North American Management

Your True North

SUMMER 2020
PLANNING NOTE

Cybersecurity Best Practices

During the global COVID-19 pandemic, technology has helped all of us stay connected. However, as the amount of monetary and fiscal stimulus courses through the economy, cyber thieves have tuned in and become more active. Incidences of cyberfraud continue to escalate. With the fraudsters' methods becoming more sophisticated, the importance of maintaining cybersecurity vigilance has never been greater (see Fidelity's investor protection checklist at the end of this document).

While North American Management (NAM) is confident in its cybersecurity measures, we want to make our clients aware of a growing number of threats targeting businesses and individuals. Criminals are relying upon a variety of tactics, including email scams, to steal a victim's personal information or login credentials in order to create "synthetic identities" that they use to commit financial fraud. For example, one of the fastest growing identity theft crimes is using children's stolen Social Security numbers to open bank and credit card accounts. The more common attacks and suggested responses include the following:

Malware

Malware is malicious software designed to damage, create disruption, or gain unauthorized access to a computer system. Cybercriminals will often use this software to gather sensitive personal information such as Social Security numbers, account numbers, and passwords.

How it works: Malware can be inserted into a victim's computer by viruses, ransomware or spyware. It can be activated when an unwary user clicks an unfamiliar link on a text message or opens an infected email attachment.

How to react: Keep your antivirus software up-to-date. Be wary of all attachments and never click on a link or call the phone numbers provided in an email. Instead, go directly to the organization's website to access your account or to locate the customer service number.

Phishing

Phishing is a pervasive scam used by cybercriminals to steal your account details or login information. It is often initiated with a deceptive email or text ("smishing") message from a financial services provider prompting you to take immediate action relating to your account. This fraudulent electronic communication is almost always designed to trick you into divulging information and/or unwittingly granting access to a protected site. Phishing is often accomplished with the help of a fake website that closely resembles a real site in terms of logos and graphics.

How it works: Masquerading as a company with which the victim may have a financial relationship (e.g., a bank, credit card, or brokerage company), the criminals use fear tactics to trick victims into opening email links or attachments. Then, victims are prompted to enter sensitive information into a fake website, or their devices may automatically install malware to capture login and account information.

How to react: Never click on a suspicious email link. Set up your email inbox to filter out spam and phishing email. Hover your mouse over a link to verify it is going where you expect before you click or, better yet, go directly to the website.

Blake E. Stuart, CFA
Chief Operating Officer
Chief Compliance Officer

(617) 695-2100
bstuart@namcorp.com

More than 15 billion consumer credentials are circulating on the dark web.

– Digital Shadows Photon Research, July 2020

Vishing

An amalgam for voice phishing, "vishing" is another term for fraudulent phone calls designed to steal the same type of sensitive information targeted by phishing scams.

How it works: While people have started to develop a healthy awareness of suspicious emails and other electronic communications, fraudulent phone calls remain a blind spot for many. This makes vishing — whether through a person-to-person or robocall — a particularly valuable technique for cyber criminals.

- Successful vishers often use "vague enough to be real" details about the victim in order to inspire trust. Others will call you under the guise of an emergency or with a promise that the victim has potentially won money, gifts, or trips.
- Some vishers use blocked, fake, or spoofed phone numbers to impersonate a legitimate person or organization. Cyber criminals also use robocalls to carry out vishing schemes on a far larger scale.
- A vising exploit or robocall might pretend to be tech support and request remote access to your computer, while others use it to compromise two-factor protocols.

How to react: Hang up and call back the organization at a verified phone number (such as the one on your bank statement or the back of your credit card). Report the call to your financial institution or government agencies such the Internet Crime Complaint Center, the Federal Trade Commission (FTC), and the Better Business Bureau (BBB).

Credential Replay

Many people use the same exact credentials, including password, on many sites. One of the most common passwords is "123456," which is never a good choice! Unfortunately, despite being very convenient, this practice of using one password leaves people vulnerable to credential-replay attacks.

How it works: A cybercriminal obtains the password for one compromised account and then tries to use it to log into the victim's other accounts. The more often a password is reused, the more vulnerable the password is to be compromised or stolen.

How to react: Use multiple versions for user IDs and passwords, especially on financial websites that contain sensitive personal information.

The U.S. Federal Communications Commission (FCC) has been working with telecom providers to create new ways to digitally validate Caller IDs through STIR/SHAKEN authentication standards.

