Tips for preventing fraud

Cybercrime and fraud are serious threats and constant vigilance is key. While Stonnington Group plays an important role in helping protect your investment assets, you can also take action to protect yourself and help secure your information. This checklist 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 to 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.
- **Expect us to call you to confirm email requests** to move money, trade, or change account information.
- **Establish a verbal password** with our firm to confirm your identity, or request a video chat.

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 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

☐ Review and verbally confirm all disbursement request details with us thoroughly before providing your approval, especially when sending funds to another country. Never trust wire instructions received via unsecure email. We will send you confidential, financial and/or personal information and documents via secure email or via an encrypted and secure web portal.

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 using a random combination of upper and lower case letters, numbers and symbols/special characters (if applicable). Change them 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 activate the firewall.

☐ 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

☐ Call us at (818) 444-0600 so we can watch your investment accounts for suspicious activity and collaborate with you on other steps to take.

☐ See also our "How to Respond to a Data Breach" flyer for more information and steps to take in the event your are the victim of a data breach whether large scale or individually.

Learn more

Visit these sites for more information and best practices:

- 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.