Practical Steps to Protect Your Accounts & Data

Core Vulnerability Reality: Most personal account compromises and financial losses still start with someone being tricked—through a convincing email, text, or phone call—into revealing a password, code, approving a transfer, or clicking bad links. The steps shared below reduce the damage from those attempts and ensure a single mistake won't open the door to the rest of your accounts and personal data.

1 Turn on two-factor authentication (2FA/MFA)

This adds a mandatory second verification step when you log in, ensuring a stolen password alone isn't enough to gain access to your account.

Use an authenticator app (such as Google Authenticator, Microsoft Authenticator, or Authy) or passkeys when available. SMS text verification codes are better than nothing, but remain the weakest option.

The Better Alternative: Passkeys

Passkeys are a newer, significantly more secure alternative to traditional passwords. Instead of typing a password, you unlock your device with your fingerprint, face, or PIN. The private key remains encrypted on your device and never leaves it, meaning it cannot be stolen in a remote corporate breach or phished via a fake website. When a service offers passkeys, use them; if not, fall back to an authenticator app.

FIDO Alliance: What are Passkeys? (Official overview)

WIRED: What Is a Passkey? How to Set Up & Use Them

Apple Users: How to use passkeys on Apple Devices (support.apple.com)

Google/Android: Sign in with a passkey (support.google.com)

2 Use a password manager

A password manager creates, stores, and fills in a unique, strong password for every account. In other words, stop creating your own passwords that you "can remember!" Because what inevitably happens is that you use the same password, or similar versions of your core password, across multiple sites. Once that password is compromised, many of your accounts have a higher risk of being breached.

Main Advantages of a Password Manager

- **One unique password per site:** If one company is breached, your other accounts stay protected because none of them share the same password.
- **Stronger passwords without the memory burden:** The manager generates long, random passwords you never have to remember or type.
- **Faster, safer logins:** It autofills credentials only on the legitimate site, reducing the chance of entering them on a phishing page.
- **Easier multi-device access:** Most managers sync securely across your phone, computer, and browser so you can log in anywhere.
- **Built-in extra security:** Many include password breach monitoring, secure notes for sensitive info, and support for passkeys or two-factor codes.

Popular free or low-cost options include **Bitwarden** (free tier available), **1Password**, and the built-in managers from Apple and Google. For most people, a password manager is one of the highest-impact security steps available.

Protective Safeguards & Email Defense

3 Keep devices updated

Install available updates promptly on phones, computers, browsers, and Wi-Fi routers. Updates patch critical known security holes. Turn on *automatic* updates wherever supported.

4 Isolate smart devices

Move smart TVs, cameras, smart plugs, and speakers onto your home router's guest Wi-Fi network. This prevents a compromised gadget from accessing your personal computers and financial phones.

5 Freeze your credit

Place a free credit freeze with **Equifax**, **Experian**, and **TransUnion** to stop unauthorized accounts from opening in your name. You can unfreeze anytime. This is one of the highest-impact steps for identity defense.

6 Be skeptical of emails, phone calls, and text messages

The greatest source of personal breaches is someone being tricked into providing sensitive data or clicking malicious links. Even with strict spam filters, sophisticated and convincing illegitimate messages slip through weekly. With modern AI tools generating flawless grammar and layout, apply these rigorous checks:

Check the real sender address

Don't trust the friendly display name (e.g., "Your Bank"). Click or tap the name to reveal the complete email address. Look for subtle typos, extra hyphenated words, or domain spoofing (e.g., *support@yourbank-secure.com* instead of *support@yourbank.com*).

Inspection Tip: Email clients frequently use fonts where lookalike characters are hard to tell apart (lowercase "L" vs. capital "I", zero "0" vs. "O", `rn` vs. `m`). Copy the domain text after the @ and paste it into a monospaced font or plain text editor to make anomalies immediately visible.

Preview all links before clicking

On desktop computers, hover your cursor over links (without clicking) to inspect the exact destination URL. On mobile devices, tap and hold the link to preview the target web address. If the domain does not match the official website, do not open it.

Watch for artificial urgency or aggressive threats

Messages that pressure you to "act immediately," threaten that your account will be permanently closed, or demand immediate funds are classic coercive tactics. Reputable institutions rarely impose sudden deadlines by email.

Protecting your financial accounts starts with basic digital hygiene. Taking even two or three of these steps this week makes a substantial and lasting impact on your online safety.

IMPORTANT DISCLOSURES

This communication is for general educational purposes only and does not constitute investment, tax, legal, or other professional technical advice. It is not an offer or solicitation to buy or sell any security.

Cybersecurity threats and technical standards change rapidly; this information is current as of the date issued and may not apply to every personal computing configuration. Consult specialized advisors as appropriate. Ken Melotte is not a cybersecurity or technical specialist.

Melotte Financial Advisors, LLC is a registered investment adviser. Registration does not imply a certain level of skill or training.