TEAM KENTUCKY
PUBLIC PROTECTION CABINET
Department of Financial Institutions

Are You an Informed Investor? Spoofing/Phishing Scams

August 2024

Technology allows businesses to expand their operations, increase efficiency and save money. One increasingly common area into which financial service providers inject technology is customer service. While this may be a solution for some companies, reliance on technology-based customer service comes with risks, both for investors and for financial services companies themselves. Two ways these risks can materialize is through spoofing and phishing attacks by scammers.

WHAT ARE SPOOFING AND PHISHING?

Spoofing and phishing are tactics cybercriminals use to gain a person's trust so they can be manipulated into divulging personal or sensitive information which the cybercriminal will use fraudulently. This manipulation is also referred to as "social engineering." While scammers often use spoofing and phishing together, they are two different concepts.

Spoofing is when a cybercriminal deliberately duplicates and alters an otherwise real phone number, email address, screen name, or website to make it appear to be that of a trusted or well-known source. Simply adding or deleting a single character can transform a legitimate website into a fake one. Spoofing often enables phishing to occur.

Phishing is when a cybercriminal uses fraudulent emails, text messages, or phone calls to impersonate legitimate people and entities to trick consumers into giving out their personal information. The scammer can then use the personal information fraudulently or sell it on the online black market. A related type of cyberattack is Smishing, which targets individuals through SMS (Short Message Service) or text messages. (The term is a combination of "SMS" and "phishing.")

Cyber-criminals can use spoofing and phishing attacks to target investors or financial service providers. Depending upon the target and the success of the attack, a wide array of confidential information can be put at risk.

HOW CAN SPOOFING AND PHISHING AFFECT INVESTORS?

If you work with an investment professional employed by an investment adviser or broker-dealer, there is a good chance the representative or the firm uses technology to communicate with customers and clients. This digital connection is intended to be convenient for both parties, as it can eliminate the need for frequent face-to-face communication and can free up staff to do the work that truly provides value to the firm's clients. However, you may not suspect anything if someone posing as the firm reached out to you for a seemingly routine or reasonable request. This kind of innocent assumption could put you

Continued

at risk of unknowingly disclosing personal or financial information to a scammer.

Financial service providers can also be targets of spoofing and phishing attacks. Cyber criminals will direct phishing attacks at these firms hoping to trick an employee into downloading malware or sharing sensitive information. Fraudsters can then use this information to target clients of these firms with fake messages or offers that entice them to hand over sensitive information, like their account information or passwords. Many clients don't bat an eye when they receive communications from their firm because most business is done online these days.

RED FLAGS OF PHISHING AND SPOOFING

- A firm asking for personal or financial information over the phone. If you work with an investment adviser or a broker, they should have all your information on file. A legitimate financial professional or firm will not request private information via email, text, or online chat out of the blue. If you get such a request, reach out to the firm using the contact information that you have for it, and ensure that the communication is legitimate.

- Spelling or grammatical errors, or unfamiliar language in digital communications. Communications from an established entity will rarely contain these types of flaws. Errors in spelling or language could be a sign of automated translation tools or phishing attacks originating from other countries. Read your texts and emails carefully.

- Inconsistencies in links, addresses, and domains. In order to mimic the online appearance of a reputable firm, scammers will create websites and email addresses that look almost identical to the real thing. Be sure to hover over suspicious links before clicking on them, and closely review the spelling of domain names and email addresses.

- Reloading scams. These scams target investors who previously lost money to a scam or to a business failure that resulted in bankruptcy. The scammer will use information about investors in an existing scam or a bankrupt entity to reach out to them and try to convince them to hand over more money in order to get their original investment back. Only communicate with trusted sources who you reach out to using known contact information. Investors shouldn't have to pay money to get their share from a bankruptcy estate, so be wary and think twice (or three or four times) if you receive such a request.

THE BOTTOM LINE

It can be difficult to spot phishing and spoofing scams. To protect yourself, be wary of potential attacks and never give away your own private information unless you are sure you know who you are dealing with. In addition, take reasonable measures to safeguard your own data from cyberattacks by using commonly available tools like virus scanners and computer firewalls.

To learn more, contact the Kentucky Department of Financial Institutions

500 Mero St., 2SW19, Frankfort, KY 40601 | (800) 223-2579 | KFI.ky.gov

TEAM KENTUCKY
PUBLIC PROTECTION CABINET
Department of Financial Institutions