In this issue:

- **Phone scams aren't dead: How to protect yourself**
- **Cybersecurity shorts**
- **Software updates**

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

Welcome to your March Savvy Cybersecurity newsletter. Read on to learn more about the cybersecurity happenings this month including:

- Hacks affecting Covid-19 vaccine manufacturers
- A Facebook Messenger scam making the rounds
- Details on a new privacy feature from Apple
- And much more

Phone scams aren't dead: How to protect yourself

While many think of cybersecurity and picture computers and complicated code, the truth is many scams still rely on human connection and fear. Countless scams begin with a phone call that tells the victim someone has made a fraudulent purchase with their account or that they need to verify personal information. The scammer poses as a helper to gain the trust of the victim and then defraud them. For example, here is a story I heard this week…

Elaine's phone rang one afternoon. She didn't recognize the number but she picked up. The voice on the other end said they were from Amazon and they wanted to confirm if she just purchased a $700 laptop. Elaine had not purchased a laptop and told the caller so.

The caller reassured her that it was no problem—he could help her resolve this issue. He asked her to go to her computer and type in a web address. The URL led her to a remote desktop download. Being savvy about her cybersecurity, Elaine stopped and told the caller she was not comfortable downloading any software onto her computer considering she did not know who he was. The caller tried to reassure her by directing her to search his name on Amazon. It listed him as a tech specialist but there was no way to confirm that he was truly the person he said he was.

Elaine did the right thing and told the caller she was not going to download the software and she would resolve the charge with her credit card company instead. She hung up the phone and successfully avoided a scam that could have done serious damage to her computer and bank account.

This story is a great reminder that many of the scams we see begin with a phone call and a conversation. If the caller had convinced her to download the remote desktop software, what could have happened? For one, the caller would have been able to see everything on Elaine's computer and access passwords and documents. He could have also easily installed malware that could have collected more information or done damage to the computer.

Here are some ways you can protect yourself from phone scams like this.

1. Be aware and alert

The first key to avoiding a scam like this is being aware that they exist and still occur frequently. Awareness allows you to think critically if you receive a call that may be fraudulent. If you receive a call from an unknown number, consider just sending it to voicemail. If you do decide to answer, be on alert for any warning signs of a scam. Some warning signs include asking you to divulge personal information or requiring you to download anything on your computer.

2. Verify the phone number and caller

If you are ever unsure about a phone call you receive, tell the caller that you are going to hang up and call the company number directly. When you do this, do not call back the number that called you. Instead, look up the phone number for the company online and call that number. When someone answers, you can verify that the person who called you is an employee or see if what they were saying is true.

Many scammers will "spoof" the phone number they call you from to look like a legitimate company. You cannot simply trust your caller ID because of this. Always hang up and call the correct number back directly.

3. Take your time

If someone calls you to confirm a fraudulent purchase or asks for personal information, pause before responding. These scammers rely on urgency and fear to get you to act quickly. Take a moment to think about what they are saying and remember your Savvy Cybersecurity principles. It is easy to react quickly when your money is on the line—take a moment to breathe and think.

Phone scams are still a common occurrence. Scammers rely on making that human connection and appealing to your emotions over the phone. It is always important to be cautious when receiving calls from numbers you don't know or recognize. Think twice before sharing any personal information or downloading anything on your computer.

Cybersecurity shorts

Hackers steal COVID-19 vaccine data from BioNTech. Throughout the COVID-19 pandemic, many research labs and pharma's have been victims of cyber-attacks. Additionally, last month Microsoft said that a Russian group and two North Korean groups attempted to break into systems at seven pharmaceutical companies and researchers in five different countries. To learn more about the data breaches on COVID-19 vaccines and their information, you can read more here.

U.S Capitol building stormed by pro-Trump rioters potentially causes cybersecurity risks. On January 6th, 2021, numerous pro-Trump rioters occupied portions of the U.S. Capitol building to protest and disrupt the counting and certification of electoral votes from the November 2020 election. This breach into the U.S. Capitol poses potentially serious cyber risks for all the affected offices, including Congress. Here you can read more about the questions raised about the cyber safety that remains in question and what the House and Senate staff should do immediately to avoid any cyberattacks.

Seven actions you can take to help you prevent any cyberattacks. In light of the massive SolarWinds compromise, many have been asking what they can do to keep their information safe and avoid any attacks. This article has laid out seven different actions you can take to help you prevent any cyber-attacks including getting a password manager, updating your router, two-factor authentication, and more.

President Biden announces Anne Neuberger as a member of his National Security Agency. Neuberger's hiring indicates that the Biden White House intends to reelevate cybersecurity as a key national security priority after President Trump eliminated the role of cybersecurity coordinator in 2018. Read more into President Biden's plans for cybersecurity and what Neuberger's hiring means for the future of National Security here.

Ubiquiti urges customers to change passwords and enable multi-factor authentication. The company, a major vendor for cloud-enabled Internet of Things (IoT) devices such as routers, network video recorders, security cameras, and access control systems, urges customers to change their passwords and enable multi-factor authentication. This is due to a third-party cloud provider potentially exposing customer account information and credentials. You can read more about the potential risk and Ubiquiti's letter to their customers here.

SolarWinds announces malicious code that attackers used. The company says attackers used malware to manipulate its software and it remained undetected for months. The discovery adds to the public understanding of one of the most complex digital espionage operations in recent memory. The attackers used not only SolarWinds' software but other digital entry points in carrying out the hack which has affected major firms including Microsoft and FireEye, as well as multiple federal agencies. Cyberscoop has put out a detailed article explaining the attack.

What will election security look like in future elections? The Hill reports that efforts to boost election security are likely to gain traction in the new Congress, as Democrats who have pushed for election reform take control of both chambers and the White House. Read this article to learn more about what election security may look like in future elections.

Bureau of Cyberspace Security and Emerging Technologies announced. Former Secretary of State Mike Pompeo approved the creation of a new office at the State Department to address cybersecurity and emerging technologies. This new Bureau of Cyberspace Security and Emerging Technologies (CSET) will help lead diplomatic efforts around these topics, including working to prevent cyber conflicts with potentially adversarial nations. To learn more about this, read The Hill's article.

Apple launches new privacy label requirements. In June at Apple's Worldwide Developers Conference, the company announced it would soon require developers to disclose their app's privacy practices to customers via new, glanceable summaries that appear on their apps' product pages on the App Store. These new labels aim to give Apple customers an easier way to understand what sort of information an app collects across different categories. Read more about the launch of these new privacy labels here.

Facebook Messenger scam is on the rise. There have been Facebook Messenger scam that used bogus video to lure you onto a fake Facebook login page. In this scam, the scammers were using stolen Messenger passwords to phish for more Messenger passwords by sending messages that genuinely seemed to come from friends and family. Naked Security has written an article about the Facebook scam and what to do if you become victim to it.

T-Mobile announced second data breach at the end of 2020. The company said that it had recently discovered unauthorized access to some customers' account information, including the data that T-Mobile makes and collects on its customers in order to provide cell service. You can read the statement and more in-depth about it here.

Software updates

Adobe: Adobe released updates this month for multiple programs including Photoshop, Illustrator, and others. This is the first official month that Adobe Flash is retired. If you have not removed Flash from your devices, you must do so now.

Microsoft: Updates closing over 80 security vulnerabilities were released by Microsoft this month. The security issues impact Windows operating system, Windows Defender, and other Microsoft programs. Your device should prompt you to update but you can learn more 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. CRN202301-277685