Next Steps

As a fiduciary to your financial accounts, we encourage you to embrace a series of measures to help protect your identity and mitigate potential security risks. Fidelity's investor protection checklist, attached to the end of this Planning Note, outlines some best practices for investors across six key areas to help you manage all your digital devices, protect all user IDs and passwords, and safeguard your email accounts and financial accounts.

Please carefully review this checklist with all members of your household. We also ask that you do the following:

- If you change any addresses, notify us so that we can update our records.
- If you suspect that your email account has been compromised, call us immediately.

- If you suspect that your brokerage account has been compromised, call us immediately. If it's after business hours and your custodian is Fidelity, leave us a message and then call 1-800-FIDELITY and ask for the Customer Protection Team to inform them of suspicious account activity.
- Consider dedicating a computer or tablet for accessing financial accounts and executing financial transactions.

Keeping your personal information safe has been and continues to be a top priority at NAM. To better protect you and your accounts from cyber threats, we regularly review security procedures to help ensure that we are following best practices recommended by the custodians, financial institutions, and industry experts with whom we work.

Please contact your NAM Wealth Adviser with questions or concerns about how we protect your accounts or the steps you and your family can take to better protect yourselves and mitigate risk. As always, we appreciate your trust and the opportunity to help you achieve your financial goals.

In a survey of 1,068 Americans aged 18 and older, 22% said they have been the target of digital fraud related to COVID-19.

– "TransUnion Research Quantifies How Social Distancing is Changing Shopping Patterns," Press Release, May 24, 2020

CYBER FRAUD RESOURCES

Investor protection checklist

The educational checklist presented below is designed to help you take appropriate action to better protect you and your family and mitigate risk of cyber fraud. Carefully review the items in each of the categories below to determine which apply to your unique situation.

TOPICAL AREA	ACTIONS TO CONSIDER	CHECK WHEN COMPLETED
Manage your devices.	• Install the most up-to-date antivirus and antispyware programs on all devices and update these software programs as they become available. These programs are most effective when users set them to run regularly rather than just running periodic scans, which may not provide maximum protection to your device. • Access sensitive data only through a trusted device and secure Internet connection; avoid use of public Internet connections other than through a Virtual Private Network (VPN). • If you have children, set up a separate computer they can use for games and other online activities. • Keep operating systems and software up to date (PCs, laptops, tablets, smartphones). Many updates are made to resolve recently identified security risks. • Do not install pirated software. It often contains security exploits. • Frequently back up your data in case of ransomware attacks.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Protect all passwords.	• Avoid storing passwords in email folders or un-encrypted files on your computer. Consider using a password manager program instead. These programs help generate and manage complicated passwords. • Use a personalized custom identifier for financial accounts you access online. Never use your Social Security number in any part of your login activity. • Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships, and avoid using a single password across multiple sites. • Utilize multi-factor authentication, especially for financial and email accounts.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Surf the web safely.	Exercise caution when connecting to the internet via unsecured or unknown wireless networks, such as those in public locations like hotels or coffee shops. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data directly, without the proper protection of a secure VPN connection.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Protect information on social media.	Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birthdate, home address, and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays, or the loss of loved ones. Sharing too much information can make you susceptible to fraudsters and allow them to quickly pass a variety of tests related to the authentication of your personal information. Never underestimate the public sources that criminals will use to learn critical facts about people.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.

TOPICAL AREA	ACTIONS TO CONSIDER	CHECK WHEN COMPLETED
Protect your email accounts.	• Delete any emails that include detailed financial information beyond the time it's needed. In addition, continuously assess whether you even need to store any personal and financial information in an email account. • Use secure data storage programs to archive critical data and documents. • Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those warning that your computer is infected with a virus requesting that you take immediate action. • Establish separate email accounts for personal correspondence and financial transactions. • Choose a unique password and utilize multi-factor authentication. • Review all emails carefully before clicking on links or attachments.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Safeguard your financial accounts.	• Consider contacting the three major credit bureaus to add a "security freeze" and prevent new accounts being opened in your name: – **Equifax:** 800-685-1111 – **Experian:** 888-397-3742 – **Transunion:** 888-909-8872 • Lock down personal credit reports with Experian®, TransUnion®, and Equifax®. Proactively enroll in an identity theft protection service to protect personal data. • Review all your credit card and financial statements as soon as they arrive or become available online. 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, chat, or any other unsecured channel. • Suspiciously review any unsolicited email requesting personal information. Further, never respond to an information request by clicking a link in an email. Instead, type the website's URL into the browser yourself. • Avoid developing any online patterns of money movement, such as wires, that cyber criminals could replicate to make money movement patterns appear more legitimate.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.

917236.1.0