# TIPS FOR PREVENTING FRAUD

Fraud is a serious threat to your financial well-being, and our growing reliance on technology is making us ever more vulnerable to online criminal activity. A hacker or fraudster's goal is to obtain information to access your account and assets, or to sell your information. The online methods used by cyber criminals to compromise a victim's identity or login credentials – such as malware, phishing, and social engineering – are increasingly sophisticated and difficult to spot. Fortunately, criminals often take the path of least resistance. We can make their "job" harder, by following best practices and applying caution when sharing information or executing transactions.

PPS has stringent anti-fraud processes in place, and we urge you to consider strengthening your defenses. Below are some common cybercrime and fraud tactics, along with tips and best practices. Some suggestions may be things you're doing now, while others may be new. If you have questions, let us know. We're here to help.

## EMAIL IS NOT SECURE


Cyber criminals are very savvy. It's not uncommon for them to monitor a hacked email account for weeks or months before striking with legitimate-looking communications that mimic the victim's writing style and reference prior emails and activities. Access to a victim's email also means a fraudster can replace valid wire transfer details with instructions that send the funds to the thief's bank account, or capture images of a victim's signature for later use on forged requests for funds or sensitive information.

- **Always use an encrypted channel, not email, to send personal information.** Let us know when you are ready to return completed forms or provide sensitive data. We can help you initiate an encrypted channel, or start the exchange from our end.
- When moving money, **consider leveraging your custodian's electronic authorization tool** to verify/authorize requests. Featuring built-in safeguards, this is the fastest and most secure way to move money.
- **Expect us to call you to confirm electronic requests** to move money, trade, or change account information.
- If you ask us to arrange a wire transfer to a third party, **verbally confirm all details with the wire recipient – don't rely on their email**. We are always available to assist and can set up a conference call with all parties to ensure we have the correct information.

## BE WARY OF EMAILS, TEXTS AND PHONE CALLS ASKING YOU FOR PERSONAL INFORMATION OR MONEY

Urgent-sounding phone calls and legitimate-looking texts and emails are intended to tempt you to accidentally disclose personal information or download malware.

- **Do not respond to unexpected emails, texts or phone calls requesting confidential information** or money, if you can't independently confirm its' authenticity. No legitimate organization should make such a request out of the blue.
- If a caller claims to be from a company you do business with, **hang up and call back using a known phone number**, even if the caller has some details regarding your account or dealings with them. Use the number on the back of a credit or debit card….not the number provided by the caller.

## STAY SAFE ONLINE

The Internet is a powerful and useful tool, but in the same way that you shouldn't drive without buckling your seat belt, you shouldn't venture online without taking some basic precautions.


- Keep the web browser, operating system, software, antivirus, anti-spyware, and applications **updated on all of your devices**. This is the best defense against new viruses, malware and other online threats.
- **Check the security settings** on your applications and web browser. Make sure they are strong.
- Turn off Bluetooth when it's not needed.
- **Don't open links or attachments from unknown sources**; they may contain viruses or malware.
- Hover over questionable links to reveal the URL before clicking. **Secure websites start with "https," not "http."**
- **Check your email and account statements regularly** for suspicious activity.
- Don't use personal information as part of your login ID or password and don't share login credentials.
- **Never use the same password on different accounts**. Create a unique, complex password (include letters, numbers and characters) for each website, and change passwords regularly. Consider using a password manager to simplify the process.
- Never enter confidential information in public areas, or when using public computers or free Wi-Fi.

## WHAT TO DO IF YOU SUSPECT A BREACH

- IMMEDIATELY call our office and your custodian (Schwab Alliance: 800-515-2157) so that we can watch for suspicious activity on your account and collaborate with you on other steps to take.
- Refer to our "How to Respond to a Data Breach" flyer for more information.

## 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.