Financial Empowerment

Protecting Your Accounts

A FRAUD AND CYBERSECURITY CHECKLIST

You don't need to be suspicious of every email. Just close the big gaps scammers use.

Federal regulators tell us that most people who lose money were not "hacked" in the technical sense. They were convinced, by a message that looked real, to share a code or move money themselves. This list is built to prevent that.

Your household is only as protected as its least careful member, so anyone who shares your accounts or devices should work through this too.

1. Spotting the approach

- ☐ Treat any call, text, or email that reaches out to you first as unverified, even when it shows your bank's name or a familiar number. Reach out yourself using a number or website you already trust.
- ☐ Use the same rule when a message seems to come from a family member in trouble. Hang up and call them back on the number you already have saved.
- ☐ Be most careful when a message creates urgency, fear, or secrecy. Pressure is a red flag.
- ☐ Never pay for anything, or "protect" your money, with a wire transfer, gift card, cryptocurrency, or a Bitcoin ATM. A real institution will not ask you to.

Source: U.S. Federal Trade Commission · consumer.ftc.gov

2. Locking down your log-ins

- ☐ Use a long, unique password for every important account. A password manager such as Bitwarden, 1Password, or Apple Passwords turns this into the easy choice.
- ☐ Turn on multi-factor authentication everywhere it is offered.
- ☐ Where a site supports passkeys or a physical security key, use them. They cannot be phished the way a texted code can.
- ☐ Protect your email account above all. Whoever controls your email can reset passwords elsewhere.
- ☐ When a site asks you to set security questions, you do not have to answer them honestly. A random answer saved in your password manager cannot be guessed or looked up.

Source: Cybersecurity and Infrastructure Security Agency (CISA) · cisa.gov

3. Protecting your personal information

- ☐ Give out your Social Security number, account numbers, and passwords only in a conversation you started, through a number or website you trust. Never in reply to someone who contacted you.
- ☐ Use a passphrase, several unrelated words strung together, wherever an account allows it.

> **How to build a passphrase**
> Pick four or five unrelated words at random and string them together. Length is what makes it strong, not symbols or numbers. Skip song lyrics and famous sayings, which are easy to guess, then let your password manager remember it for you.
> *Example pattern, then invent your own: copper-lantern-drift-walnut-echo*

- ☐ Never log in through a link inside a message. Type the address yourself or use your saved bookmark.
- ☐ Turn on alerts for money leaving an account, a new account being linked, or a change to your contact information.

Source: U.S. Securities and Exchange Commission · investor.gov

4. Your investment accounts

- ☐ Turn on any transfer or disbursement lock your custodian offers.
- ☐ Add a trusted contact to each account, and complete the Trusted Contact form we fill out together. The SEC, FINRA, and NASAA built this exact tool for moments when someone cannot reach you or suspects exploitation.
- ☐ Ask whether a verbal password can be required for any request made by phone.

Source: SEC, FINRA, and NASAA · finra.org/investors

5. Identity and credit

- ☐ Freeze your credit at all three bureaus (Equifax, Experian, TransUnion), and add a freeze at Innovis and ChexSystems. A freeze is free, backed by federal law, and you lift it in minutes when you apply for new credit. (A credit "lock" is a weaker, often paid, app version of the same idea. You do not need to pay for one.)
- ☐ Get an IRS Identity Protection PIN and renew it each year.
- ☐ Lock your Social Security number against employment fraud with E-Verify's free Self Lock. If you believe your number is already exposed, you can also block electronic access to your SSA record by calling 1-800-772-1213, though that turns off your own online access too.
- ☐ Ask your mobile carrier to add SIM-swap protection to your number.
- ☐ Shred paperwork that shows account numbers or personal details instead of tossing it.

Source: U.S. FTC, IRS, SSA, and Consumer Financial Protection Bureau · consumer.ftc.gov

6. Devices and home network

- ☐ Keep phones, computers, and browsers updated, ideally set to update on their own. Outdated software is one of the most common ways in.
- ☐ Lock every device with a strong passcode or a face or fingerprint unlock, and turn on find-my-device with the option to erase it remotely.
- ☐ Change your router's default name and password, keep its software current, and put smart-home gadgets on a separate guest network.

Source: Cybersecurity and Infrastructure Security Agency (CISA) · cisa.gov

7. If something feels wrong

- ☐ Stop. Do not move money and do not share anything.
- ☐ Contact the institution yourself using the number on your statement, not a number from the message.
- ☐ Call me. A second set of eyes before money moves is a good part of what having someone in your corner is for.
- ☐ Report it at ReportFraud.ftc.gov, even if you caught it in time. It helps investigators and costs you nothing.

Source: U.S. FTC and Consumer Financial Protection Bureau · consumerfinance.gov

8. Plan ahead

- ☐ Name a trusted contact now, while everything is calm.
- ☐ Keep a current list of your accounts and the people who help you manage them. (Our "Where Everything Is" worksheet does this.)
- ☐ Decide who you would call first if something felt off, and tell that person so.

Source: Consumer Financial Protection Bureau and FDIC · fdic.gov

Where to go for help

Report fraud: ReportFraud.ftc.gov Recover from identity theft: IdentityTheft.gov IRS Identity Protection PIN: irs.gov
Investment-account guidance: Investor.gov Ongoing scam alerts: AARP Fraud Watch Network.

Built from public guidance issued by the U.S. Federal Trade Commission, the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Securities and Exchange Commission, the Social Security Administration, the Consumer Financial Protection Bureau, and the FDIC.

This checklist is general information to help you protect your accounts. It is not individual financial, legal, or security advice.

Financial Empowerment LLC · McKinney, TX · empowermenttools.net · Texas-registered investment adviser (CRD #328342)

CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute. CFP® and CERTIFIED FINANCIAL PLANNER™ are certification marks owned by Certified Financial Planner Board of Standards, Inc.