Guarding Against Fraud and Cybercrime

Cybercrime is evolving rapidly, and even the most careful individuals can be targeted and fall victim. With the right habits and vigilance, you can help reduce your risk. This guide outlines key steps to help you protect your personal information, credit, and financial accounts, and provides clear direction on how to respond if something seems suspicious or if you suspect you've been a victim of fraud.

How to Reduce Your Risk

Review your accounts regularly

Monitor statements, trade confirmations, and profile details for accuracy. Look for unfamiliar transactions or changes you didn't make.

Use strong authentication

Enable two-factor authentication on all financial accounts. If available, enable fingerprint or face ID.

Strengthen your passwords

Use long, unique passwords for every account. A password manager is ideal. Avoid saving passwords in your browser, as they are vulnerable to malware.

Protect your home network

- Change the default administrator password on your router.
- Ensure Wi-Fi encryption (WPA2 or higher) is enabled.
- Replace outdated routers that lack modern security.
- Keep computers and devices updated with the latest operating system and security patches.

Keep sensitive information private

Never email Social Security numbers, account numbers, credit card numbers or tax documents. Modera will never ask you to send sensitive information via email. We encourage using our secure client hub.

Be cautious with email, calls, and links

- Caller ID can be spoofed and should not be trusted.
- Be skeptical of urgent or alarming messages. For example, the IRS will never email you requesting personal information or payment.
- Never read back one-time security codes.
- Never give remote access to your computer to an unverified caller.
- Hover over email addresses and links to confirm legitimacy.

Use secure Wi-Fi

Avoid public Wi-Fi for financial activity. Use trusted, encrypted networks or a VPN.

Freeze your credit

A credit freeze restricts access to your credit report, making it significantly harder for criminals to open accounts in your name, even if they have your personal information. Contact information for the credit bureaus is provided toward the end of this document.

Monitor your credit reports

You're entitled to one free report annually from each bureau at AnnualCreditReport.com. Review them for unfamiliar accounts or inquiries.

Fraud Trends to Be Aware Of

Cybercriminals are using more sophisticated tools than ever. These are the most current trends:

AI-Powered Impersonation (Voice, Video and Email)

Criminals can now clone voices or generate convincing fake videos using only a few seconds of audio or images. Be cautious of unexpected calls, emails, or videos requesting money or sensitive information, even if they sound or look familiar.

Text-Message Scams or "Smishing"

Fake alerts claiming your account is locked, a package is delayed, or a payment is due are increasingly common. Never click links in unsolicited texts.

QR Code Scams, "QR Phishing" or "Quishing"

Fraudsters may replace real QR codes with fake ones or send malicious codes by email or text, to steal information, download malware, or redirect payments. Only scan QR codes from trusted sources.

Tech Support Pop-Ups

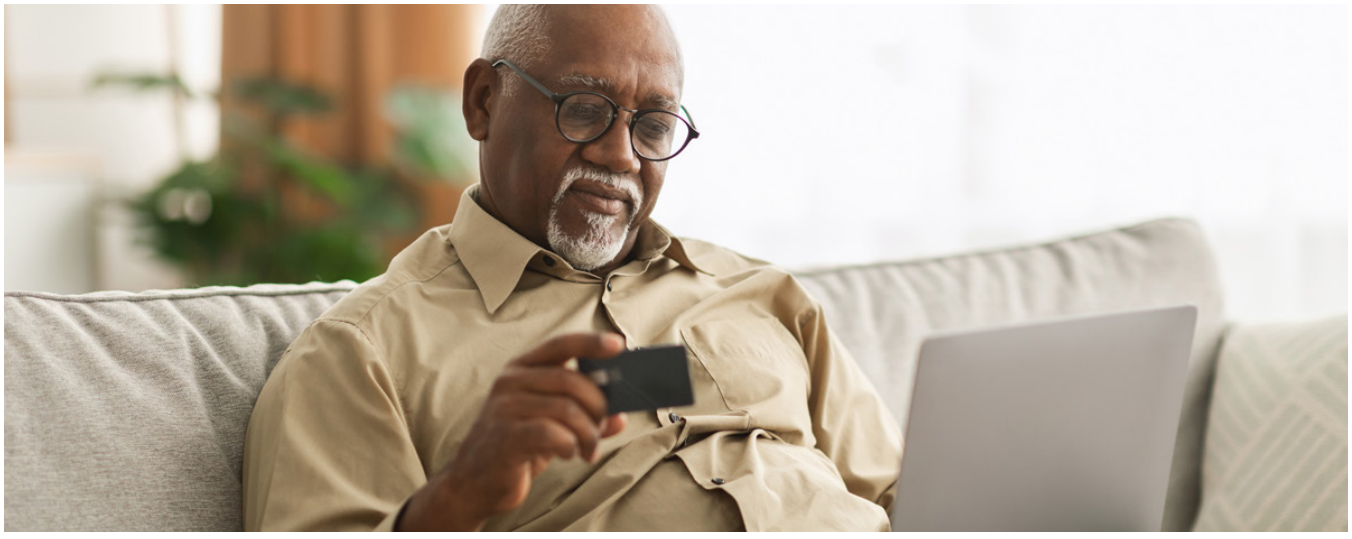
Fake warnings pop up on your device, claim your device is infected and urge you to call a phone number or allow remote access. Close the browser and do not call the number or allow remote access.

