ARTICLE OF INTEREST

Don't Be Caught Off Guard by a Phishing Attack

Presented by David M. Weidmayer, CFP®

According to the 2017 Verizon Data Breach Investigations Report, 90 percent of all security incidents and breaches start with phishing attacks. Hackers use these attacks to trick people into divulging personal information. Unfortunately, many often don't realize they have fallen for a phishing scam until after the fact.

In all phishing attempts, some type of personal information is requested—a social security number, user ID, or password—through an e-mail that requires a direct reply or provides a link to a "phishy" (i.e., bogus) website. Keep in mind that **no legitimate organization requests personal data or confidential information via e-mail**. If you receive an e-mail that requests this type of information, consider it a major red flag.

Protecting yourself from phishing attacks

To help protect your devices from these insidious intrusions, follow these recommendations:

1. **Don't click on links or attachments** that come with suspicious e-mails. If you recognize an e-mail as a phishing attempt, delete it immediately. Clicking on a link or opening an attachment could install malicious software (malware) that could access the accounts and passwords stored on your computer.
2. If an e-mail purports to come from a company with which you do business, **go directly to the company's website** to verify the e-mail's authenticity. Open a new browser window to check for messages or review your account activity.
3. **Be wary of links from people you don't know** or messages that don't read the way a friend normally writes.
4. **Don't try to *win* anything**—contests and advertising that suggest something is free are typically bogus. "Win a free iPad!" or "Get a $500 Target gift card!" messages represent an easy way to trick you into clicking on a link and redirecting you to a toxic website. These sites can then embed viruses and keyloggers on your computer that will record your passwords and IDs when you sign in to any account.
5. **Don't panic** when pop-ups appear telling you that "Your computer has been compromised. Click here to fix it!" When you click on these fraudulent pop-ups, you are typically brought to a site asking you to purchase applications that will actually *harm* your computer—*not fix* it. Be sure to enable pop-up blockers on your web browser, and read any pop-up carefully *before* clicking.
6. **Get real security** by using software on your computer that scans for viruses, spyware, adware, and more. If you accidentally access a dangerous attachment or click on a link, contact an information security specialist as soon as possible to run scans on your computer.

As a reminder, *never* respond to text messages or automated voice messages requesting personal information or access to your computer. They are likely scams. Always verify who sent or left an e-mail or voicemail and don't react spontaneously. If you feel you have to, confirm a message's legitimacy by returning the call to a phone number that is known to you!

Rest assured I am always concerned about information security. I will strive to keep you up to date on new security threats, as well as potential solutions to help protect your information. If you have any questions, please contact me.

David M. Weidmayer is a financial advisor located at 9850 Westpoint Drive, Suite 550 Indianapolis, IN 46256. He offers securities and advisory services as an Investment Adviser Representative of Commonwealth Financial Network®, Member FINRA/SIPC, a Registered Investment Adviser. He can be reached at (317) 579-9400 or at dave@wwealthsolutions.com.