In this issue:

- **Hackers try to poison Florida water supply**
- **Cybersecurity shorts**
- **Software updates**

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

Welcome to the April Savvy Cybersecurity newsletter. Cybersecurity was prominent in the news this month with a story of a water facility hack in Florida. We'll take a closer look at that story in this month's newsletter, as well as other cybersecurity happenings:

- Updates in the SolarWinds hack
- An uptick in romance scams
- The latest on TikTok's status
- And much more

Hackers try to poison Florida water supply

The town of Oldsmar, Florida narrowly avoided a scary cybersecurity attack—a hacked water supply. Earlier this month, a supervisor for the town's water supply noticed a change in the concentration of lye as he worked on his computer. The supervisor had not made the change but watched in real-time as the levels increased ten-fold. Too much lye, or sodium hydroxide, can cause gastrointestinal issues such as abdominal pain and difficulty swallowing.

For years, cybersecurity experts have warned that much of our infrastructure is vulnerable to cyberattacks. Hacks of power grids, water supply, or natural gas companies could cause catastrophic damage., Water facilities are exceptionally vulnerable to attacks as there are over 50,000 in the country—all run by small corporations or towns. Because of this, many water facilities are lacking in proper cybersecurity, leaving them vulnerable to attack.

In Oldsmar, hackers gained access to the water facility's network through dormant remote access software. They were able to access all the computers on the network, allowing them to change the levels of different chemicals in the water supply. The hackers increased the lye levels to over 10,000—an amount that could have made 15,000 people sick.

Luckily, the supervisor noticed the change immediately and was able to stop the water from being affected. But this hack highlights the security issues that water facilities all over the country face. Many of these small facilities, including Oldsmar's, only have one IT person on staff to protect the network. If this hack had occurred in the middle of the night, it may not have been caught until hours later.

What does this hack tell us about our own cybersecurity?

The Oldsmar water facility hack reminds us that we must insist that our public infrastructure is better protected from cyberattacks. Write to your local government and representatives to demand more funds to protect these facilities.

Take a lesson from this hack and ensure that your work networks are secure. The hackers in this story gained access through remote access software, programs that many are using to work from home right now. Companies must ensure that these programs are up-to-date and secure before employees use them to connect to the network. Employees should also be using a VPN (virtual private network) to connect.

Employers must require strong passwords from employees when accessing the network or any other sensitive programs. Two-factor authentication should also be used for these account to provide an extra layer of security.

Cybersecurity shorts

$2.2 million cybersecurity system may have stopped SolarWinds hack. As the damage of the SolarWinds attack is assessed, ProPublica has learned of a promising defense that could have prevented damage from the hack. It is believed that the cybersecurity system the government paid $2.2 million to develop, "In-Toto," might have protected against the SolarWinds attack. But the government never required vendors to use the software. You can learn more about the program here.

Cybersecurity firm says more flaws were found in Solarwinds' software. This month, a cybersecurity company, Trustwave, identified three new "critical" flaws in software that has been produced by SolarWinds. Trustwave said that they had informed SolarWinds about the vulnerabilities, which could have enabled an attacker to compromise the networks of SolarWinds' customers. NBC News has written about the exploitable flaws.

Every CEO should know these five things about cybersecurity. Many CEOs often overlook cybersecurity. Often, they think that because their company is smaller or has nothing important to steal, they would be safe. However, most cyberattacks cost an average of $2.5 million dollars, which many small businesses wouldn’t be able to recover from. This article gives you five things every CEO should know about include risk management, compliance, and more.

FDA Named new Director of Medical Device cybersecurity. The FDA has named Kevin Fu, a University of Michigan Associate professor, to serve a one-year term as acting director of medical device cybersecurity. Many see Fu's appointment as an indication that the agency is looking to make cybersecurity a priority in 2021. To learn more about what others think of Fu's appointment and how it will help the FDA's cybersecurity, click here.

Should you revamp your cybersecurity training? Many security leaders have realized that having a once-a-year, boring, PowerPoint training has not been effective. In the past decade, cybersecurity trainings have become more fun, interactive, and even enjoyable. But despite

innovative cybersecurity training, people are still clicking links and not recognizing security threats. This article talks in-depth about things you should continue to include in your cybersecurity training such as accountability, input from security professionals, and more.

Do you have cybersecurity insurance? As cyberattacks cause major loss of revenue for businesses, cybersecurity insurance is being discussed more and more. A Sophos survey found that 84% of its 5,000 respondents have a cybersecurity insurance policy--but how do you know if it's the right fit for you? SecurityIntelligence lays out the pros and cons of cybersecurity insurance and gives you their verdict.

Many educators lack proper cybersecurity training. Keeping virtual classrooms secure is now more important and difficult than ever with almost 80% of K-12 and college-level educators reporting they are using some sort of online learning platform during the pandemic. Many haven't received cybersecurity training although most of school has moved online. You can learn more about the risks schools and educators are currently facing here.

The Biden Administration postpones Trump's plans to ban WeChat and TikTok. In August 2020, former President Trump signed an executive order to ban the apps WeChat and Tiktok as a response to what was deemed a national security threat they posed. In response, the Biden administration has "indefinitely placed on hold the plans to force the sale of TikTok's American division to Oracle and Walmart." To learn more about the apps' bans, click here.

Romance scams report a new high in 2020 at $304 million. Romance scams cost a record $304 million in 2020—a 50% increase over the previous year. CyberScoop goes in-depth and quotes the FTC saying, "Gift cards, along with wire transfers, are the most frequently reported payment methods for romance scams." The article also provides some tips to help you figure out if the person you are talking to online is a real or not.

Serious vulnerabilities have been found in LifeShield security cameras. Bitdefender experts announced that they had found serious vulnerabilities in LifeShiled home security cameras that could have allowed hackers to live-stream in your home without your permission. To learn more about this security breach, click here.

Smartphone users being attacked in new hacker scheme. A new scheme has hackers taking control of phones, intercepting calls and texts. Hackers have found an easy way to take over your smartphone, letting them confiscate your email and even clear out your bank accounts. This is even happening to tech-savvy people. These victims are falling for something known as SIM swapping. The SIM in your phone is the card that holds all of your information. Many cybersecurity firms are seeing fraudsters come in to stores claiming they've lost their SIM card; they get a new one or do a SIM card transfer. To learn more about these new schemes, click here.

Software updates

Adobe: Adobe released an update closing over 50 security vulnerabilities in various products this month, including Photoshop and Reader. There is also a zero-day vulnerability for Acrobat/Reader which is currently being exploited. You can learn more about the update here.

Google: If you use Google Chrome, be sure to update and restart your browser now. There is an active zero-day exploit. If you see the "update" button on your browser, click it to update your browser as soon as possible.

Microsoft: Microsoft released updates this month for over 50 security flaws. Nine of the vulnerabilities are considered critical with one already being actively exploited. The updates affect the Windows Operating system as well as other Microsoft programs. You can learn more about the updates here.