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.