knowledgeable thoughtful ethical experienced interactive

summaries

SIGMA INVESTMENT COUNSELORS

the official newsletter of sigma investment counselors July 2014

Protecting Your Assets from Cyber Fraud

Cyber Fraud has become a prevalent issue in our daily lives. News feeds are flooded with stories of shockingly sophisticated identity theft rings and data breaches from our favorite retailers. Efforts by criminals to impersonate and defraud individuals have become more sophisticated and widespread in recent years. Technology continues to evolve, changing the way we conduct business and lead our lives, and cyber criminals continue to evolve as well. Cyber criminals now have a wealth of tools they can deploy to separate people from their assets. Both financial advisors and investment custodians have seen a noticeable increase in attempts to steal money through fraudulent wire transfers. An estimated 5% of U.S. adults fall victim to wire fraud, identity theft and email scams every year. (White, Mary Jo. "Opening Statement at the SEC Open Meeting." *U.S. Securities and Exchange Commission* April (2013): *SEC Open Meeting*. Web. 1 July 2014.)

We felt that it was important to alert our clients and contacts to recent industry conversations on this topic. Keeping our clients information secure from criminals is a top priority at Sigma. We continuously review security procedures, to ensure that we are following the best practices recommended by custodians, financial institutions, and industry experts.

While we are taking clear and actionable steps in our own firm's security measures, cyber fraud continues to escalate, is becoming more sophisticated, and is ever-changing. As a fiduciary, we are encouraging our clients to be aware of the various types of threats, and to embrace a series of measures to help protect your identity and prevent potential security risks.

Common Ways That Identity And Login Credentials Are Stolen

Malware - Using malicious software, criminals gain access to private computer systems (e.g. your home computer), and gather sensitive personal information such as Social Security numbers, account numbers, passwords, and more. Malware can be inserted into a victim's computer by various means, but most commonly occurs when a user clicks an unfamiliar website link or opens an infected email.

Phishing - Phishing is one of the most common cyber fraud tactics observed in the financial services industry. Criminals attempt to acquire sensitive personal information by impersonating an entity with which the victim already has a relationship (e.g., a bank, credit card company, or other financial services firm). The criminals then proceed to electronically solicit sensitive personal information from the unwitting recipient.

Social Engineering - Using social media and other electronic media, criminals gain the trust of victims

summaries

over time, and manipulate them into divulging confidential information. Usually, the scammer will leverage something that they already know about the victim, such as their name, birthdate, or the names of their spouse and children, to gain their confidence and get them to provide additional personal information that they can in turn use to commit fraud.

Spoofing – This technique is used when a criminal attempts to impersonate individuals that have relationships with professional financial advisors. The criminal obtains access to a client's email password through key logging software, or by creating a new email account that closely resembles the client's real email address. In either case, this person makes contact with the advisor to request a transfer of funds to a third party account.

Ways to Protect Yourself from Cyber Crime

There are several proactive things that you can do to reduce the likelihood that you will become a victim of these types of crime.

Manage Your Devices – Install the most current anti-virus and anti-spyware programs on all of your devices (PC's, laptops, tablets and smartphones). These programs are most effective when they are setup to run regularly scheduled scans vs. running periodic scans, which may not provide maximum protection for your device.

Protect All Passwords – Use a personalized custom password for financial accounts that you access online. It is also a good practice to regularly change your passwords, including those for your email accounts. You should also avoid storing passwords in email folders. A good alternative is to use a password manager program.

Surf The Web Safely – Do not connect to the internet via unsecured or unknown wireless networks, such as those in public locations like hotels and coffee shops. Those networks may lack virus protection, and are highly susceptible to attacks. Networks such as these should never be used to access confidential personal or financial information.

Protect Information On Social Networks – Limit the amount of personal information you post on social networking sites. Sharing too much information can make you susceptible to fraudsters, and allow them to pass a variety of tests related to the authentication of your personal information.

Protect Your Email Accounts – Delete any emails that include detailed financial information and continuously assess whether you even need to store any personal or financial information in email folders. If necessary, consider using a secure data storage program to archive important data and documents. Sigma clients have access to a secure client vault that can be used to store important documents. You should also review unsolicited emails carefully, and avoid clicking

links in unsolicited emails or pop-up ads, especially those that warn that your computer is infected with a virus and request you to take immediate action. Finally, you should consider maintaining separate email accounts for personal correspondence and financial or business correspondence.

Safeguard Your Financial Accounts – Review all of your credit card and financial statements as soon as they become available. If any transaction looks suspicious, immediately contact the financial institution where the account is held. Never send account information or personally identifiable information over email or other unsecure channels.

As your trusted financial advisor, we take numerous precautions to protect our clients' identities and assets. For example, we ensure that wire transfer requests, especially those to third parties, are legitimate before acting on them. There is nothing especially ominous about third party wire requests – clients may request transfers to third parties to buy houses or cars, pay insurance or medical expenses, or pay college tuition. However, as a fiduciary, it is our responsibility to verify that the request is legitimate. This is one of the many reasons why Sigma believes it is critical to know and have regular contact with our clients; providing us the capability and opportunity to properly assess the validity of the request and the identity of the individual making the request.

As added protection, it is also our policy to use secure formats when we transfer documents or communicate sensitive information using email. This may include encryption, password protection, and whenever possible, we encourage clients to utilize our client portal, which allows us to share and transfer documents securely. Our client portal utilizes the necessary security controls to protect your sensitive data. Its security measures include password protected entry into the portal, redacted account numbers so that no specific identifying account numbers are listed on the portal, and a document vault that allows us to securely share important documents with our clients.

This article is not intended to incite fear. Our hope is that providing you with this information allows you to become savvy about protecting your sensitive data, and mitigating the risk of cyber fraud.

Tamika M. Hall
Director of Operations

27777 Franklin Road • Suite 1100 • Southfield, MI 48034 • tel (248) 223-0122 • fax (248) 223-0144 • www.sigmainvestments.com