

TIPS FOR PREVENTING FRAUD

Cybercrime and fraud are serious threats and constant vigilance is key. While Summit Financial Strategies plays an important role in helping protect your assets, you can also take action to protect yourself and help secure your information. This guide summarizes common cyber fraud tactics, along with tips and best practices. Many suggestions may be things you're doing now, while others may be new. We also cover actions to take if you suspect that your personal information has been compromised. If you have questions, we're here to help.

Cyber criminals exploit our increasing reliance on technology. Methods used to compromise a victim's identity or login credentials – such as malware, phishing, and social engineering – are increasingly sophisticated and difficult to spot. A fraudster's goal is to obtain information to access your account and assets or sell your information for this purpose. Fortunately, criminals often take the path of least resistance. Following best practices and applying caution when sharing information or executing transactions makes a big difference.

How we can work together to protect your information and assets

Safe practices for communicating with our firm

Keep us informed regarding changes to your personal information, such as your mailing address, email, and phone numbers.

Expect us to call you to confirm email requests to move money, wire funds, or change account information, such as beneficiary designations.

Establish a verbal password with our firm to confirm your identity or request a video chat. Every client at Summit should have such a verbal password on file. Ask one of your team members to confirm your verbal password.

Custodians such as Schwab and Fidelity protect your accounts using a variety of methods. Here are a few techniques unique to each custodian.

Schwab and Fidelity take your security seriously and leverages protocols and policies to help protect your financial assets. Below are actions you can take to reinforce their efforts and resources to assist you in keeping your account safe:

Confirm your identity using Schwab's voice ID service when calling the Schwab Alliance team for support.

Both use two-factor authentication, which requires you to enter a unique code each time you access your accounts.

Review the [Schwab Security Guarantee](#) or [Fidelity Security and Protection](#) to learn how losses would be covered in any of your accounts due to unauthorized activity. To learn more, visit [Schwab's Security Knowledge Center](#) or [Fidelity's Security Overview](#) page. Fidelity's website also includes a helpful guide alerting you and family members to the most common [Elder Fraud Schemes](#).

Follow general best practices

Be suspicious of unexpected or unsolicited phone calls, emails, and texts asking you to send money or disclose personal information. If you receive a suspicious call, do not accept it, hang up, and call back using a known contact number.

Be cautious when sharing sensitive information and conducting personal or confidential business via email, since it can be compromised and used to facilitate identity theft.

Do not disclose personal or sensitive information on social media sites, such as your birthdate, contact information, and mother's maiden name.

Be cautious when receiving money movement instructions via email. Call the sender at their known number (not a number provided in the email) to validate all instruction details verbally before following instructions or providing your approval.

Protect yourself from phishing attempts and malicious links (see glossary for additional information).

Check your email and account statements regularly for suspicious activity.

Do not verbally disclose or enter confidential information on a laptop or mobile device in public areas where someone could potentially see, hear, or access your information.

Verify payment requests you receive by phone or email. Requests for you to make payments using prepaid debit cards, gift cards, or digital currency are frequently associated with fraud or scams.

Keep your technology up to date

Keep your web browser and operating system up to date, and be sure you're using appropriate security settings. Old software, operating systems, and browsers can be susceptible to attack.

Install anti-virus and anti-spyware software on all computers and mobile devices.

Enable the security settings on your applications and web browser.

Do not use free or found USB thumb drives, as these could be infected with viruses or malware.

Turn off Bluetooth when it's not needed to protect against individuals gaining access to your devices using Bluetooth connections.

Safely and securely dispose of old hardware.

Be cautious with public networks

Avoid using public computers. If you must use one, go to the browser settings and clear the browser history (cache) and cookies when you're finished.

Only use wireless networks you trust or that are protected with a secure password.

Use your personal Wi-Fi hotspot instead of public Wi-Fi.

Do not accept software updates if you are connected to public Wi-Fi.

Be strategic with your login credentials and passwords

Do not use personal information such as your Social Security number or birthday as part of your login ID.

Create a unique password for each financial institution you do business with that are long and contain a combination of characters, numbers, and symbols. Consider using a password manager to create, manage, and store passwords that are unique and secure.

Do not share your passwords.

Use two-step verification whenever possible.

