In this issue

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

Welcome to February's Savvy Cybersecurity newsletter. Read on to learn about the cybersecurity news this month such as:

- A hack affecting U.S. government agencies
- Scams targeting the Covid-19 vaccine rollout
- What experts predict for cybersecurity in 2021
- And much more

Massive hack hits U.S. government agencies and Fortune 500 companies

U.S. government agencies—such as the Department of Homeland Security and the Treasury Department—suffered a major hack that may have begun in the spring of 2020. According to reports, experts allege that the Russian government is behind the attacks. Russia denies the allegations at this time. The hack is being called the "greatest intelligence failure of modern times."

While the U.S. national security agencies focused on protecting the 2020 election from hackers, they now believe that hackers targeted other agencies through a vulnerability in SolarWinds Orion software. Over 300,000 companies and agencies use the software to monitor computer networks. SolarWinds believes that 18,000 customers were using the vulnerable software.

Experts believe that hackers exploited SolarWinds' supply chain to spread malicious software. The company suffered a breach last year that exposed employee passwords. Hackers used the exposed password—solwarewinds123—to gain access to the network. Hackers were then able to add the malicious code to SolarWinds' software and when the company pushed out the update, customers unknowingly downloaded the malware as well.

As of now, the Energy Department and National Nuclear Security Administration, Commerce Department, Department of Homeland Security, Pentagon, Treasury Department, U.S. Postal Service, and National Institute of Health appear to be affected by the hack. Many Fortune 500 companies also use the software.

The security community is still determining how many customers were affected by this cyberattack. Federal investigators are now working with Microsoft to determine other agencies and companies that downloaded the malicious software. Microsoft was also a victim of the widespread hacking campaign.

At this time, it is unknown what information was stolen or whether any data was changed by the hackers. There is a concern in the security community that internal information may have been exposed or stolen. Experts also worry about future attacks stemming from this breach. For example, if email addressed were accessed, hackers can create sophisticated phishing campaigns to infiltrate other systems and agencies.

This hack is a reminder that all agencies and companies are vulnerable to cyberattacks. We must always be vigilant with our cybersecurity—protecting our passwords, avoiding phishing campaigns, and keep our systems up to date. We will continue to update you as we learn more about this major cyberattack.

Cybersecurity shorts

Businesses continue to face cyberattacks during work-from-home policies. At the height of the ovidCovid19 pandemic, the global workplace paradigm adjusted to a remote workplace within a matter of weeks. Yet many businesses found themselves unprepared to ensure their employees' cybersecurity from home. As a result, most businesses faced more cyberthreats within six months than they had endured throughout all of 2019. This article goes more in-depth on why our ";ood enough" work-from-home cybersecurity protection needs to be better.

More homes face cyberattacks during remote learning and work. The most vulnerable connected home devices include laptops, computers, smartphones and tablets, networked cameras, networked storage devices, and streaming video devices. You can learn more about the increase in cyber-attacks here.

The United States Congress has enacted the Internet of Things Cybersecurity Improvement Act of 2020, which establishes minimum security standards for Internet of Things (IoT) devices owned or controlled by the U.S. Federal Government. This Act helps the National Institute of Standards and Technology establish standards and guidelines for the Federal Government on federal agencies' use and management of IoT devices. This article explains the Act and what it means for cybersecurity at the federal level.

The Covid-19 pandemic has accelerated the rate at which the health care sector transforms. Because of Covid-19, there are more telemedicine appointments available for patients. Although there are major benefits of going digital, the health care industry has become increasingly vulnerable to cyberattacks that you can read about here.

President-elect Joe Biden's pick to lead the Department of Homeland Security will bring a boatload of cybersecurity experience to the job. Alejandro Mayorkas worked on several international cybersecurity agreements as deputy DHS secretary during the Obama administration. Learn more about Mayorkas, his expertise, and what President-elect has planned for cybersecurity here.

What will cybersecurity look like in 2021? Cybersecurity vendors will accelerate AI and machine learning app development to combine human and machine insights so they can out-innovate attackers' intent to escalate an AI-based arms race. This year, attackers and cybercriminals capitalized on the chaos by attempting to breach a record-breaking number of enterprise systems in e-commerce, financial services, healthcare, and many more industries. Click here to read what 20 leading cybersecurity experts are predicting for the year to come.

Scams likely as the Covid-19 vaccine is rolled out. Security experts warn that they expect to see phishing and phone scams during the vaccine rollout period. While they have not seen such scams yet, they urge the

public to be aware and keep an eye out for such scams. Do not share any personal information with an unknown caller contacting you about the vaccine.

How can healthcare providers improve cybersecurity in 2021? Panelists at the HIMSS Healthcare Security Forum said that cybercriminals will likely use tried-and-true techniques, such as phishing emails themed around Covid-19 vaccines or President-elect Joe Biden. Cybersecurity has become a patient safety issue. This article breakdowns what cybersecurity could look like in 2021.

Security experts are warning holiday gift-givers and receivers to be cautious of risks that internetconnected devices and home appliances could pose to home security. A survey has shown that electronic usage is expected to be at an all-time high this holiday season. Read this article to learn more about the cyber risks this holiday season as most families celebrate together virtually.

IRS will allow all taxpayers to use an IP PIN beginning in 2021. The U.S Internal Revenue Service will allow all taxpayers to apply for an identity protection personal identification number (IP PIN). This IP PIN will be a single-use code designed to block identity thieves from falsely claiming a tax refund in your name. You can learn more about the IP PIN, tax refund fraud, and more here.

Microsoft security experts detailed how internet attackers are abusing some of the world's most popular web browsers, which at its height has affected more than 30,000 devices per day. This article explains that the scammers are using malicious browser extensions, a classic fraud tactic, that injects bogus advertisements into the results displayed on a search engine page. The malicious campaign has affected browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Russian-language Yandex to reach as many users as possible.

Vaccine makers face cyberattacks during rollout period. The European Medicine Agency that is currently helping roll out two Covid-19 vaccines has been hit by hackers. Attackers successfully accessed documents relating to the regulatory submission for Pfizer and BioNTech's Covid-19 candidate. The EMA is currently working with law enforcement to investigate further. You can learn more about the attack here.

Software updates

Adobe: This is the last month that Adobe Flash Player will be supported by Adobe. Be sure to uninstall the program if it is on any of your devices. Google and Firefox currently block Flash and Windows will follow suit--removing the program from its browser. Adobe did release updates for Prelude, Experience Manager, and Lightroom this month. You can learn more about the update here.

Microsoft: Microsoft released nearly 60 security fixes this month in its batch of updates. Nine of the vulnerabilities are considered critical. These updates are for Microsoft Exchange Server, Windows 10, and Sharepoint Server. There are also updates for Microsoft Office. Your device should prompt you to update but you can read more about it here.