In this issue:

- **Colonial Pipeline Pays $5 Million Following Ransomware Attack**
- **Cybersecurity shorts**
- **Software updates**

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

Welcome to the Savvy Cybersecurity newsletter. This month we'll be sharing information on the Colonial Pipeline ransomware attack. Read on for more information on that, as well as:

- What all Peloton users should know about their security
- Necessary updates for all Apple users
- And much more

Colonial Pipeline Pays $5 Million Following Ransomware Attack

The largest gas and diesel pipeline system in the country was hit with a ransomware attack halting delivery of fuel to customers from Texas to New York earlier this month. Colonial Pipeline, which moves more than 100 million gallons of fuel daily, shut down after falling victim to a cyberattack.

DarkSide, a new ransomware group, is confirmed by the FBI to be responsible for the attack. The group, believed to be based in Russia, makes some $15 billion in annual revenue from ransomware attacks. Colonial Pipeline's IT department was hit with the ransomware, but the company took other systems offline during the attack out of an abundance of caution. As a result, there was a brief stoppage of all pipeline operations leading to panic and gas shortages in some states.

Colonial Pipeline is now up and running again after paying about $5 million in cryptocurrency to the DarkSide gang. Historically, the FBI has dissuaded companies from paying ransom in these attacks as it may encourage more ransomware activity. However, without a data backup it can be difficult to resolve this kind of hack without payment. According to experts, DarkSide is notorious for providing a very slow decryption process following a ransom payment.

This attack demonstrates the vulnerability of the infrastructure systems in the United States. Earlier this year, a Florida water supply was targeted by hackers. The Colonial Pipeline ransomware attack is yet another example of how cybersecurity can impact our national security. In response to the attack, President Biden signed an executive order tightening cybersecurity standards and rules for government contractors. The order requires federal contractors to quickly report incidents to agencies, establishes a new government entity to review data breaches, and sets a baseline of security standards for any software a government agency buys.

Ransomware is a threat to all

Government agencies, private companies, and individuals all need to be cognizant of ransomware attacks. The FBI has issued multiple warnings in the past few years on the growing threat of ransomware. And there are steps that you can take to protect yourself from it.

1. Beware of phishing emails

The first step in avoiding a ransomware attack is to be on the lookout for phishing emails. Often, hackers use phishing emails as a vehicle for ransomware. Be suspicious about any unsolicited email you receive. Before clicking on anything, follow the Savvy Cybersecurity rule of E.M.A.I.L—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.

2. Back up your data

If you do fall victim to a ransomware attack, you can avoid paying the ransom if you have your data backed up in other places. The Savvy Cybersecurity program teaches the rule of three—you should have all of your data saved in three places: your device, the cloud, and an external storage system.

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

Google moves to make two-step verification the default setting for users. Currently, Google users can opt in to the added security features. Google believes making multi-factor authentication the default on accounts will help boost security. Users will still be able to opt out but studies show that two-step verification makes someone's account 99.9% less likely to be compromised.

The Federal Rotational Cyber Workforce Program Act was reintroduced by a bipartisan group of senators this month. The Act would create a cybersecurity personnel rotation program to help grow and retain a highly skilled Federal cyber workforce. This Workforce Program Act would allow cybersecurity employees to work across multiple Federal agencies.

DOL issues their first guidance concerning cybersecurity and retirement plans. This is a part of their efforts to protect an estimated $9.3 trillion in retirement plan assets from increasing "internal and external cybersecurity threats." The guidance contains "Online Security Tips" for plan participants, explaining how individuals can protect their retirement information from hacks.

Cybersecurity training still needs work. A study by TalentMS revealed that cybersecurity training undertaken during the Covid-19 pandemic is still deemed insufficient. It was found that despite 59% of employees receiving cybersecurity training from their companies, 61% failed simple cybersecurity tests.

Do you use your dog's name as your password? Think again. Experts are urging people to create harder-to-crack passwords after new research found 15% of people use their pet's name as a log-in. The UK government's National Cyber Security Centre (NCSC) argues that such passwords can make it easier for hackers to force their way into people's accounts simply by guessing common pet names.

Health organizations are still targeted by ransomware hackers. A San Diego-based health organization and a Kansas-based organization have both faced cyberattacks in recent weeks. Fortunately, patient care was not affected, but the hacks highlight the threat healthcare organizations face.

Experian fixes weakness with partner website, yet researchers still worry. The major credit bureau, Experian, recently fixed a weakness with a partner website that let anyone look up the credit score of tens of millions of Americans just by supplying their name and mailing address. Experian has said it has plugged the data leak, but the researcher who reported the finding says he fears the same weakness may be present at countless other lending websites.

Peloton vulnerabilities may reveal personal information. The vulnerabilities could allow an individual to view personal information on Peloton users, including their location, gender and age, as well as class attendance, even if users have private mode on.

Software updates

Apple: Apple has released iOS 14.6 to close a number of security issues for iPhones and iPads. If you are an Apple user, be sure to update as soon as possible. One of the security flaws allows malicious audio files to reveal personal information to hackers. You can learn more about the update here.

Microsoft: Over 50 security vulnerabilities are patched with Microsoft's latest security update. Windows operating systems and Internet Explorer are affected by this update. One of the security issues could lead to ransomware attacks. Your device should prompt you to update, but you can learn more about it here.