Stonnington Group

PROTECT YOUR ON-LINE SAFETY

We at Stonnington Group want to take this opportunity to remind our clients of the importance of protecting their personal information, particularly online and keeping their financial accounts secure.

Cyber fraud continues to increase at an exponential pace not only in this industry but in just about every aspect of one's life. Data breaches of various institutions from banks, credit reporting services to retail stores where customer information is stolen and sold also continues apace. Cyber fraud cases particularly involve instances where hackers illegally gain access to a customer's email account to then request that the financial advisor wire funds to an account they control are becoming more and more sophisticated.

While vigilance on your part is essential, as part of increased security, we have adopted procedures to respond to customer requests for the transfer/withdrawal of cash and securities. Any request to Stonnington to transfer/withdraw cash or securities to a "new" or previously unknown account, payee or address, Stonnington may contact you through alternative methods to verify your identity and/or instructions prior to entering the order. Custodians will also continue to require your signed Letter of Authorization or their applicable money movement request form. Signatures may also be compared against legitimately signed client documents to try and detect any instances of forgery.

We have also instituted methods to send encrypted and secure email that involves confidential or personal information or documents containing confidential or personal information.

Stonnington Group

Additional Safety Steps You Can Take:

- Notify Stonnington immediately if your email account has been compromised.
- Be sure Stonnington has your current contact information, including your mailing address and email address.
- Do not use your email address as your login for access to your online banking or investment account websites; consider creating separate user IDs instead to login to your financial institutions' websites.
- Create longer passwords using a combination of upper and lower case letters, numbers and symbols (e.g. # $@% if available) in random order. Do not create passwords based on any of your personal information, (e.g. name, nickname, date of birth, etc.) Do not use the same password(s) to login into your financial institutions' websites.
- Read your financial accounts statements promptly to make sure all transactions shown are ones that you actually made.
- Think twice before you respond to emails requesting personal information.
- Use extra caution with wireless connections, public wi-fi "hotspots".
- Do not click on any attachments or links in emails from email addresses you do not recognize;
- Beware of phishing emails (emails purporting to be from legitimate business you may have accounts with) Do not provide any personal or account information by clicking on link in an email purporting to be from a company you do business with. Logon directly to the company's website with your login credentials instead to verify the request is valid and provide/update the information
- If you have been the victim of a data breach or hacking where your financial, personal information has been compromised or potentially compromised, please see our companion document "How to Respond to a Data Breach" for more information and steps to consider taking.

Stonnington Group

For More Information & Additional Resources:

- Identity Theft – http://www.finra.org/Investors/ProtectYourself/P037885
- Phishing Scams – http://onguardonline.gov; www.sec.gov/investor/pubs/phishing.htm

Questions:

If you have any concerns or questions you would like to discuss with us, please give us a call at 626.469.8166 .