In this issue:

- **A Primer on Password Managers**
- **Cybersecurity shorts**
- **Software updates**

**The following content is provided courtesy of Horsesmouth, LLC, and provided courtesy of Miles Harris.*

This month we'll be talking about password managers. Read on for more information on that, as well as:

- The latest company hit with a ransomware attack
- Urgent updates for Microsoft users
- New government guidelines related to cybersecurity
- And much more

A Primer on Password Managers

Earlier this month, I gave a cybersecurity presentation to a group of advisors. During the presentation, I gave eight or so actions advisors could take themselves and share with clients to help protect them from cyber threats. I wasn't surprised to receive several after the presentation—but I was surprised when I saw that most of them had to do with one topic. Password managers.

When Sean Bailey and I began developing the Savvy Cybersecurity program in 2013, we too had questions about password managers. Were they safe? Did we feel comfortable recommending them to advisors and their clients? After some research of our own—including downloading and using password managers—we decided that they were safe and one of the best password practices you could take.

A password manager is a digital device that stores all of your username and passwords in an encrypted file on your computer and/or in the cloud. Your passwords are protected by one master password—the only one you need to remember.

Once you are signed in to your manager with your master password, the program will autofill the username and password fields for any known website. If you visit a new site that is not yet stored, you can easily save your login credentials to your password vault.

Using a password manager eliminates the challenge of having to remember unique passwords for all of your accounts. You only need to remember your master password to access everything else. Since we got so many questions on the topic, I thought I would answer some of them in this month's newsletter.

How safe are password keepers? What password manager do you recommend?

Password managers are generally very safe. Password managers use strong encryption to secure your password files. Your passwords are so secure that if you forget your master password, not even the company can retrieve your passwords.

Password managers typically cost $10–$30 annually and most allow you to access your manager from your various devices such as your smartphone and tablet. Free versions exist but typically those only work on one device and have limited features. There are many password managers to choose from and it's best to do some research to see which program best fits your needs. Some options you may consider are Dashlane, LastPass, 1Password, and KeePass.

Are password managers included on the iPhone acceptable?

The iCloud Keychain available on the iPhone and other Apple products is a safe and secure password manager. Apple uses strong encryption to protect this software feature and you can increase protection by enabling two-factor authentication on your device. One limitation of the iCloud Keychain is that it will not sync with non-Apple devices. If you have an iPhone but a Windows PC, you won't be able to access your passwords on the PC. Other password managers allow syncing between different devices.

How do hackers figure out passwords?

Most often hackers purchase lists of usernames and passwords that have been breached at companies. Hackers know that most people reuse their passwords, so they will try your username and password on other sites. There are, of course, other ways hackers get your passwords, but this is the most common.

Cybersecurity shorts

NASA is aiming to correct cybersecurity management issues that were identified in a recent inspector general report. Although attacks on NASA's networks aren't new, NASA has found that the ability to prevent, detect, and mitigate cyberattacks is limited by a disorganized approach to Enterprise Architecture. You can learn more here.

Following the Colonial Pipeline ransomware attack, the government takes action. The Department of Homeland Security has decided that it needs to regulate cybersecurity within the pipeline industry. This will be the first time the government intervenes in a cybersecurity incident and it is expected to require key infrastructure companies to report all cyber incidents to the federal government.

Billions more going towards federal cybersecurity. The White House has allocated $9.8B to its cybersecurity budget request for 2022. This is an $8.7 billion increase from the 2021 fiscal year budget. Additionally, the money allocated to go specifically toward civilian cybersecurity programs across the government.

Cybersecurity education deemed vital for companies continuing remote work. Remote work has become a normal practice for many businesses. However, with remote work, there is also a new set of cybersecurity challenges. If continuing to work from home is part of the picture for your company, cybersecurity education is vital to ensure that your remote working policies are followed. Here are four cybersecurity mistakes your remote workers are probably making.

Meat processing plant the latest hit with ransomware attack. JBS, one of America's biggest meat processors, said that it paid cybercriminals an $11 million ransom after falling victim to a ransomware attack. This ransom payment is more than double the $4.4 million that Colonial Pipeline paid to recover its data in a similar attack. You can learn more about the cyber attack here.

President Biden issued executive order that overturns the ban of TikTok and WeChat. The order also offers new guidelines for federal agencies to assess the national security risks. The new order emphasizes additional criteria for the Commerce Department to use in assessing whether to restrict U.S. use of foreign software apps.

Electronic Arts had 780GB of new games stolen. The hack was first reported by Motherboard, which discovered the hackers selling the code for $28 million on the R0 Crew forum on the Dark Web. The hackers also included proof of their exploits using anonfiles.com as well as a 2015 email between EA and games security provider Denuvo.

Bank of America to spend over $1 billion a year on cybersecurity. CEO Brian Moynihan, announced that the company has ramped its cybersecurity spending to over $1 billion a year. This is in response to a series of sweeping cyberattacks that have struck private companies and federal government networks over the past year.

Justice Department able to recover $2.3 million of Colonial Pipeline Co's initial ransom. Colonial Pipeline Co. paid roughly $4.4 million in cryptocurrency to hackers that were holding its computer system hostage. With the FBI following the cryptocurrency, the Justice Department said it has recovered some of the cryptocurrency that equals roughly $2.3 million of Colonial's initial ransom.

Software updates

Adobe: Adobe released software updates for Acrobat, Reader, Photoshop, and Creative Cloud this month. You can learn more about the updates for these programs here.

Microsoft: Nearly 50 security vulnerabilities are addressed in this month's Microsoft update—six of these issues are considered critical and should be patched immediately. Your device should prompt you to update automatically but you can learn more about the updates here.

B. Miles Harris is a registered representative of and offers securities, investment advisory and financial planning services through MML Investors Services, LLC. Member SIPC. Harris Financial Group is not a subsidiary or affiliate of MML Investors Services, LLC, or its affiliated companies. 13455 Noel Road, 20th Floor, Dallas, TX 75240 (972) 246-1800. CRN202407-568273