In this issue:

- **Cybersecurity shorts**
- **Software updates**

Welcome to your September Savvy Cybersecurity newsletter. As always, we saw new cybersecurity threats this month including those facing remote workers. Read on to learn about that, as well as:

- An update on the Twitter hack
- A breach affecting Garmin devices
- Investigations into Zoom and TikTok
- And more

Cybersecurity shorts

Fitness-tracking company Garmin suffers cyberattack causing a major outage. Earlier this month Garmin users noticed the syncing system was down for several days. Garmin says the outage was caused by a cyberattack but does not believe that customer data was stolen. The attack seems to have been caused by a new strain of ransomware called WastedLocker.

EMV cards help prevent fraud, but it depends on the bank you use. A new story by security expert Brian Krebs discovered that the effectiveness of EMV chip cards to prevent fraud varied based on the bank issuing the cards. With EMV cards, the embedded chip creates a one-time iCVV code when the card is inserted for that transaction. If the retailer is hacked, the iCVV card should not work for future transactions and the static CVV code (what is used for non-chip cards) should not be shared. Some banks, however, are sharing the static CVV code and iCVV code for the same purchase. The CVV code can be used for fraudulent online purchases or to create fake cards. Unfortunately, Krebs does not know which banks are not following EMV standards, but you can read the full story here.

Your booze order may come with a side of identity theft. Popular online delivery company Drizly fell victim to a data breach this month. The company gained many customers during the stay at home orders across the country as a safe way to get alcohol delivered. However, Drizly announced this month that a hacker gained access to customer email addresses, dates of birth, addresses, and passwords. Over two million customers are thought to be affected.

Zoom and TikTok face possible investigations from the Department of Justice at the request of Senators Josh Hawley (R-Mo.) and Richard Blumenthal (D-Conn.). The senators urge the DOJ to take a closer look at the two tech companies' data sharing policies as they are concerned about ties to the Chinese Communist Party. Both Zoom and TikTok have pushed back against the allegations.

Last month's massive Twitter hack was the result of a spear-phishing attack targeted at employees. Many of these employees had privileges for account management tools which allowed them access to verified Twitter accounts. Once the hackers were inside the employee accounts, they were able to tweet out from the accounts of public figures such as Jeff Bezos and Joe Biden. Twitter has not disclosed more details on how many employees were targeted.

Schools will face more cyberattacks as virtual learning begins across the country. Doug Levin, president of the K-12 Cybersecurity Resource Center warns that many school districts will face a cybersecurity crisis this year, since most are unprepared to fend off attacks. Levin believes hackers could target schools with ransomware and phishing attacks. Schools should audit their IT and communicate cybersecurity best practices to staff, students, and parents.

Working from home has changed the cybersecurity landscape, according to experts. As many are six months into working from home full-time, some workplaces have struggled with cybersecurity. To avoid future issues, experts advise employers to educate their employees on good cybersecurity practices and to ensure they have the correct tools to succeed. In many cases, this may be providing a work laptop or a Virtual Private Network (VPN). Experts predict that ransomware and phishing will continue to be major threats as companies work from home.

Take a second look before you click—that text about an unpaid bill is likely a scam. Consumers are reporting receiving phishing text messages that appear to be from AT&T about an unpaid internet or cell phone bill. The text will often advise you to call a number to unlock your account but the number goes to a scammer. If you get a text from any company about an unpaid bill, call the number listed on its website--not the text message.

Hackers go after small business loans and unemployment benefits after stealing personal information from a compromised data broker. Interactive Data LLC is a consumer data broker that appears to have been breached. Hackers have used the stolen information to apply for fraudulent benefits. You can read more about the story here.

Medical debt collection firm is hit with a ransomware attack. R1 RCM has taken its system offline after the ransomware took over its system. The company believes that the attack began with a phishing attack. R1 RCM is currently investigating but holds data on millions of people.

Software updates

Adobe: Adobe released critical updates for Acrobat and Reader this month. Be sure you update those programs as soon as possible here.

Microsoft: Microsoft released updates to close over 100 security issues this month. Two of these vulnerabilities are being exploited currently. One major issue affects Internet Explorer and can cause your entire system to be hacked by browsing a malicious website. Be sure to update your devices as soon as possible.