Do **not** enter account logins, wallet keys, or passwords here. This form is for your notes and checks only.

Date	
Name of offer, platform or person	
How did they contact me?	
Promised return	
Amount they want	

Red flags (tick any that apply)

- ☐ They contacted me first (text, social media, dating app, wrong-number chat).
- ☐ Guaranteed, “risk-free” or unusually high returns.
- ☐ Pressure to act quickly or “before the window closes”.
- ☐ They want crypto, wire or gift cards, or want me to move to a private chat app.
- ☐ I can’t find who owns the company or where it is located.
- ☐ I’m shown screenshots of gains but cannot withdraw my own money.
- ☐ They ask for more money to “unlock”, “verify” or pay “taxes” on my returns.

Checks I will do independently

- ☐ **Canada:** is the firm or person registered? Search the Canadian Securities Administrators’ National Registration Search at **aretheyregistered.ca**.
- ☐ **U.S.:** check FINRA BrokerCheck (**brokercheck.finra.org**) and the SEC adviser search (**adviserinfo.sec.gov**).
- ☐ Search the company name with “warning”, “scam” and “regulator” using sources I find myself.
- ☐ Ask for written documents; read the fine print about withdrawals and fees.
- ☐ Call the company on a number from a source I trust, not the one they gave.
- ☐ Talk to a second family member, accountant or licensed advisor before any transfer.

Decision

- ☐ Not sending — red flags found
- ☐ Waiting 7 days and consulting a licensed professional
- ☐ Reported suspected fraud (FRG1-18)

Registration is only a first check — it does not guarantee that an investment is suitable or safe, and a scammer may falsely claim a registered firm’s name. Always contact the registered firm yourself.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Post-Click Decision Tree

Find the row that matches what happened. Act in order. Use a different, clean device for password changes if your device may be compromised.

What happened?	Do now (first 15 minutes)	Then (same day)	Reporting & follow-up
A. I clicked a link or opened an attachment — nothing else.	Close the page. Don't enter anything. Disconnect Wi-Fi if you opened a file.	Run a security scan (built-in or a reputable brand). Update the device. Clear browser data.	Mark the message as phishing and delete it. Watch for unusual activity.
B. I entered a username and password	On the **real** site (typed address or app), change that password immediately. Do the same anywhere you reused it.	Turn on two-step verification. Sign out of all sessions. Check recovery email, forwarding rules and recent logins.	Tell your bank if it was a financial account. See FRG1-18.
C. I entered card, bank, SIN/SSN or ID details	Call your bank / card issuer on the official number. Freeze or replace the card. Ask them to watch the accounts.	Place a fraud alert or credit freeze with the credit bureaus (see FRG1-18). Review statements.	Report to the CAFC or FTC. Keep a record in FRG1-15.
D. I installed an app, or allowed remote access	Disconnect from the internet. Uninstall the app. Don't log into anything on that device.	Using a different device, change passwords and call your bank. Have a professional check or reset the device.	Report it. Check for new accounts or unknown payment apps.
E. I gave a one-time code or called them back	Contact the company or bank immediately using an official number and tell them what you shared.	Change passwords; review linked accounts and devices; set up account alerts.	Report to your bank and FRG1-18 agencies.
F. I sent money	Go to **FRG1-14** (Money-Loss Response Checklist) right now.		

Being tricked is not a character flaw — these messages are built by professionals. **Speed matters more than embarrassment.** Tell someone you trust today.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Money-Loss Response Checklist

Time-sensitive steps after sending money or financial information. Work down the list; call your bank first.

Call your bank or payment provider now. Every hour matters. Use the number on your card or in the official app.

First hour

- ☐ Call the bank, card issuer or payment app. Say: “I’ve been the victim of a scam and need to report a fraudulent payment.” Ask to recall, freeze or dispute, and get a **reference number**.
- ☐ **Wire / bank transfer:** ask for a recall or fraud hold right away.
- ☐ **Gift cards:** call the card company (number on the card or receipt) with the card numbers and your receipt.
- ☐ **Crypto:** contact the exchange or ATM operator immediately with the wallet address and transaction details.
- ☐ **Cheque / draft:** tell your bank before any funds are moved or spent.
- ☐ If you shared passwords or codes, change them on the real sites and sign out of all devices.
- ☐ If a scammer has remote access to your device, disconnect it from the internet first.

Same day

- ☐ Report to the police (local non-emergency line) and get a report number.
- ☐ Report to the **Canadian Anti-Fraud Centre** and/or the **FTC** and **FBI IC3** — see FRG1-18.
- ☐ Place a fraud alert or credit freeze with the credit bureaus if ID details were shared.
- ☐ Gather evidence: texts, emails, phone numbers, usernames, payment receipts. Screenshot — don’t delete.
- ☐ Start the Scam Evidence Log (FRG1-15).
- ☐ Tell a family member or trusted person today.

Next days

- ☐ Review bank and card statements daily for two weeks. Set up alerts.
- ☐ Watch for **recovery scams** — people who say they can get your money back for a fee. Report them.
- ☐ Update passwords and enable two-step verification everywhere important.
- ☐ Reset your family’s safe word if a family member was impersonated (FRG1-03).
- ☐ Review your Family Verification Plan and fix the gap that let it through (FRG1-02).

Bank / provider called (time) _____

Reference number _____

Police report number _____

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Scam Evidence Log

Record what happened while it is fresh. Use one row per contact or payment.

Security

Sensitive record. Store securely (locked drawer or password-protected file), share only with your bank, police or investigators, and shred when no longer needed. Do not record full card numbers, passwords or PINs — last 4 digits only.

