charles SCHWAB

Tips for preventing fraud

While cybercrime and fraud are serious threats, you can take practical steps to protect your identity and assets. To reduce your exposure to fraud and reinforce your efforts, Schwab also has mechanisms in place to help safeguard your data and accounts.

You can also have an impact on safeguarding your information and assets by following the guidelines below and applying caution when sharing information and executing transactions. This checklist summarizes common cyber fraud tactics, along with tips, best practices, and actions to take if you suspect a breach.

Ways to protect your information and assets

Safe practices for working with your advisor

- Talk with your advisor to understand how he or she protects your information and assets.
- Keep your advisor informed regarding changes to your personal information.
- Expect your advisor or their office to call you to confirm email requests to move money, trade, or change account information.
- Establish a verbal password with your advisor's firm to confirm your identity, or request a video chat.

How we protect your accounts

Schwab leverages protocols and policies to help protect your financial assets. Below are actions you can take to reinforce our efforts:

- Confirm your identity using Schwab's voice ID service when calling the Schwab Alliance team for support.
- Use two-factor authentication, which requires a unique code each time you access your Schwab accounts.
- Review the Schwab Security Guarantee (Schwab.com/Schwabsafe), which covers 100% of losses in any of your Schwab accounts due to unauthorized activity.

To learn more, visit Schwab's Client Learning Center (Content.Schwab.com/LearningCenter).

What you can do

- Be aware of suspicious phone calls, emails, and texts asking you to send money or disclose personal information. If a "service rep" calls you, hang up and call back using a known phone number.
- Never share sensitive information or conduct business via email, as accounts are often compromised.
- Beware of phishing and malicious links. Urgent-sounding, legitimate-looking emails are intended to tempt you to accidentally disclose personal information or inadvertently install malware.
- Don't open links or attachments from unknown sources. Enter the web address in your browser.
- Check your email and account statements regularly for suspicious activity.
- Never enter confidential information in public areas. Assume someone is always watching.

Exercise caution when moving money

- Speak with your advisor about how to leverage our electronic authorization tool – the fastest, most secure way to verify requests when moving money.
- Review and verbally confirm all disbursement request details thoroughly before providing your approval, especially when sending funds to another country. Never trust wire instructions received via email.

Adhere to strong password principles

- Don't use personal information as part of your login ID or password and don't share login credentials.
- Create a unique, complex password for each website and change it every six months. Consider using a password manager to simplify this process.

Maintain updated technology

- Keep your web browser, operating system, antivirus, and anti-spyware updated and active.
- Do not use free/found USB devices. They may be infected with malware.
- Check security settings on your applications and web browser. Make sure they're strong.
- Turn off Bluetooth when it's not needed.
- Dispose of old hardware safely by performing a factory reset or removing and destroying all storage data devices.

Use caution on websites and social media

- Do not visit websites you don't know (e.g., advertised on pop-up ads and banners).
- Log out completely to terminate access when exiting all websites.
- Don't use public computers or free Wi-Fi. Use a personal Wi-Fi hotspot or a virtual private network (VPN).
- Hover over questionable links to reveal the URL before clicking. Secure websites start with "https," not "http."
- Be cautious when accepting "friend" requests on social media, liking posts, or following links.
- Limit sharing information on social media sites. Assume fraudsters can see everything, even if you have safeguards.
- Consider what you're disclosing before sharing or posting your résumé.

What to do if you suspect a breach or fraud

- Call your advisor or the Schwab Alliance team immediately at 800-515-2157.
- Ask your advisor if they have used our "How to Respond to a Data Breach" flyer or have additional recommendations.

Learn more

- StaySafeOnline.org: Review the STOP. THINK. CONNECT™ cybersecurity educational campaign.
- 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 provides additional tips: https://www.fbi.gov/scams-and-safety.