



SHAPIRO FINANCIAL SECURITY GROUP, INC.

"PLANNING IS THE KEY TO SECURITY"

Financial Planning, Investment and Tax Planning Specialists

1 Bethany Road
Building 6, Suite 90
Hazlet, NJ 07730

Toll Free (800) 229-0168
P. (732) 739-8991 F. (732) 739-8667
www.ShapiroFSG.com

March 31, 2015

Dear Valued Client,

Keeping your information secure from criminals is a top priority for our firm. To better protect you and your accounts from cybersecurity threats, we continuously review security procedures to ensure that we are following best practices recommended by the custodians, financial institutions, and industry experts with whom we work.

While we feel we are taking clear and actionable steps in our own firm's security measures, cyber fraud continues to escalate, is becoming more sophisticated, and is ever changing. These threats take various forms, including email scams (e.g., phishing), where criminals obtain investors' identity and use that information to commit various forms of wire fraud.

The checklist in this letter describes these phishing scams and other tactics that we believe investors should be aware of.

As a fiduciary to your financial accounts, we are encouraging our clients to embrace a series of measures to help protect their identity and mitigate potential security risks. This investor protection checklist outlines some best practices for investors across six key areas to help you:

- Manage your devices
- Protect all passwords
- Surf the Web safely
- Protect information on social networks
- Protect your email accounts
- Safeguard your financial accounts

Please carefully review this checklist with all members of your household.

We also ask that you do the following:

- If you change a current address, notify us so that we can update our records.
- If you suspect that your email account has been compromised, call us immediately.
- If you suspect that your Fidelity account has been compromised, call us immediately.

If it's after business hours, call us and call 1-800-FIDELITY and ask for the Customer Protection Team to inform them of suspicious account activity.



Do not hesitate to contact us with questions or concerns about how we protect your accounts or the steps you and your family can take to better protect yourselves and mitigate risk. As always, we appreciate the opportunity to help you achieve your financial goals.

Common tactics used to steal identity and login credentials:

Some of the most common tactics criminals use to compromise a victim's identity or login credentials are described below. After gaining access to an investor's personal information, criminals can use it to commit various types of fraudulent activity.

◎ **Malware.** Using malicious software (hence, the prefix "mal" in malware), criminals gain access to private computer systems (e.g., home computer) and gather sensitive personal information such as Social Security numbers, account numbers, passwords, and more.

How it works: While malware can be inserted into a victim's computer by various means, it often slips in when an unwary user clicks an unfamiliar link or opens an infected email.

◎ **Phishing.** In this ruse, the criminals attempt to acquire sensitive personal information via email. Phishing is one of the most common tactics observed in the financial services industry.

How it works: Masquerading as an entity with which the victim already has a financial relationship (e.g., a bank, credit card company, brokerage company, or other financial services firm), the criminals solicit sensitive personal data from unwitting recipients.

◎ **Social engineering.** Via social media and other electronic media, criminals gain the trust of victims over time, manipulating them into divulging confidential information.

How it works: Typically, these scammers leverage something they know about the person—like their address or phone number—to gain their confidence and get them to provide more personal information, which can be used to assist the criminal in committing fraud.

Social engineering has increased dramatically, and many times fraudsters are contacting investors by telephone.

The action items presented in the following investor protection checklist are intended to help you and your family better protect yourselves against such activity.

Investor Protection Checklist

The educational checklist presented below is designed to help you take appropriate action to better protect you and your family and mitigate risk of cyber fraud. Carefully review the items in each of the categories below to determine which apply to your unique situation.

TOPICAL AREA	ACTIONS TO CONSIDER	CHECK WHEN COMPLETED
Manage your devices	<ul style="list-style-type: none"> • Install the most up-to-date antivirus and antispyware programs on all devices (PCs, laptops, tablets, smartphones) and update these software programs as they become available. These programs are most effective when users set them to run regularly rather than just running periodic scans, which may not provide maximum protection to your device. • Access sensitive data only through a secure location or device; never access confidential personal data via a public computer, such as in a hotel or cybercafé. • If you have children, set up a separate computer they can use for games and other online activities. 	<ul style="list-style-type: none"> <input type="checkbox"/> I've reviewed and understand all the items in this topical area. <input type="checkbox"/> I've taken action for those that apply to my situation.
Protect all passwords	<ul style="list-style-type: none"> • Use a personalized custom identifier for financial accounts you access online. Never use your Social Security number in any part of your login activity. • Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships. • Avoid storing passwords in email folders. Consider using a password manager program. 	<ul style="list-style-type: none"> <input type="checkbox"/> I've reviewed and understand all the items in this topical area. <input type="checkbox"/> I've taken action for those that apply to my situation.
Surf the Web safely	<ul style="list-style-type: none"> • Do not connect to the Internet via unsecured or unknown wireless networks, such as those in public locations like hotels or cybercafés. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data. 	<ul style="list-style-type: none"> <input type="checkbox"/> I've reviewed and understand all the items in this topical area. <input type="checkbox"/> I've taken action for those that apply to my situation.
Protect information on social networks	<ul style="list-style-type: none"> • Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birthdate, home address, and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays, or loss of loved ones. Sharing too much information can make you susceptible to fraudsters and allow them to quickly pass a variety of tests related to the authentication of your personal information. Never underestimate the public sources that individuals will use to learn critical facts about people. 	<ul style="list-style-type: none"> <input type="checkbox"/> I've reviewed and understand all the items in this topical area. <input type="checkbox"/> I've taken action for those that apply to my situation.
Protect your email accounts	<ul style="list-style-type: none"> • Delete any emails that include detailed financial information beyond the time that it's needed. In addition, continuously assess whether you even need to store any personal and financial information in an email account. • Use secure data storage programs to archive critical data and documents. • Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those that warn that your computer is infected with a virus and request that you take immediate action. • Establish separate email accounts for personal correspondence and financial transactions. 	<ul style="list-style-type: none"> <input type="checkbox"/> I've reviewed and understand all the items in this topical area. <input type="checkbox"/> I've taken action for those that apply to my situation.
Safeguard your financial accounts	<ul style="list-style-type: none"> • Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held. • Never send account information or personally identifiable information over email, chat, or any other unsecure channel. • Suspiciously review any unsolicited email requesting personal information. Further, never respond to an information request by clicking a link in an email. Instead, type the Web site's URL into the browser yourself. • Avoid developing any online patterns of money movement, such as wires, that cyber criminals could replicate to make money movement patterns appear more legitimate. 	<ul style="list-style-type: none"> <input type="checkbox"/> I've reviewed and understand all the items in this topical area. <input type="checkbox"/> I've taken action for those that apply to my situation.