In this issue:

- **Thousands of businesses hacked through Microsoft Email Exchange**
- **Cybersecurity shorts**
- **Software updates**

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

Welcome to your Savvy Cybersecurity newsletter. A major Microsoft hack took over cybersecurity news recently, we'll be covering what you need to know about that hack in this newsletter. Read on to learn more about that and:

- Why you should think twice about sharing your vaccination card on social media
- Security and privacy concerns with a popular new app, Clubhouse
- How to keep health data safe as telehealth appointments gain popularity
- And more

Thousands of businesses hacked through Microsoft Email Exchange

Over 30,000 U.S. organizations were hacked in recent weeks after a Chinese cyber espionage group exploited flaws in Microsoft Exchange Server email software. This massive attack on organizations including small businesses, hospitals, local governments, and credit unions is now being called a global cybersecurity crisis.

The hacking group, called Hafnium, is believed to have been conducting targeted attacks on the email systems of many organizations for months. Through the flaws in the Microsoft Exchange Server, hackers are able to gain remote control over affected systems with administrative access.

In addition to exposing sensitive business information, the hacked email servers could also lead to ransomware campaigns affecting hundreds of thousands of individuals. Once the hackers have remote control, they can send fraudulent emails out to contacts of the business.

Microsoft has released security updates patching the flaws in its email server software. Security experts say, however, that Hafnium has increased its activity by scanning the Internet for servers that have not yet been patched. If you are running Exchange and have not yet applied the patch, you are likely compromised. And unfortunately, even if you have patched your server there may still be malware on your network.

You can use this detection tool created by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to see if your server has been compromised. If your organization is a victim of this hack, be sure to patch your software immediately. You can learn more about the updates here.

Microsoft reports that nearly 90% of vulnerable servers have been patched but that still leaves thousands open to attack, and it is likely that we will see further hacks stemming from this one. As always, we will continue to update you with new information.

Savvy Cybersecurity lessons

The Microsoft hack highlights the importance of keeping software and systems up to date at all times. Patching software in a timely manner is critical to strong cybersecurity, both for individuals and organizations.

In addition, we must all be on the lookout for ransomware emails in the coming months. Security experts have already seen ransomware attacks launched from affected email servers. Look over every email closely before clicking on any links or sharing any personal information.

Cybersecurity shorts

Think twice before posting your vaccine card on social media. Although experts are not aware of any widespread hacks or scams specific to the vaccine cards, they are urging the public to stop posting their vaccination cards on social media. The card shows personal and sensitive information that can help scammers. For more information, take a look at this CNN article.

Cities are requesting cybersecurity education for everyone. Local governments need to embrace universal cybersecurity education to help reduce the risk of breaches and attacks. Los Angeles' civil servants in particular are subjected to "a lot" of internal phishing to test city employees' ability to detect malicious links, says Jeanne Holm, Los Angeles' deputy mayor for budgets and innovation. Learn more about why city officials think cybersecurity education for all is crucial.

Telehealth's success has created a cybersecurity nightmare. As the Covid-19 pandemic hit, healthcare systems from across the world brought down the regulating barriers to provide patient care via popular video chatting platforms such as FaceTime, WhatsApp, Zoom, and Facebook Messenger. All of the virtual visits are generating a mountain of healthcare data that has to be secured against aggressive cyberattacks. Quartz has more information on this.

Bad cybersecurity habits can cost you customers. Cybersecurity has now become an essential business practice. Failing to put cybersecurity measures into place could harm your business in ways you may not have considered. But how do you decide which cybersecurity measures your business should implement? CMS Wire points you in the right direction with four tips. .

FBI and CISA release advisory on cybersecurity compromise of Microsoft Exchange Server. The FBI and CISA released a Joint Cybersecurity Advisory (CSA) to address the recently disclosed vulnerabilities in Microsoft Exchange Server. The CSA is meant to highlight the cyber-threats associated with the active exploitation of vulnerabilities in Microsoft Exchange on-premises products. Learn more here.

How can we achieve better cybersecurity now that we've worked at home for a year? Finally reaching the one-year mark of working from home, federal IT teams continue to grapple with new and heightened security concerns.. Surveys of recent federal IT leaders indicate that agencies should conduct routine cybersecurity training for all employees and should also have employees participate in security simulations. Read more in this Washington Technology article.

Firms race to patch Microsoft Exchange flaws after hack. Suspected Chinese government-linked hackers were allegedly the first to exploit the Microsoft vulnerabilities. However, as soon as the company released a fix for the bugs, which took the issue public, a range of other hacking groups also appeared to try leveraging the flaws. At least ten different advanced threat groups are working to exploit the vulnerabilities now. Read Cyber Scoop's article on how the company is trying to get ahead of the.

Scammers exploit Covid-19 vaccine confusion for fraud efforts. The rush to deliver Covid-19 vaccinations has been confusing at best, making cyberspace a more fertile place for pandemic-related scams. Researchers have said that vaccine-related spear-phishing emails rose 26% from October to the end of January. This coincides with the time Pfizer and Moderna announced vaccine availability. To learn more, read Cyber Scoop's article.

Many question Clubhouse's security and privacy. Clubhouse, an invite-only social media app, seems to be dealing with a lot of data protection issues. More than 10 million people have downloaded Clubhouse. But researchers and frustrated users have articulated concerns about a number of security issues. Cyber Scoop goes into more details about the issues here.

Software updates

Microsoft: Microsoft released updates for over 80 security issues this month. Ten are considered critical updates. Unfortunately, some experts are seeing issues with these updates and many of the patches have actually been removed. For this reason, you may want to delay updating your system. Read more about the patches here.