ON COURSE

Gone Phishing: Cyber Criminals View Crisis as Opportunity

MICHELE NOWELL

JANUARY — FEBRUARY 2021

Gone Phishing: Cyber Criminals View Crisis as Opportunity

MICHELE NOWELL

Executive Vice President

RICHARD P. SLAUGHTER ASSOCIATES, INC.

> The past year has been challenging for all of us. Stress levels and confusion are high and confidence in information is extremely low. Despite these conditions, the use of electronic communication and internet browsing is as popular as ever for consuming information because of its convenience. However, it also makes us more vulnerable to cybercrime.

One important aspect to always remember is that cyber-criminals are reliant upon user carelessness, indifference, or ignorance with technology user habits. So, confidence in your communication points is critical. Still, there have been significant increases in attempts to defraud through the theft of personal information such as social security numbers, birth dates, account credentials, and login information.

According to Webroot, a cybersecurity technology and software leader, 1.5 million new phishing sites are created each month. The FBI estimates more than $12 Billion is lost in phishing attempts every year. Furthermore, of the millions of phishing attempts sent every year, 30% of the distributed messages are opened by the targeted user.

As a financial advisor and fiduciary, Slaughter Associates is always on the lookout for ways to protect our client's wealth through sound financial advice and, in this case, an understanding of the methods that cybercriminals will use to gain access to information and wealth. Currently,

phishing attacks are one of the top cybercrime schemes.

For clarity, Phishing.org defines 'phishing' as cybercrimes "in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss."

The reality is, the average person gets phishing attempts every day, sometimes multiple times per day. The use of antivirus software and spam filtering along with keeping operating systems up to date will help reduce exposure to phishing attempts. In addition to utilizing tools to protect yourself, it is important to be aware of the various types of phishing techniques. Phishing.org lists these as:

- **Too Good To Be True:** Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many will claim that you have won an iPhone, a lottery, or some other lavish prize. Remember that if it seems too good to be true, it probably is!
- **Sense of Urgency:** A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Sometimes, they will tell you that your account is in jeopardy of being suspended unless you update your personal details or financial information immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.
- **Embedded Hyperlinks:** A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different, or it could be a popular website with a misspelling, for instance, www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully before clicking.
- **Attachments:** If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.
- **Unusual Sender:** Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character, or just suspicious in general, don't click on it!

"The reality is, the average person gets phishing attempts every day, sometimes multiple times per day."

While your service team

ABOUT RICHARD P. SLAUGHTER ASSOCIATES, INC.

Richard P. Slaughter Associates is a leading wealth-management firm specializing in delivering tailored strategies as a fiduciary for high net worth individuals, families, and businesses. Slaughter Associates constructs a comprehensive financial relationship with its clients by delivering expertise in financial planning and asset management while coordinating with tax, insurance and estate professionals. The result is a holistic approach—unique in the financial industry—that generates a clear path to the individual financial goals of the client. Founded in 1991 in Austin, Texas, Slaughter Associates was among the first fee-only firms in the nation, a fiduciary status that allows it the freedom to provide advice that is always in the best interests of the client. Slaughter Associates is a NABCAP Premier Advisor, recognized for its commitment to maintaining top business standards, first-class financial-management capabilities and dedication to preserving transparency in the financial services industry.

EXPERTISE

Areas of Expertise
Specialization in comprehensive wealth-management services for families with over $1 million in net worth

Other Interesting Fact
One of the first fee-only advisor firms in the United States

at Richard P. Slaughter Associates are not cybercrime experts, we do believe it is our duty to keep you informed of potential threats and assist in keeping you safe in the event of a breach in your security.

Should you fall victim to an actual phishing scam, there are some steps you can take to help prevent loss. As soon as you detect that your information is compromised, contact the financial institutions and service providers that may have access to your finances. Run malware software on the infected computer, like Malwarebytes or Symantec, to help identify and eliminate the infection. And, as soon as possible, change your passwords.

You can also notify the spoofed organization of the fraud (like your bank or retailer), and file a report with the Federal Trade Commission (FTC). Finally, place a fraud alert on your credit report to make it harder for criminals to acquire new debt in your name.

Keeping your advisor team at Slaughter Associates informed is very important. If you suspect you are a victim of fraud, we can assist you in notifying your custodian and watch your accounts under our management for any unusual attempted activity. We have worked with many clients over the past several years and in each case, the sooner we know the more helpful we can be.

Richard P. Slaughter™ Associates

Michele Nowell, AIF®
Executive Vice President

Richard P. Slaughter Associates, Inc.
13809 Research Boulevard, Suite 905
Austin, TX 78750
Tel. 512-918-0000

invest@slaughterinvest.com
slaughterinvest.com