Protect Yourself from Cybercrime

A Practical Quick-Reference Guide

Why This Guide Matters

Cybercriminals are faster, smarter, and more targeted than ever. This guide cuts through the noise so you can spot scams, protect yourself, and help others do the same.

⚠ HERE'S THE LATEST! NEW SCAM ALERTS:

AI voice cloning — scammers fake a family member's voice to demand emergency cash.
Deepfake video calls — fraudsters pose as executives or celebrities on live video.
QR code phishing ("Quishing") — fake QR codes redirect you to credential-stealing sites.
Government impersonation texts — fake IRS, Social Security, or HMRC messages with urgent demands.
Job offer scams — fake remote jobs that ask you to move money ("money mule" schemes).

Top 10 "Red Flags" of Online Scams

- They push you to move to WhatsApp, Telegram, or Signal early in the conversation for greater privacy.
- They share emotional personal stories — hardship, illness, tragedy — to build fast intimacy.
- You're urged to invest in crypto, especially on a platform you've never heard of.
- They use flattery, spiritual language, or emotional vulnerability to gain your trust.
- Pressure to act fast or send large sums — "This offer expires today" or "Please help!"
- A third-party authority appears — a "customer service rep" or "lawyer" — to confirm the story or to demand compliance.
- Profits or withdrawals are suddenly "locked" unless you send more money first.
- **You feel afraid or ashamed to tell family or friends what's happening.**
- They walk you through steps inside a banking or finance app (especially using screenshots).
- **Your gut says something is wrong — but they talk you out of trusting it.**

If You've Been Scammed — Act Now

1. Stop all contact with the scammer immediately.
2. Call your bank or credit union. Report all transfers and ask about reversal options.
3. Report to the FTC at reportfraud.ftc.gov — takes under 5 minutes.

4. File a report with the FBI’s Internet Crime Complaint Center at ic3.gov.
5. If crypto was involved, also report to the Commodity Futures Trading Commission (CFTC) at cftc.gov/complaint.
6. Document everything: save screenshots, emails, chat logs, and transaction records.
7. Contact a counselor or therapist — scam trauma is real and you deserve emotional support.

How to Talk to Someone Who Was Scammed

Lead with compassion, not judgment. Cybercriminals are professional manipulators — anyone can be targeted. Avoid phrases like “How could you fall for that?” Instead, say: “I’m glad you told me. Let’s figure this out together.”

Share this guide. Help them update passwords, enable two-factor authentication, and review privacy settings on social media.

Helpful Resources

United States

Federal Trade Commission (FTC): https://reportfraud.ftc.gov

FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov

CFTC Crypto Fraud Tip Line: https://www.cftc.gov/complaint

AARP Fraud Watch Network: https://www.aarp.org/money/scams-fraud/

Better Business Bureau Scam Tracker: https://www.bbb.org/scamtracker

Identity Theft Resource Center: https://www.idtheftcenter.org

Canada

Canadian Anti-Fraud Centre (CAFC): https://www.antifraudcentre-centreantifraude.ca

Royal Canadian Mounted Police (RCMP) Fraud Prevention: https://www.rcmp-grc.gc.ca/en/fraud-prevention

Financial Consumer Agency of Canada: https://www.canada.ca/en/financial-consumer-agency.html

United Kingdom & Europe

Action Fraud UK: https://www.actionfraud.police.uk

Europol Cybercrime: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

European Union Fraud Prevention: https://commission.europa.eu/topics/consumers/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en#covid-19

Australia & New Zealand

Scamwatch (Australia): https://www.scamwatch.gov.au

Australian Cyber Security Centre: https://www.cyber.gov.au

CERT NZ: https://www.cert.govt.nz

Consumer Protection NZ: https://www.consumerprotection.govt.nz