CyberExperts

FREE GUIDE

# Scam Survival Kit

Plain-English red flags, recovery steps, and official places to report — for everyday people and small businesses.

CyberExperts.com · November 2026

This guide summarizes official consumer-protection advice. It is not legal advice.

# How to use this kit

Scams work by rushing you. A text, call, email or pop-up tries to make you click, pay, or share a password before you have time to think. This kit is meant to sit next to your phone: a short list of warning signs, and a clear first hour if something already went wrong.

You do not need technical training to use it. When in doubt, stop, use a phone number or website you already trust, and report what happened.

## What scammers usually want

- Money, gift cards, cryptocurrency, or a “small fee” that gets your card number.
- A password, passcode, one-time code, or remote access to your phone or computer.
- Enough personal information to open credit, file a tax return, or break into other accounts.

## A simple rule

A bank, delivery company, Apple, Google, Microsoft, the IRS, or the police will not ask you — by unexpected text, email, or cold call — to pay a fee, read out a passcode, or install remote-access software. Hang up. Open the official app or type the real website yourself.

# Today’s most common scam types

Names change. The pressure does not. Watch for these patterns.

## Phishing texts and emails

A message that looks like your bank, employer, Microsoft, or a government agency asks you to “confirm” a login or update a payment method. The link is the trap. Type the official address yourself, or use the app you already have.

## Fake delivery texts

A carrier you may even be waiting on says a package is held for a small customs or delivery fee. Real carriers do not collect random $1–$5 fees by text. Look at the web address: extra words or odd endings mean it is not the real company.

## Bank or card impersonation

A call or text says your account was frozen or a purchase was flagged. They want you to move money “to safety,” read a one-time code, or grant remote access. Hang up and call the number on the back of your card.

## Tech-support pop-ups and calls

A screen warning or a caller claiming to be Apple, Microsoft, or your internet provider says your device is infected. They want remote access or payment. Close the browser (force-quit if you must) and contact the company through official support only.

## AI voice cloning and “family emergency” calls

A voice that sounds like a child, grandchild, or boss says they are in trouble and need money or a passcode now. Hang up. Call that person on a number you already have. Do not trust caller ID. A real loved one can wait while you check.

## QR-code (“quishing”) scams

A sticker over a parking meter, a flyer, or a “parking ticket” QR code sends you to a fake payment site. Look at the URL before you enter a card. Prefer official apps or a meter you know is real.

## Marketplace and payment scams

A buyer or seller wants to move off the platform, overpays and asks you to send money back, or sends a fake tracking number. Keep the chat and payment on the site. Never accept a check or “too much” transfer as a reason to pay someone back.

## Romance and investment pitches

Someone you met online builds trust, then asks for money, gift cards, or crypto for a “sure” investment or a personal emergency. Real partners and real investments do not start this way. Do not send money to someone you have not met in person, and report it.

# 10 red flags

If two or more of these show up, stop. It is safer to be slow than to be right later.

01 The message was unexpected, even if it uses a familiar logo or a real-looking name.

02 It pushes you to act in minutes: “Your account will close,” “Your package will be returned,” “Don’t tell anyone.”

03 It asks you to click a link, scan a QR code, or call a number that came in the same message.

04 The web address is not the company’s real domain — extra words, hyphens, or a strange ending.

05 It asks for a password, passcode, one-time code, remote access, or a photo of your ID or card.

06 It asks you to pay a small “fee,” buy gift cards, or send cryptocurrency.

07 It asks you to move money to a “safe” account, or to refund an overpayment.

08 Caller ID or the email “From” line looks official, but you did not start the conversation.

09 A voice sounds like someone you know, but the story is urgent and new.

10 They tell you not to talk to your bank, a family member, or the police.

# If something already happened

Work in this order. Official recovery tools are free.

## If you clicked a link or typed a password

- Do not keep entering information. Close the tab or app.
- On a real browser or official app you typed yourself, change the password for that account. Then change it on any other account that used the same password.
- Turn on two-factor authentication (an authenticator app or a passkey is stronger than a text-message code).
- If you typed a banking or email password, call the institution using a number on the back of your card or on their official site — not a number in the message.
- Run a security scan with software you already trust, and install system updates.

## If you paid, or gave a card or account number

- Call your bank or card issuer immediately and ask them to stop or reverse the payment and watch the account. Use the number on the card.
- If you paid with a gift card, contact the card issuer and report the scam. If you paid with crypto, contact the exchange. Recovery is not guaranteed, but speed matters.
- Report the scam at ReportFraud.ftc.gov so investigators and other consumers can see the pattern.
- If a transfer involved a possible crime or a large loss, also file at the FBI's Internet Crime Complaint Center, ic3.gov.

## If you gave personal information, a passcode, or remote access

- Change passwords and sign out of other sessions. If a support person had remote access, assume they could see what was on the screen.
- Start a recovery plan at IdentityTheft.gov — the official U.S. site for identity-theft recovery. It will walk you through next steps and generate a personalized plan.
- Consider a free credit freeze at all three nationwide credit bureaus (below) so a stranger cannot open new credit in your name.
- If a Social Security number may be involved, review your Social Security account at ssa.gov and follow the prompts on IdentityTheft.gov.

# Official places to go

These are U.S. government or official bureau sites. Type them yourself or use the links in the online version of this kit. You should not have to pay to freeze your credit or to file these reports.

## Report a scam

https://reportfraud.ftc.gov/ — Federal Trade Commission, ReportFraud.ftc.gov

## Identity-theft recovery plan

https://www.identitytheft.gov/ — IdentityTheft.gov

## Internet crime complaint

https://www.ic3.gov/ — FBI Internet Crime Complaint Center

## Free credit reports

https://www.annualcreditreport.com/ — the official annualcreditreport.com site

## CISA security basics

https://www.cisa.gov/topics/cybersecurity-best-practices

## Equifax credit freeze

https://www.equifax.com/personal/credit-report-services/credit-freeze/

## Experian credit freeze

https://www.experian.com/help/credit-freeze/

## TransUnion credit freeze

https://www.transunion.com/credit-freeze

# Lock down your phone and accounts

Do these even if you are not sure a scam worked. They are free and they close the most common holes.

## On your accounts

- Use a unique password or passkey for email and banking. A password manager helps you do this without memorizing every one.
- Turn on two-factor authentication. Prefer an authenticator app or a passkey over a code sent by text when the account offers it.
- Review recovery email and phone numbers. Remove any you do not recognize.
- Check recent logins or “devices” and sign out anything you do not know.
- Turn on account alerts for new logins, password changes, and transfers.

## On your phone and computer

- Install system and app updates. Then restart.
- Use a screen lock (PIN, password, or biometrics). Do not read a passcode to anyone who calls you, even if the voice sounds official.
- Only install apps from the official App Store or Google Play.
- Do not give anyone remote access unless you placed the support call yourself, using a number you already had.
- Forward scam texts to 7726 (SPAM) for U.S. mobile carriers, then delete the thread.

## Tell someone

If this involved a parent, a partner, or a colleague, tell them what the message looked like. Scammers often hit the same workplace or family more than once. You can also forward this kit: cyberexperts.com.

---

CyberExperts publishes plain-English security news every weekday. This kit is free to share. It summarizes official consumer-protection guidance and is not a substitute for legal, tax, or financial advice. Sources: Federal Trade Commission (ReportFraud.ftc.gov, IdentityTheft.gov), FBI Internet Crime Complaint Center (ic3.gov), CISA, Equifax, Experian, and TransUnion credit-freeze pages, all checked in November 2026.