Your name

Date first contact

Date / time	Contact method	Phone / username / email / site	What they said or asked	Amount, method, last 4 digits, recipient	Actions & report #

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

One-Hour Family Scam-Proofing Agenda

A 60-minute session to turn the book into household habits. Gather everyone who uses a phone, email or money.

Date and time

Where / how (in person, video)

Facilitator

Attending

Time	Item	What to do	Tools
0–5	Welcome	Explain why: scams are professional and can fool anyone. No blame, no embarrassment.	—
5–15	Share stories	Each person shares a scam message they saw or a near-miss.	Book chapters
15–30	STOP. LEAVE. CHECK.	Walk through the card, then role-play the exit scripts and callback script.	FRG1-01, 08, 09
30–40	Our rules	Agree the Family Verification Plan and set the safe word (in person, don't write it).	FRG1-02, 03
40–50	Payment & device setup	Review payment red flags; check two-step verification, bank alerts, spam filters and credit freezes.	FRG1-05, 11
50–58	If it happens	Practise: who calls the bank, how to report, how to keep evidence.	FRG1-13, 14, 15
58–60	Close	Assign actions and set the next review date.	FRG1-18

Decisions made

Action items

Task	Owner	Due date

Next review date

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Fraud Firewall Quick Guide

Two pages that sum up the whole book. Keep it on the refrigerator or by your desk.

STOP. LEAVE. CHECK.
Stop before you click, reply, pay or share a code. **Leave** the call, text or link. **Check** through a second channel you already trust.

Spot the red flags

- **Urgency** or threats — “act now”, “your account is locked”.
- **Secrecy** — “don’t tell anyone”.
- **Unusual payment** — gift cards, crypto, wire, cash couriers.
- **Requests for codes**, PINs or passwords.
- **Pressure** not to hang up or call back.

Our four household habits

1. **Second channel:** confirm on a different channel you start (FRG1-04).
2. **Safe word:** a family secret for urgent help or money requests (FRG1-03).
3. **Pause:** no unusual payments without a pause and a second person (FRG1-05).
4. **Plan:** everyone knows who to call and what to do (FRG1-02).

What to say

Situation	Say this
“Your bank is calling”	“I’ll call the number on my card.”
“Grandma, I’m in trouble”	“What’s our safe word? I’m calling you back.”
“Pay with gift cards / crypto”	“No real organization asks for that.”
A text with a link	Don’t tap. Open the official app or type the address.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

If you clicked

- Close it. Don’t enter anything. Run a security scan.
- Entered a password? Change it on the real site, reuse nowhere, turn on two-step verification.
- Entered card or ID details? Call your bank; consider a fraud alert or credit freeze.
- Installed something or allowed remote access? Disconnect and get help. (FRG1-13)

If you sent money

- Call your bank or payment provider **immediately** and ask for a recall or dispute.
- Report to police and to the Canadian Anti-Fraud Centre or the FTC / FBI IC3.
- Keep every message, receipt and number; use the Evidence Log (FRG1-15).
- Beware of “recovery” offers that charge a fee. (FRG1-14)

Everyday protection

- Use a password manager and unique passwords; turn on two-step verification, preferably an app or security key.
- Keep phones and computers updated; use built-in spam filters.
- Limit what you post: birthdays, travel, family names and voice clips help scammers.
- Set bank alerts and transfer limits; review statements monthly.
- Review the Family Verification Plan and replace your safe word every 6–12 months.

Report

Where	Contact
Canada	Canadian Anti-Fraud Centre: antifraudcentre-centreantifraude.ca · 1-888-495-8501
U.S.	FTC: reportfraud.ftc.gov · FBI IC3: ic3.gov
Text scams	Forward to 7726 (SPAM)
More links	See FRG1-18 Reporting Links Sheet

Share this guide with a parent, child or neighbour. Scam protection works best when everyone knows the same simple routine.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.

Canada / U.S. Reporting Links Sheet

Where to report scams and get help. Verify links before relying on them; agencies and links can change.

Last reviewed November 2026. This PDF is a dated snapshot. The live, maintained version is on the Cogitent Press companion-resources page for this book. In an emergency, call your bank first and local police if someone is in danger.

Country	Organization	Use it to…	Web address	Phone
Canada	Canadian Anti-Fraud Centre (CAFC)	Report fraud and cybercrime; scam alerts	antifraudcentre-centreantifraude.ca	1-888-495-8501
Canada	Your local police (non-emergency line)	File a report; get a report number	Look up on your police service's website	
Canada	Competition Bureau of Canada	Deceptive marketing and online scams	competitionbureau.canada.ca	
Canada	Canadian Centre for Cyber Security – Get Cyber Safe	Cyber safety guidance and tips	getcybersafe.gc.ca	
Canada	Credit bureaus: Equifax Canada, TransUnion Canada	Fraud alerts and credit reports	equifax.ca · transunion.ca	
Canada	Canadian Securities Administrators	Check registration before investing	aretheyregistered.ca	
U.S.	Federal Trade Commission (FTC)	Report scams and identity theft	reportfraud.ftc.gov	1-877-382-4357
U.S.	FBI Internet Crime Complaint Center (IC3)	Report internet-enabled crime	ic3.gov	
U.S.	IdentityTheft.gov	Create an identity theft recovery plan	identitytheft.gov	
U.S.	FINRA BrokerCheck / SEC adviser search	Check brokers and advisers	brokercheck.finra.org · adviserinfo.sec.gov	
U.S.	Credit reports and freezes	Annual credit reports; freezes at each bureau	annualcreditreport.com · equifax.com · experian.com · transunion.com	
U.S.	Consumer Financial Protection Bureau	Complaints about banks and financial firms	consumerfinance.gov/complaint	
Both	Your mobile carrier – report spam texts	Forward the scam text to your carrier	Forward to 7726 (SPAM)	

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.