ADVISER
INVESTMENTS

INVESTOR PROTECTION CHECKLIST

Keeping our clients' information secure is of paramount importance for Adviser Investments. And while we have taken clear, actionable and evolving steps in our own security measures, cyberfraud is always progressing. These threats take various forms and no one is fully immune.

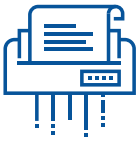
To reduce the likelihood of fraud, we encourage you to adopt a series of measures to protect your identity and mitigate potential security risks. This checklist lays out a number of commonsense steps you can take to help keep your information safe.

We also offer all of our clients access to Adviser Insights, a personal financial website where you can aggregate accounts and securely store important documents in our encrypted digital Vault, which can help check off a number of the actions suggested below.

Financial Account Management

Financial and personal information is increasingly transmitted online, so taking proper safety measures is more important than ever.

RESPONSIBILITIES	STEPS	✔	N/A
Safeguard Your Custodial Accounts	Keep contact information for your custodian close at hand so you can call them immediately if you suspect your account has been compromised. We've listed the custodians we work with below (if you're a client, you should also call your portfolio team ASAP): **Charles Schwab:** 1-800-515-2157 **Fidelity:** 1-800-343-3548 (ask for the Consumer Protection Team) **TDAmeritrade:** 1-800-669-3900 **Vanguard:** 1-877-223-6977	❑	❑
Make a Plan With Your Financial Adviser	If you're not an Adviser Investments client, ask your adviser what they're doing to protect you and what they would do if, for example, they received an email purportedly from you asking for a $10,000 transfer.	❑	❑
Keep Personal Info Up-to-Date	Make sure your cell phone and email address are up to date with every bank, financial adviser and other professional service provider you employ.	❑	❑
Review Statements Regularly	You are your own best defense against fraud. Set a regular time every week or month to review your financial account statements.	❑	❑
Add Alerts	Banks and other financial institutions can alert you by text or email when there's activity in your account—have you activated this service?	❑	❑
Be Unpredictable	Where possible, avoid developing online patterns of money movement, especially regular wire transfers to individuals, that criminals could replicate to make withdrawals look legitimate. (Automatic bill pay services are less easy to mimic and considered safe practices.)	❑	❑
Back Up Info	Regularly back up sensitive data to an external drive and the cloud so you can recover it easily if your computer becomes inaccessible.	❑	❑
Credit Freeze	Consider contacting credit bureaus to enact a "security freeze" that prevents additional accounts from being opened in your name. (Note that it can take several business days to lift a freeze, an important consideration if you need a credit check or are applying for a loan.)	❑	❑
Shred It or Lock It Up	Is your personal information secure? Safely dispose of or store sensitive paperwork in a fire-proof safe or safety deposit box.	❑	❑



Email Essentials

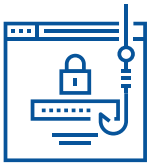
Whenever possible, consider whether the convenience of email outweighs the risk in storing personal and financial information in an email account.

RESPONSIBILITIES	STEPS	✔	N/A
Financial Information	Delete any emails that include detailed financial info beyond the time that they're needed. (Assess whether you *ever* need to store personal/financial data in your email.)	❑	❑
Storing Data	Do you employ data-storage programs to archive critical data and documents? (If you are a client, do you know about the Adviser Insights portal and its encrypted Vault document-storage feature?)	❑	❑
Take Care Clicking Links	Make it a practice to avoid clicking links in unsolicited emails or pop-up ads, especially those warning that your computer may have a virus or offering free software.	❑	❑
Multiple Accounts	Establish a separate email account for financial transactions.	❑	❑
Review Autoreplies	Limit personal information and travel plans in "out-of-office" and other autoreplies.	❑	❑

Device Management

With laptops, smartphones, tablets and watches increasingly interconnected, close attention to their security is a critical defense.

RESPONSIBILITIES	STEPS	✔	N/A
Use Protection	Have you installed the most up-to-date antivirus, antispam and antispyware on all devices (PCs, laptops, smartphones, tablets)? Are your PC and devices password-protected?	❑	❑
Look for Discounts	Ask your bank or custodian if they offer free software or discounts on cybersecurity protection. Many do!	❑	❑
Erect a Firewall	Do you have hardware firewalls set up on your home broadband router and software firewalls on your computer?	❑	❑
Think Twice	Make a list of well-known or trusted sources for downloads or applications. Don't install programs outside of this list.	❑	❑
Be Wary in Public	Ensure that your WiFi is secure. Do not access confidential information via public computers or networks.	❑	❑
Separate Computers	If you have children or other gamers, set up a separate computer to be used solely for games or other online activity and don't access financial accounts on it.	❑	❑



Password Protection

Hackers use a variety of techniques to figure out passwords, including powerful and freely available tools on the internet. Poorly chosen or predictable passwords can leave you at risk for intrusion.

