

Stay Secure

The Essential Cybersecurity Checklist

By adopting cybersecurity best practices, you can stay vigilant against emerging threats, including risks associated with the rising use of artificial intelligence (AI). This checklist outlines essential steps to enhance your cybersecurity and safeguard your data—and your family’s financial future.

Understanding Cybersecurity Self-Test

Check the box when you feel comfortable with the following concepts:

- ☐ **What is cybersecurity and why is it important?** Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks. It helps safeguard sensitive information and prevent unauthorized access to accounts.
- ☐ **What red flags should I watch for?** Watch for imposter scams where cybercriminals pretend to be someone you know; high pressure demands to act quickly to resolve a problem or claim a prize; and any requests for money, account credentials, or personal information.
- ☐ **How can I protect myself and my transactions?** Preparation is the name of the game. Use strong passwords, understand the threats, defend yourself online, and stay vigilant. The following sections of this checklist will lead you through these concepts.

Password Strength Test

Using strong passwords and passphrases is an easy first step to mitigating cybercrime. Check each box once you’ve completed the action.

- ☐ Set up a password manager to safely create and store passwords online.
- ☐ Revisit your passwords to ensure they have at least 16+ characters. Typically, the longer, the better.
- ☐ When creating passwords, use a combination of numbers, symbols, and words not found in the dictionary.
- ☐ Check that none of your accounts have the same password. If they do, change them.

AI-Related Risks

AI makes it harder to discern what’s real, heightening the risk of falling victim to social engineering scams. Here are some ways to protect yourself:

- ☐ Double check all emails, texts, and calls that request personal information or include a link, even if they seem legitimate.
- ☐ Avoid answering calls from unknown numbers. AI can record your voice and create a “deep fake” that allows criminals to impersonate you.
- ☐ Be suspicious of any communication that seems out of the ordinary, including family emergencies. AI can fake the voice of someone you know.
- ☐ Don’t upload any private information to AI.

Know the Common Traits of Phishing

Phishing is a form of cyberattack where malicious actors impersonate real organizations through email, text, websites, or voice calls to deceive individuals into providing sensitive information. When you agree with each statement, check the box:

- ☐ I understand that **phishing attacks** often use urgent or enticing messages to trick people into clicking fake links or downloading harmful attachments.
- ☐ I am cautious of emails from unfamiliar sources, and those that contain misspellings or bad grammar.
- ☐ I verify the email domains of suspicious emails; sometimes, they can be off by a single character.
- ☐ I do not click on links in suspicious emails, even if they seem to come from a brand or person I trust.
- ☐ I always hang up on callers who request information over the phone or make threats.
- ☐ I am wary of unsolicited text messages, especially those that include an offer, urgent alert, or a link to claim money.

Defend Yourself Online

Online transactions require extra layers of protection to keep your information secure. To defend yourself online:

- ☐ Implement multi-factor authentication (password, PIN, fingerprint, facial recognition, etc.) for all applications that access sensitive information, including banking, email, and personal accounts.
- ☐ Use firewalls and up-to-date anti-virus software, and only access financial accounts from your computer or secure wifi locations.
- ☐ Don't autosave your passwords or sign-on credentials.

Email is Not Secure

Email is unencrypted, meaning anything you send could be viewed by unauthorized parties. To keep your information safe, confirm you understand the following points.

- ☐ Never email personal information to anyone. Use encrypted email or secure portals instead.
- ☐ Never request financial transactions via email.
- ☐ Use verbal communication or secure messaging provided by your financial institution, bank, or financial advisor.
- ☐ Only click links and download documents from known senders.

Have You Been a Victim of Fraud?

If you believe your financial accounts have been compromised or your identity has been stolen, take immediate action:

- ☐ Place a hold on your Wealth Enhancement accounts by contacting your advisor directly using a known, verified number from a previous statement, not a number provided in a suspicious text or email.
- ☐ Close or freeze other compromised accounts by contacting your credit card companies, financial institutions, and investment account custodians.
- ☐ Place a fraud alert on your credit reports by contacting the major credit bureaus:
Experian (888-397-3742 or [experian.com](https://www.experian.com));
Equifax (800-525-6285 or [equifax.com](https://www.equifax.com));
TransUnion (888-909-8872 or [transunion.com](https://www.transunion.com)).
- ☐ Ask the credit bureaus to monitor your credit and flag you if they notice a large movement of money. You can also put a security freeze on your credit reports.
- ☐ File a complaint with the Federal Trade Commission at 1-877-ID-THEFT or [identitytheft.gov](https://www.identitytheft.gov).
- ☐ File a report with the local police. This will provide you with proof to share with creditors who require evidence of criminal activity.

You can also report additional types of fraud here:

- **Tax fraud:** IRS Identity Protection Specialized Unit: 1-800-908-4490
- **Passport fraud:** U.S. Department of State: www.travel.state.gov/passport
- **Phone fraud:** contact your service provider to cancel the account
- **Social Security fraud:** Office of the Inspector General: 1-800-269-0271
- **Investments fraud:** contact your brokerage firm or file a complaint with the SEC
- **Mail fraud:** notify the local postal inspector