Tips for preventing fraud

Fraud and cybercrime are serious threats, so constant vigilance is key. Our firm plays an important role in helping safeguard your assets, but you can also take action yourself to protect and help secure your information. This checklist summarizes common cyber fraud tactics, as well as security tips and best practices. Some suggestions may be things you're doing already, whereas others may be new to you. 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 to sell your information for this purpose. Fortunately, criminals often take the path of least resistance. Following best practices and applying caution when sharing information and 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
- **Expect us to call you to confirm email requests** to trade, move money, or change account information
- **Establish a verbal password** with our firm to confirm your identity—or request a video chat

How Schwab protects your account

Schwab takes your security seriously and leverages protocols and policies to protect your financial assets. The following are actions you can take to reinforce these efforts, as well as resources to keep your account safe.

- **Confirm your identity** using Schwab's voice ID service when calling the Schwab Alliance team for support
- **Use two-factor authentication**, which requires that you enter a unique code each time you access your Schwab accounts
- **Review the** Schwab Security Guarantee, which covers losses in any of your Schwab accounts due to unauthorized activity

To learn more, visit Schwab's Client Learning Center.

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, hang up, then call the client back, using a known contact number.
- **Be cautious when sharing sensitive information** and conducting personal or confidential business via email because it can be compromised and used to facilitate identity theft.

- **Do not disclose on social media sites personal or sensitive information**, such as your birth date, 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 verbally validate all instruction details 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 payment using gift cards, prepaid debit 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 are more susceptible to attack.
- **Install anti-virus/anti-malware/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**—they 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.
- **Use only 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 birth date as part of your user ID.
- **Create a unique password** for each financial institution with which you do business; use passwords 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 whether 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 into a Schwab website. Some browsers use green text or security symbols to indicate a secure and verified site.
- **Download apps only from Google Play or Apple's App Store.**
- **Do not visit websites you don't know**—such as those advertised in pop-up ads and banners.
- **Log out completely** to terminate access when you've completed a secure session, such as for 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, such as **https://www.schwaballiance.com**, in your browser.
- **Hover 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—they may have been sent to a mass distribution list.
- **Check the sender's domain name in the email address**, such as **john.doe@schwab.com**, to see if it matches what you would expect to see.
- **Activate the spam filters** in your email settings to help prevent unsolicited emails from going to your inbox.
- If you suspect that an email appearing to be from Schwab is a phishing email, forward it to **phishing@schwab.com**.
- **If you have questions about an email from Schwab** or personal information you entered about your Schwab account after clicking an email link, call your advisor or the Schwab Alliance team immediately at **800-515-2157**.

What to do if you suspect a breach or fraud

- Call my office or your Schwab Alliance team immediately at **800-515-2157** so that they can watch for suspicious activity and collaborate with you on other steps to take
- Request Schwab's **How to Respond to a Data Breach** flyer for more information

Glossary

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**.
malware	Software that is intended to damage or disable computers and computer systems.
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.
phishing	The fraudulent practice of sending emails or text messages appearing to be from reputable companies or trusted individuals in an attempt to get users to reveal personal information such as passwords and credit card numbers. Phishing attempts are usually legitimate-looking, urgent-sounding 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 websites that resemble legitimate business sites.
spam filter	A program that detects unsolicited and unwanted emails and prevents them from reaching your inbox. Usually these types of emails are instead routed to a spam or junk folder.
two-step verification	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 user ID and password, and the second step might be to enter a randomly generated number sent to you via email, text, token, or phone call. Also known as *multi-factor authentication.*

Learn more

Visit these sites for more information and best practices:

- National Cybersecurity Alliance > **StaySafeOnline.org**
- Federal Trade Commission > **OnGuardOnline.gov**
- Federal Deposit Insurance Corporation > **Consumer Assistance Topics**
- Federal Bureau of Investigation > **Scams and Safety**