RESPONSIBILITIES	STEPS	✔	N/A
Change It Up	Establish a calendar reminder to reset passwords every three months.	❑	❑
Spread It Out	Do you use different passwords for different accounts?	❑	❑
Keep Them Safe	Avoid storing passwords in email folders.	❑	❑
Use a Pro	Employ a password management program to spare the hassle of having to remember a long list of credentials.	❑	❑
Make It Random	Use a random password generator (available online) to create unpredictable, secure passwords that are very difficult to crack.	❑	❑
Use Your Uniqueness	Enable multifactor authentication (highly recommended for financial accounts or those linked to a credit card) or biometrics such as fingerprint sensors or retina/facial scans if your devices offer that option.	❑	❑

Social Media Safekeeping

Cybercriminals will not only glean personal info from social media sites (Facebook, Twitter), but also those for business networking (LinkedIn) and genealogy (Ancestry.com).

RESPONSIBILITIES	STEPS	✔	N/A
Review Security Settings	Enable and review security settings on social media sites, and do your best to stay informed about current privacy policies.	❑	❑
Be Discrete	Set a time to review your online biographies and limit the level of specific personal details.	❑	❑
Keep Travel Plans Offline	Don't broadcast itineraries, avoid posting photos tagged with faraway locations and refrain from overly revealing status updates ("Our 10-day Paris vacation begins right now!").	❑	❑
No Socials on Social!	Look over your social media to confirm that your Social Security number isn't posted anywhere, even the last 4 digits.	❑	❑

Common Frauds To Avoid

While the frauds listed below all use different approaches, the goal is always the same: To get access to your personal information, financial accounts or extort a payment. When in doubt, independently verify any of the claims being made, and don't be afraid to call a family member, friend or professional contact to help you do so.

THE PIGEON DROP

The right to a large sum of money is promised in exchange for a "good faith" payment withdrawn from an individual's bank account. Con artists will often employ an accomplice posing as a lawyer, banker or other seemingly trustworthy third party.

THE FAKE ACCIDENT

The con artist asks for a wire transfer or check to pay for a relative's urgent medical care. This can be particularly convincing if the scammer has done his homework and researched the names of family members via social media. A similar scam involves calling to say a family member has been arrested and needs money for bail.

CHARITY SCAMS

Where money is solicited for bogus charities. These are especially prevalent after natural disasters. You can use www.charitynavigator.org or www.charitywatch.org to check the validity of any charitable organization before making a donation.

IRS IMPERSONATOR

In this scenario, someone claiming to be from the Internal Revenue Service (IRS) calls to inform you that there is a problem with your tax return or that you owe taxes, and will threaten legal consequences (arrest, lawsuit, revocation of a driver's license or deportation are the most common) to convince you to make an immediate payment. (An alternate version of this scam will have them claiming you are owed a big refund to lure you into sharing personal information instead of seeking payment.) The IRS will never call you if they haven't first mailed a bill, and they will never demand immediate payment without allowing you to question or appeal what you owe. They will also never ask for a credit card number over the phone or require a specific form of payment like a prepaid debit card.

If you get such a call, don't agree to make the payment or share any personal information. Instead, note the number, hang up and then independently verify whatever it is they were claiming through www.IRS.gov/account. (Alternately, you can call the IRS at (800) 829-1040.)

RANSOMWARE

A fraudster posing as a Microsoft or Apple employee calls to alert you that there's a problem with your software. The bogus technician then asks you to log in to your computer and grant him or her access so that they can fix the problem. Then, the scammer locks access to your computer, "kidnapping" it and all of your data until you pay a ransom. Unless you've called them first, real employees of these companies will never call you to preemptively alert you to a problem, and you should not follow their instructions.

Glossary

CYBERSECURITY
The activity or process wherein computers and information are protected and/or defended against damage or theft.

FIREWALL
Hardware or software that limits network traffic to only authorized users or programs.

MALWARE
Software that compromises the operation of a computer system by performing an unauthorized function or process.

PHISHING
A digital form of social engineering to deceive computer users into providing sensitive information or passwords.

RANSOMWARE
Software that threatens to publish or block access to a user's data or computer unless a ransom is paid.

SPYWARE
Software secretly installed onto a computer system without the user's knowledge that can track keystrokes and/or other activity.

VIRUS
A computer program that can replicate itself, infect a computer without knowledge of the user and then spread to another computer.

ABOUT ADVISER INVESTMENTS
Adviser Investments is the adviser you can talk to. We are an independent, professional wealth management firm with expertise in actively managed mutual funds, ETFs, fixed-income investing, tactical strategies and financial planning. We advise more than 3,000 clients with over $5 billion under our care. Our team focuses on helping individual investors, trusts, foundations and institutions meet their long-term investment goals. For more information on how we can help you, please contact us at **(800) 492-6868** or **info@adviserinvestments.com**.