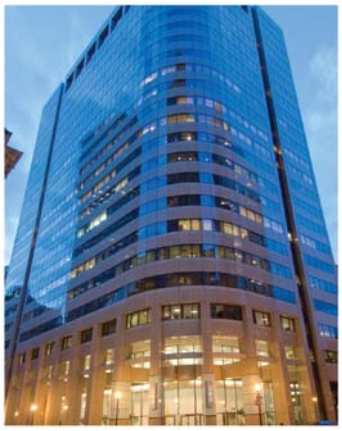
TFC FINANCIAL
The Financial Counselors

TECHNOLOGY UPDATE
DECEMBER 1, 2015

OUR VIEW



Protecting Your Personal Information

The SEC's Office of Investor Education and Advocacy is distributing cybersecurity notices more frequently to the investment community, and at TFC, keeping your information secure from cyber criminals is a top priority. To better protect you and your accounts from cybersecurity threats, we continuously review our internal security procedures to ensure that we are following best practices recommended by the industry experts with whom we work. As we continue to take clear and actionable steps in our own firm's security measures, cyber fraud escalates and fraudsters are becoming more sophisticated.

Investor Bulletin: Protecting Your Online Brokerage Accounts from Fraud
Securities and Exchange Commission (SEC) Investor Alerts and Bulletins: Feb. 3, 2015
http://investor.gov/news-alerts/investor-bulletins

Keeping your information secure from cyber criminals is a top priority.

The purpose of this communication is to make you aware of the various forms of cyber fraud and to provide useful tips to protect your personal information.

Common Cyber Tactics

Below is a list of common tactics used to steal identity and login credentials:

- *Malware* – Criminals using malicious software to gain access to your private computer to gather sensitive personal information such as your Social Security number, account numbers, passwords, and more.
- *Phishing* – Criminals attempt to acquire sensitive personal information via email by masquerading as an entity with which you already have a financial relationship like a bank, credit card company, brokerage company, or other financial services firm.
- *Social engineering* – Criminals using social media to gain your trust over time by manipulating you into divulging confidential information.

Protocols for Preventing Identity Theft

As a fiduciary to your financial accounts, we encourage you to review the useful tips below to help protect your identity and mitigate potential security risks:

Did you KNOW?

A 10-character password can be cracked in 3 months, but a 12-character password can take more than 12 YEARS!

- *Manage your devices* – Install the most up-to-date antivirus and anti-spyware programs on all your devices such as PCs, laptops, tablets and smartphones and update these software programs as they become available. Access sensitive data only through a secure location or device and never access confidential personal data via a public computer. If you have children, make sure they use a separate computer for games and other online activities.
- *Protect all passwords* – Use a personalized custom identifier for financial accounts you access online and never use your Social Security number in any part of your login activity. Avoid using the same password across accounts and reset your passwords at least every 90 days. Never share User IDs or passwords. Consider using a password manager/vault program for storing passwords.
- *Surf the Web safely* – Do not connect to the Internet via unsecured or unknown wireless networks such as those found in public places.
- *Make sure the website is secure* - Look for the "s" after the "http" in the address bar of a webpage to ensure that your personal data is being transmitted across an encrypted channel to avoid unwanted parties from intercepting your personal information.
- *Protect information on social networks* – Be careful with the amount of personal information you post on social networking sites and never post your Social Security number. Sharing too much information could possibly make you susceptible to fraudsters.
- *Protect your email accounts* – Delete any emails that might contain financial or personal information beyond the time that it's needed and only use secure data storage programs for archiving documents. Review unsolicited emails carefully and never click on links in the body of the email or in pop-up ads.
- *Safeguard your financial accounts* – Review all your credit card and financial account activity on a regular basis for unauthorized transactions. Never send personally identifiable or account information over email or any other unsecure channel.

TFC FINANCIAL
The Financial Counselors

Access sensitive data only through a secure location or device and never access confidential personal data via a public computer.

How TFC Can Help

Please be sure to review the above information with all members of your household. We also ask that you do the following:

- If you change a current address (postal or email), verbally notify us so we can update our records as well as your custodian (Schwab, Fidelity or National Advisors Trust).
- If you suspect that your email account and or custodial account has been compromised, please call us immediately, as we will provide guidance on how to best notify the proper financial institutions.

If you have any questions or concerns about any of this information, please don't hesitate to contact your Advisor or a member of the TFC Client Service Team.

Sincerely,

TFC Client Service
tfcclientservice@tfcfinancial.com

Elisabeth Christino: *617-210-6715*
Cara McCartin: *617-210-6700*
Michelle Volpe: *617-210-6721*
Constance Wyllie: *617-210-6725*