UNISON™
RISK ADVISORS

Protecting Your Online Presence

A PERSONAL CYBERSECURITY GUIDE FOR INDIVIDUALS AND FAMILIES

PROTECTING YOUR ONLINE PRESENCE

Cybercriminals increasingly target individuals, not just businesses. Account takeover, identity theft, wire fraud, and social engineering scams cause billions of dollars in personal losses every year, and the most effective defenses are simple habits that take minutes to set up. This guide walks through the practical steps we recommend to every client to reduce personal cyber risk. You do not need to do everything at once.

Start with the Quick-Start Checklist on the last page, then work through the sections below over time.

1 Account Security: Your First Line of Defense

Use a password manager. Reused or weak passwords are behind the majority of account takeovers. A reputable password manager (such as 1Password or Bitwarden) creates and stores a unique, strong password for every account, so a breach at one website cannot unlock the rest of your digital life.

Turn on multi-factor authentication (MFA). MFA requires a second step, such as a code from an app, to log in. Enable it everywhere it is offered, prioritizing email, banking, investment, and retirement accounts. App-based authentication (Microsoft Authenticator, Google Authenticator) or a hardware security key is stronger than text-message codes, which can be intercepted through SIM-swap attacks.

Adopt passkeys where available. Passkeys replace passwords with cryptographic logins tied to your device and are resistant to phishing. Major providers, including Apple, Google, Microsoft, and many banks, now support them.

Protect your email account above all else. Your primary email is the master key to everything: password resets for nearly every account flow through it. Give it your strongest password, the strongest MFA you can, and consider a separate email address used only for financial accounts.

2 Credit and Identity Protection

Freeze your credit at all three bureaus. A credit freeze prevents criminals from opening new accounts in your name. It is free, takes a few minutes per bureau online, and can be temporarily lifted (“thawed”) whenever you apply for credit. Freeze at Equifax, Experian, and TransUnion.

Freeze the lesser-known bureaus, too. ChexSystems covers new bank account openings and NCTUE covers utility and phone accounts. These are frequently exploited and frequently overlooked.

Get an IRS Identity Protection PIN. An IP PIN prevents criminals from filing a fraudulent tax return in your name. Any taxpayer can enroll at IRS.gov.

Set up account alerts. Enable transaction notifications on credit cards and bank accounts so you spot fraud in real time rather than on a monthly statement.

Freeze your children’s credit. Minors are prime identity theft targets because the fraud often goes undetected for years. Each bureau allows parents to create and freeze a credit file for a minor child.

3 Securing Your Devices

- **Keep software updated.** Turn on automatic updates for your operating system, browser, and apps. Most attacks exploit known flaws that patches have already fixed. Replace devices that no longer receive security updates.
- **Lock and encrypt.** Use a screen lock with biometrics or a strong PIN, and enable full-disk encryption (on by default for most modern phones; enable BitLocker or FileVault on computers).
- **Enable find-my-device and remote wipe** so a lost phone or laptop does not become a data breach.
- **Charge safely.** Avoid public USB charging ports; carry your own power adapter or a charge-only cable.
- **Install only trusted apps** from official app stores, and review app permissions periodically.

4 Phishing and Social Engineering

Most successful attacks do not hack technology; they hack people. The common thread is urgency: a message designed to make you act before you think.

- **Verify out-of-band.** If you receive an unexpected request involving money, gift cards, wire instructions, or account credentials, verify it by calling a number you already know, never the number or link provided in the message.
- **Establish a family code word.** Voice-cloning scams now impersonate family members in distress. Agree on a word or question that only your family knows.
- **Never click password-reset or "account problem" links.** Go directly to the website or app instead.
- **Slow down wire transfers.** Before sending funds for a home closing, investment, or large purchase, verbally confirm instructions with a known contact. Fraudulent "changed wiring instructions" emails are among the most financially devastating scams we see.
- **Be skeptical of QR codes** in unsolicited mail, parking lots, and emails; they can route you to credential-harvesting sites.

