SCHULTZ COLLINS
INVESTMENT COUNSEL

Online Security II

(October 8, 2020)

Due to the Covid-19 shelter-in-place rules, many of us are spending additional time online at home. Unfortunately, unscrupulous cyber communities have attempted to take advantage of the situation with an increase in so called “phishing attacks” on many of our home computers. ***Clearly, cyber security is more important than ever.*** Hightower and Schultz Collins have recently created and distributed guidance on this topic.

Hightower’s Cyber security vendor ProofPoint released a series of on-line tutorials describing how to identify many of the different types of Phishing attacks. There are eight different scenarios presented, and the tutorials are interactive: they walk the reader through the key tell-tale signs of an attack and describe how to differentiate between a legitimate message and a bogus one.

The following are the training modules available:

- Fake Browser Updates
- Fraudulent Shipping Notifications
- Lookalike Websites Trick Users
- Scammers Mimic Real Banking Emails
- OneDrive Phishing Campaign
- Phishing Campaign Delivers Dangerous Trojan
- DocuSign Phishing
- Microsoft Office 365 Credential Phishing

The web site for the tutorials can be found at https://www.proofpoint.com/us/learn-more/attack-spotlight/content. We urge you to take the time to go through each module to get a better understanding of what the different attacks look like.

As a reminder, last holiday season Schultz Collins sent out an email and posted to our website an article regarding Online Security. It was a short read covering many of the same topics, but it also discussed other ways to keep you safe in the online world. Items such as:

- Password Security
    - Use different email/password combinations for different sites. At a minimum you should have one set of credentials to use for online financial activity (banking, investments, etc.) and another for general usage (email and the like)
    - Use a password vault to help “remember” credentials and thus encourage the use of multiple credential combinations

  - Passwords should be long and complex (letters, numbers, symbols and at least twelve characters)
  - Change your passwords at least every six months, three months is better
- Two-Factor Authentication and other authentication tools
- Schultz Collins' "Trusted Contact" and "Secret Word" protocols
- Keep your computer and its associated cyber security systems up-to-date

The HT and Schultz Collins presentations give complementary information on many of the same topics and are both worth reviewing.

Should you find yourself the victim of an attack these are a few things you should consider doing immediately, depending on the severity of the breach:

- Contact your financial advisor
- Contact your banking and credit card issuers, especially those immediately affected
- Check your credit reports for any new or suspicious activity
- Freeze your credit reports (prevents anyone from signing up with for new credit with your stolen information). Thanks to a new federal law that went into effect September 21, 2018, there are no longer charges to freeze/unfreeze your credit file (details on the law https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here)
- Put a fraud alert on your credit report. By the same law change above, these now last a year, rather than 90 days
- Obtain copies of your credit report. In the case of fraud or identity theft these are usually free upon request from all bureaus every 12 months
  - https://www.consumer.ftc.gov/articles/0155-free-credit-reports
  - https://www.annualcreditreport.com
- Change your email password(s)
- Change your login credentials to all financial sites
- It may be a good idea to file a police report regarding the breach, as your insurance company may require it for any claims filed
- Report the theft/breach to the FTC (https://www.identitytheft.gov)
- Contact telephone and utility companies
- (Ongoing) Monitor your credit report for any activity. If you have frozen your report there should be no activity
- Subscribe to an Identity Protection service such as Lifelock, Identity Guard, PrivacyGuard or many others
- Other suggestions can be found at https://identitytheft.gov/Steps

Your safety is paramount to us and we hope you find the information provided here and through the other presentations not only educational and but also reassuring.

Kenneth S. McMurray
SCI Information Technologist

Third-party links and references are provided solely to share social, cultural and educational information. Any reference in this post to any person, or organization, or activities, products, or services related to such person or organization, or any linkages from this post to the web site of another party, do not constitute or imply the endorsement, recommendation, or favoring of [Insert Team Name] or Hightower Advisors, LLC, or any of its affiliates, employees or contractors acting on its behalf. Hightower Advisors, LLC, does not guarantee the accuracy or safety of any linked site.