In this issue:

- **Avoid Ransomware Catastrophe with the Rule of Three**
- **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 ransomware. Read on for more information on that, as well as:

- The latest company suffering a data breach
- Urgent updates for Microsoft users
- Cybersecurity steps to take when returning to the office
- And much more

Avoid Ransomware Catastrophe with the Rule of Three

When I sat down to write this month's newsletter, I did a quick Google search on ransomware. These headlines were all from the 18 hours before I wrote this piece.

- *Ransomware hits law firm with dozens of major corporate clients - CNN*
- *Cloudstar—IT provider for real estate, finance, insurance worlds—downed by ransomware – The Register*
- *Morgan County, W. Va. school system working its way out of a ransomware attack – WDVM*

Over the past few months, we've seen ransomware attacks take down food and gas supply chains. Some companies were forced to pay ransom to the hackers, while others managed to avoid it.

It's become clear to many that ransomware is still a growing threat for individuals, businesses, schools, hospitals—truly any group. The likelihood that you will encounter a ransomware attack—at home or work—is high. But you can avoid some of the pain and cost of ransomware attacks by setting up systems now to protect your files and data.

How does ransomware spread?

The first step in protecting yourself from ransomware is understanding how ransomware spreads. Ransomware is a type of malware that encrypts all of your data and demands a payment to get your files back. Typically, ransomware spreads through phishing emails—messages that appear to come from a friend or company you do business with—but are really from hackers.

Whenever you receive an email asking you to click a link or download an attachment, you must employ the E.M.A.I.L. rule—Examine Message and Inspect Links. When you receive an email, take a closer look at the true sender by hovering your mouse over the email address. Hackers can spoof an email address to look like they are contacting you from a legitimate organization. Looking more closely at the sender’s address can reveal the true sender. Be sure to do the same with any links in the email. Before clicking, hover your mouse over any link to see the true website.

Don’t open any attachments or click any links if you are unsure. If the email comes from a company you do business with, contact them directly on the phone to confirm the communication before clicking anything in the email.

The Rule of Three

The above rule will help you avoid falling victim to ransomware but what happens if you accidentally click on a malicious link? Not all is lost if you've followed the Rule of Three.

The Rule of Three states that you should have all of your data backed up in three places—your device, the cloud, and an external back-up storage system. Popular cloud options for storage include iCloud, Dropbox, and Microsoft OneDrive. For external options, consider an external hard drive. You should get in the habit of backing up your data to the cloud daily (or at least a couple of times a week). For the external hard drive, you can transfer files over every week or twice a month.

Backing up your files means that even if your device is hit with a ransomware attack, you won’t have to pay the ransom to get your information returned. Instead, you can have the ransomware removed from your machine by a professional and re-download your files from the cloud or an external device.

Ransomware is a threat we all face—large corporations, small businesses, and individuals. Knowing how to prevent an attack and having precautions in place in case you do fall victim is key to a quick recovery from a potential ransomware attack.

Cybersecurity shorts

Morgan Stanley faces data breach. The company disclosed that the personal data of some of its corporate clients was breached in January. Files that were stolen include client names, addresses, date of birth, social security numbers, and corporate company names. The company's bank said the attackers accessed information by exploiting a vulnerability in the vendor's server, Accellion FTA. You can learn more about the data breach here.

Hackers are pushing fake crypto-mining apps to make money off of victims interested in cryptocurrency. Lookout Security researchers have identified more than 170 apps that advertise themselves as providing cryptocurrency mining services on the cloud for a fee. Similar scams have existed in desktop form for a while, but this is the first time researchers have noticed apps designed to conduct this type of fraud.

Microsoft urges its users to update their PCs immediately after researchers have found a vulnerability in its operating system. The flaw, known as PrintNightmare, is affecting the Windows Print Spooler service. Researchers at the cybersecurity company, Sangfor, accidentally published a how-to guide for exploiting the flaw.

200+ companies were hit by a ransomware attack. The attack is believed to be affiliated with the prolific ransomware gang REvil and has been perpetuated through Kaseya, an international company that remotely controls programs for companies that manage internet services for businesses.

Hackers are using a networking platform as the ultimate phishing tool. At least 10,000 citizens have been approached by state-sponsored threat actors using fake profiles on what is suspected to be LinkedIn. The U.K.'s security agency, MI5, has yet to name the platform, but the BBC has claimed to have learned that the platform in question is, in fact, LinkedIn. You can learn more about the attack and how to keep your account safe here.

U.S.-based insurance company notifies customers of a data breach. CNA Financial Corporation is notifying their customers of a data breach following a Pheonix CryptoLocker ransomware attack that hit their systems back in March. The investigation has revealed that over 75,000 individuals have been affected and that the threat copied a limited amount of information before deploying the ransomware.

Cyberattacks have threatened critical infrastructure, the food supply chain, and people's personal data which has the U.S. government and many American businesses on defense mode. Hoping to prevent an attack, businesses have hired groups, known as red teams, to hack into their systems like would-be terrorists and expose any cybersecurity weaknesses they may have.

Returning to in-office work may be putting your company at risk. Many employees who have worked remotely due to the Covid-19 pandemic are now returning to the office on either a full-time or hybrid basis. Returning to the office could also mean bringing their bad cybersecurity habits back and this will put companies at a greater risk for cyber-related crisis situations. Here, you can learn more on how to protect your staff and company when returning back to the office.

House Approves DHS Bill on cybersecurity. A bill to fund the Department of Homeland Security (DHS), which included $2.42 billion for the Cybersecurity and Infrastructure Security Agency, is now heading to the full Appropriations Committee in the House after it was passed unopposed through its related subcommittee.

Software updates

Adobe: Updates for Acrobat, Reader, Illustrator, and other Adobe programs were released this month. Learn more about the updates here.

Apple: A new operating system update is available for iPhone, Apple Watch, and Apple TV users. iOS14.7 was released this month but the details on the software update are still unknown. Security experts hope that the update fixes a recently discovered vulnerability that could cause iPhones to not be able to connect to any Wi-Fi networks. We'll keep you updated as we learn more.

Microsoft: Microsoft released updates for over 100 security issues this month—four are actively being targeted by hackers. Included in this update, is an update to the patch for PrintNightmare that we warned you about earlier this month. That update caused some issues for Microsoft users. You can read 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. CRN202409-810671