5 Managing Your Digital Footprint

- **Tighten social media privacy settings** and limit who can see your posts, friends list and personal details.
- **Avoid posting travel in real time.** Share vacation photos after you return home.
- **Starve the security questions.** Birthdays, pet names, schools, and hometowns posted publicly are exactly what criminals use to reset your accounts. Better yet, answer security questions with random false answers stored in your password manager.
- **Remove yourself from data brokers.** Services such as DeleteMe or Optery automate removal of your home address, phone number, and relatives from people-search sites, or you can opt out manually from the major brokers.
- **Search yourself periodically** to see what an attacker, or a scammer researching you, would find.

6 Home Network Security

- **Change your router's default administrator password** and keep its firmware updated.
- **Use WPA3 (or at minimum WPA2) encryption** with a strong, unique Wi-Fi password.
- **Segment smart devices.** Put cameras, smart speakers, TVs, and other Internet-of-Things devices on a guest network so a compromised gadget cannot reach your computers and phones.
- **Disable remote administration** on your router unless you specifically need it.

7 Backups and Breach Response

Follow the 3-2-1 backup rule for irreplaceable data such as photos, tax records, and estate documents: three copies, on two different types of media, with one stored offsite or in the cloud. Backups are also your best defense against ransomware.

Know what to do when, not if, a breach touches you:

- Check exposure at **haveibeenpwned.com** and change any affected passwords immediately, starting with email.
- If identity theft is suspected, file a report and recovery plan at **IdentityTheft.gov** (FTC) and consider a fraud alert in addition to your credit freezes.
- Notify your bank and card issuers promptly; speed matters for recovering fraudulent transfers.
- Document everything, including dates, screenshots, and reference numbers.

8 Additional Steps for High-Profile and High-Net-Worth Individuals

Executives, business owners, public figures, and their families face elevated targeting and should layer on additional controls:

- **Lock your mobile number against SIM swaps.** Ask your carrier to add a port-freeze or number-transfer PIN. SIM-swap attacks are a leading cause of account takeover for high-value targets.
- **Use a dedicated email address, and ideally a dedicated device,** for banking and investment activity.
- **Formalize a wire verification protocol** with your financial advisors, attorneys, and family office: dual approval and verbal callback for any transfer or change to payment instructions.
- **Review household exposure.** Domestic staff, family members, and shared accounts are common entry points; extend these practices to everyone in the household.
- **Consider personal cyber insurance.** Coverage is available for individuals and families, addressing cybercrime losses, identity restoration costs, ransomware, and more. Ask your advisor whether standalone coverage or a homeowners endorsement fits your situation.

A PERSONAL CYBERSECURITY GUIDE FOR INDIVIDUALS AND FAMILIES

Quick-Start Checklist

If you do nothing else this month, complete these ten steps:

- [ ] Install a password manager, update your email, banking and investment passwords first.
- [ ] Enable app-based MFA on email and all financial accounts.
- [ ] Freeze your credit at Equifax, Experian, and TransUnion (and for your minor children).
- [ ] Request an IRS Identity Protection PIN.
- [ ] Add a port-freeze / SIM-swap PIN with your mobile carrier.
- [ ] Turn on automatic updates for all devices.
- [ ] Enable transaction alerts on every card and bank account.
- [ ] Set a family code word for emergencies.
- [ ] Establish a verbal callback rule for any wire transfer or payment change.
- [ ] Back up irreplaceable files using the 3-2-1 rule.

> Questions about your personal cyber risk or available insurance coverage? Contact your risk advisor — we are glad to help you put these protections in place.

UnisonRiskAdvisors.com

UNISON RISK ADVISORS

EMPOWERING YOUR FUTURE, IN UNISON

Unison Risk Advisors™ is a partnership of companies creating one of the nation's largest privately held and employee-owned insurance brokerage and risk management firms. It ranks among the largest brokerage firms and among the top five largest independently owned firms in the country. Unison Risk Advisors serves business and individual clients in 50 states and more than 85 countries. Learn more about our partner firms.

© 2026 Unison Risk Advisors. All rights reserved.