Be sure you're on a secure website

Check the URL to see if it's a secure connection. Secure sites begin with https rather than http, and are generally considered safer.

Check the address bar for site validity indicators whenever you log in to a Schwab website. Some browsers use green text or security symbols to indicate a secure and verified site.

Download apps only from the Google Play™ Store or the Apple App Store®.

Do not visit websites you don't know — for example, websites advertised on pop-up ads and banners.

Log out completely to terminate access when you've completed a secure session, such as with online banking or a credit card payment.

Beware of phishing

Do not click on links or attachments in emails and text messages if you question the validity of the sender. Instead, type the real web address, for example <https://www.schwaballiance.com> or <http://www.fidelity.com>, in your browser.

Hover your cursor over questionable links to reveal the site's full URL and see where the link really goes. Do not click on links that don't match the sender or don't match what you expect to see.

Be suspicious of emails that have grayed-out Cc: and To: lines as they may have been sent to a mass distribution list.

Check the sender's domain name in the email address (john.doe@schwab.com) to see if it matches what you would expect to see.

Activate the spam filters in your email settings tab. This will help prevent unsolicited emails from coming to your inbox.

If you suspect an email that appears to be from your account custodian is a phishing email, forward it to phishing@schwab.com or phishing@fidelity.com.

If you have questions about an email from Schwab/Fidelity or personal information you entered about your account after clicking an email link, immediately call the Schwab Alliance team at **800-515-2157** or the Fidelity Team at **800-544-6666**. Please also notify your Summit service team so we are aware of the situation.

What to do if you suspect a breach

Immediately call your Schwab Alliance team at **800-515-2157** or the Fidelity Team at **800-544-6666** so that they can watch for suspicious activity and collaborate with you on other steps to take. Please also notify your Summit service team so we are aware of the situation.

Review [Schwab's Identity Theft Checklist](#) or [Fidelity's Online Security Issue Reporting](#) site for more information.

Glossary

Two-step verification (aka multi-factor authentication)

A method of confirming your identity using a second step to verify who you are. For example, the first step might be to enter your username and password, and the second step might be to enter a randomly generated number sent to you via email, text, phone call, or token.

Phishing

The fraudulent practice of sending emails or text messages appearing to be from reputable companies or trusted individuals in an attempt to get individuals to reveal personal information such as passwords and credit card numbers. Phishing attempts are usually urgent-sounding, legitimate looking emails or texts designed to trick you into disclosing personal information or installing a virus on your device. These scams can be sent as attachments or links that, when opened or clicked, may trigger malicious activity, or take you to fake sites that resemble the real business websites.

Password manager

An encrypted online or cloud-based program that generates, retrieves, and keeps track of random passwords across countless accounts and also protects information such as passwords, PINs, credit card numbers and their three-digit CVV codes, and answers to security questions.

Domain name

As it relates to an email address, this is the information that comes after the @ symbol — for example, schwab.com in jane.doe@schwab.com.

Spam filter

A program that detects unsolicited and unwanted emails and prevents them from reaching your email inbox. Usually, these types of emails are instead sent to a spam folder.

Malware

Software that is intended to damage or disable computers and computer systems.

Learn more

Visit these sites for more information and best practices:

[StaySafeOnline.org](https://www.staysafeonline.org): Review the STOP. THINK. CONNECT™ cybersecurity educational campaign.

[OnGuardOnline.gov](https://www.onguardonline.gov): Focused on online security for kids, it includes a blog on current cyber trends.

FDIC Consumer Assistance & Information:

<https://www.fdic.gov/consumers/assistance/index.html>

FBI Scams and Safety: <https://www.fbi.gov/scams-and-safety>

Disclosure

Information provided in this document is intended to be an overview and is for educational and informational purposes only. The above-mentioned firms and their employees are not affiliated with or employees of Summit, unless otherwise noted. Information provided should not be construed as a recommendation, endorsement of, or sponsorship by Summit of any third party. Any third-party trademarks and service marks appearing herein are the property of their respective owners. Summit does not endorse any vendor, product or service depicted in this publication, and advises technology users to carefully review any security product vendors prior to using their products or services. Experiences expressed are no guarantee of future performance or success and may not be representative of you or your experience. Summit is not affiliated with Charles Schwab & Co. or with Fidelity Brokerage Services, LLC.