Payment App Fraud (Zelle, Venmo, Cash App)

Scammers pressure victims to send money quickly through instant-transfer apps. Treat payment-app transfers like cash. Remember: once sent, payments cannot be reversed.

Social Media Impersonation & Data Mining

Fraudsters use social media apps like LinkedIn, Facebook, and Instagram to impersonate professionals or gather personal details. Limit what you share publicly and be skeptical of unsolicited messages.



Wire Fraud: A Growing Threat

Wire fraud remains one of the most financially devastating forms of cybercrime. Criminals often impersonate trusted contacts, sometimes using AI, to trick victims into redirecting funds.

Key warning signs

- Sudden changes to wiring instructions
- Requests for transfers sent only by email or text
- Messages that create urgency or pressure
- Contact information that doesn't match known records

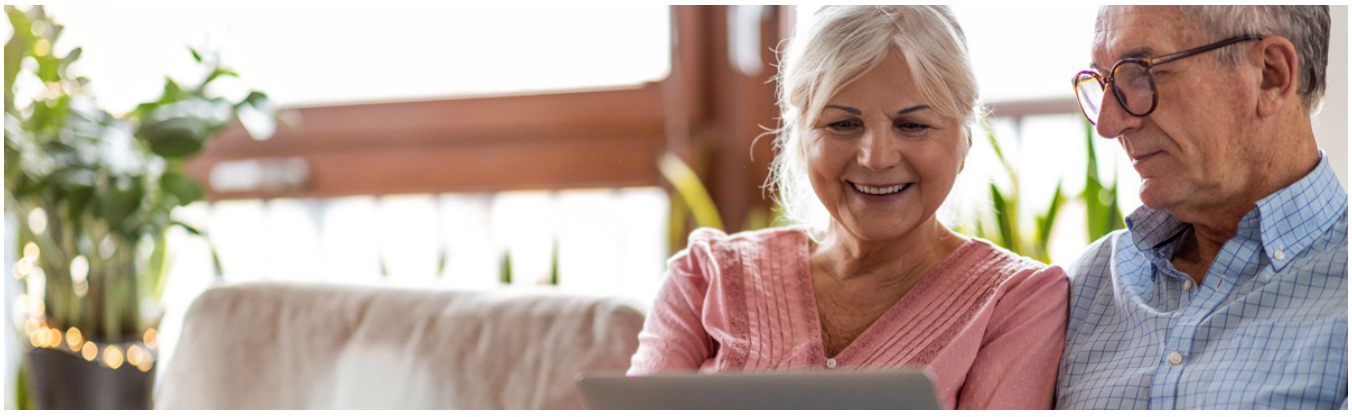
How to protect yourself

- Always verify wiring instructions using a phone number you know is legitimate.
- Never rely on contact information provided in an email.
- Confirm that any outgoing wire you initiate has been received by the intended recipient.
- Be especially cautious during real estate transactions, as this is a major target for fraudsters.

Common Fraud Red Flags to Watch For

- Mail or statements repeatedly returned as undeliverable
- Not receiving account statements you normally receive
- Requests or transactions that don't match your typical behavior
- A change of address followed quickly by a request for credentials or a large transfer
- Emails, calls, or texts claiming to be from Modera asking for sensitive information (we will never do this)
- Unexpected requests to move money or change payment instructions
- Messages that create urgency or pressure you to act quickly
- Requests for login credentials, security codes, or remote access
- Links, attachments, or QR codes you weren't expecting
- Messages from unfamiliar numbers or slightly altered email addresses

If something feels "off," trust your instincts.



How Modera Helps Protect You

Modera invests heavily in cybersecurity, including:

- Regular scans and penetration testing
- Enterprise-grade endpoint protection
- Multifactor authentication and secure VPN
- Cloud-based servers with separate backup data centers
- Strict identity-verification procedures

Our **Asset Transfer Verification Policy** requires a member of your wealth management team to speak with you directly before processing any new transfer request. This added step helps prevent unauthorized movement of your assets. If you ever receive a call that feels suspicious or fraudulent, hang up immediately and contact your advisor using their known phone number.

If You Suspect Fraud or Identity Theft

Secure your accounts immediately:

- Change your usernames and passwords.
- Log out of all devices for the affected account.
- During business hours, contact your Modera team.
- After hours, contact your custodian first:
  - Schwab: 800-435-4000
  - Fidelity: 800-544-6666

If a device appears compromised:

- Stop using the affected device.
- Disconnect it from the internet.
- Seek professional assistance.

Notify the credit bureaus:

- If unauthorized activity is confirmed, report it to one bureau and place a fraud alert. When a fraud alert is placed, they will notify the other credit bureaus.
- Place a credit freeze with each bureau individually:
  - Equifax: 800-525-6285 | equifax.com
  - Experian: 888-397-3742 | experian.com
  - TransUnion: 800-680-7289 | transunion.com

Report the incident to:

- Federal Trade Commission: identitytheft.gov
- Local law enforcement
- Your state Attorney General

Your Modera Team Is Here to Help

We're here to support you with any questions about account security, credit freezes, or best practices. Protecting your financial well-being is a shared effort, and our team is committed to helping keep your information and assets secure.