NEWS Cyber Security

Vol. 6 | Issue 6

June 2021

Welcome to the TXDPS Cyber Security Newsletter!

Can you believe it's June? We are officially half way through 2021!

Hopefully you all had an awesome Memorial Day and had a chance to enjoy the Texas sun! If you are a veteran or currently still in the military our Cyber Team greatly appreciates your service and all you and your family do for our country.

In this edition of the newsletter Cyber Security wants emphasize some of our best practices for preventing business disruption from ransomware attacks. In recent news, a black hat hacking company named DarkSide infiltrated government pipelines. Please see page #3 for full story.

Defining Ransomware: it is a type of malicious software designed to block access to a computer/network system until a sum of money is paid.

How it works: There are a number of vectors ransomware can take to access a computer. One of the most common ways is a phishing scam that will come to the victim in an email disguised as a file they should trust.

If the file is opened and allowed to execute, the attackers will be able to take over the computer, especially if they have built-in social engineering tools that trick users into allowing any sort of permissions within DPS.

Remember, as employees we are the first line of defense against any malicious attacks. Please remember to report any suspicious email activity to Cyber Security.

How can ransomware attacks be prevented?

- Require multi-factor authentication for remote access to our IT networks
- Enable strong spam filters to prevent phishing emails from reaching end users at DPS
- Report emails from unknown sources and verify website links or attachments before you click
- Stay current on annual Cyber Security Awareness Training to better recognize threats
- Update software, including operating systems, applications, and firmware on IT network assets, in a timely manner
- Set antivirus/anti-malware programs to conduct regular scans
- Implement regular and frequent data backup procedures. This won't stop an attack, but it will make recovery easier.

Cyber Risk Management

In this month's newsletter we'd like to discuss the human element of risk management.

Cyber security risk management can't be achieved with fancy techy tools alone, it takes all of us working together. For many of you, the only interaction you have with your Cyber Security team is when we bug you to complete your annual required training. Hopefully in between trainings you read some super informative newsletters to stay reminded of security best practices. That should be enough right? We're meeting the compliance requirements so we should be good. After all, your job isn't cyber security…or is it?

When it comes to cyber security, most people have a perception that it is the sole responsibility of the IT or Security department. The truth is, we all use technology on a daily basis almost continuously throughout the day. Also, every individual is a potential target for scams. Your Cyber Security team can't have visibility into everything that is going on, so we rely on you to safeguard the tools and information you are using, and to remain vigilant against potential attacks. You don't have to have "security" in your job title to be a security person, it is everyone's job to ensure the privacy and accuracy of the information we use. Congratulations, you are all security professionals!

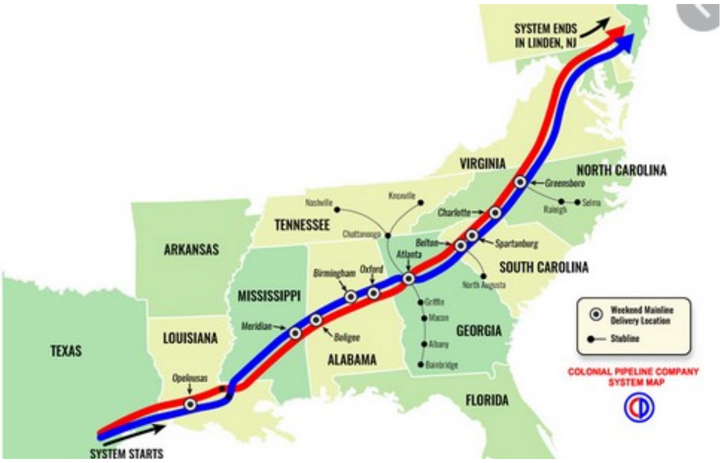
Our goal at DPS is to move beyond the minimum of security compliance and focus on security engagement. We want to help each of you develop good security habits on a daily basis. Here are a few key things to focus on:

1. Understand what information you are working with, how that information is classified, and how it should be protected. If you're not sure, ask your leadership or reach out to Cyber Security for guidance.
2. Practice good password security; make those passwords difficult for someone to guess! Get crafty with it.
3. Keep an eye on those emails and don't click or open anything that seems suspicious. Send any suspicious emails to Cyber Security so our team can review it and let you know if it's safe.
4. Be aware that phone scams are on the rise. These scams use social engineering techniques over the phone to elicit and obtain information that could be personal or confidential.
5. If you see something suspicious or unusual, or if you think you've made a mistake (such as clicking a link) don't fret, the best thing you can do is inform your security team immediately.

You all are a key part of our defense strategy and we couldn't do this without you. Because we don't say it enough, thank you for everything you do to help keep us secure! If you ever have questions or concerns please contact us at GRP_Cyber_Risk@dps.texas.gov.

Pipeline Attack/ Chase Phishing

A cyber attack forced the suspension of operations on a major US pipeline that transports 45 percent of all fuel consumed on the East Coast.



Colonial pipeline said the attack took place on Friday, May 7th, and also affected some of its information technology systems.

The company operates the largest refined-products pipeline in the US, transporting gasoline, diesel fuel, and home heating oil from Houston, Texas to New York Harbor.

An outside security firm is investigating the nature and scope of the attack and the Georgia-based company has also been in touch with law enforcement and federal agencies.

The precise nature and motive of the attack are unclear at the present time. Colonial Pipeline transports more than 100 million gallons of fuel daily, through a pipeline system spanning more than 5,500 miles between Texas and New Jersey.

Mike Chapple, teaching professor of IT, said systems that control pipelines should not be connected to the internet and be vulnerable to cyber intrusions.

Full story: Colonial Pipeline Cyber Attack

Cyber-Insurance Fuels Ransomware Payment Surge

(Lindsey O' Donnell | June 1st, 2021)

Companies relying on their cyber-insurance policies to pay off ransomware criminals are being blamed for a recent uptick in ransomware attacks.

In the first half of 2020, ransomware attacks accounted for 41 percent of the total number of filed cyber-insurance claims, according to a Cyber Claims Insurance Report released last year by Coalition.

And indeed, in real-world attacks over the past two years, many companies afflicted by ransomware acknowledged that they had utilized cyber-insurance to deal with either the ransom itself or the ensuring cost of remediation.

For instance, weeks after Rivera Beach, FL was hit by ransomware in June 2019, the city council held an emergency meeting. It voted unanimously to authorize the city's insurer to pay off a $600,000 ransom demand, after the malware had frozen crucial data. Adversaries also took systems that control city finances and utilities offline.

That same month, Lake City, FL paid ransomware attackers almost $500,000, which the city announced would be mostly covered by insurance.

Full Story: Cyber Insurance

In the News

Some Amazon devices will now share your Wi-Fi unless you opt-out — here's how

(Doug Delony | June 7, 2021)

Amazon's Sidewalk feature has raised concerns about privacy and security because it opens up a part of your home's internet connection to nearby strangers. Sidewalk automatically launches Tuesday, June 8, in the United States. But many critics say the program should be opt in instead of opt out and that it shouldn't be automatic.

Amazon claims it is secure and that your personal information will not be revealed, but still, many people who have Amazon devices have their concerns and are looking to turn off the function. (If you don't have an Amazon device, you will not be in the Sidewalk program.)

The short version: Amazon is looking to extend the range and reliability of its Ring and Echo devices, including security cameras and lights. For instance, if the internet goes out at the home where they are in use, these devices can attempt to connect to a neighbor's internet via the new Sidewalk functionality. It also aims to help tile trackers work better.

Amazon claims to only use a very small portion of your internet bandwidth, and says it is not sharing anything from your home PC or network.

It is possible to opt-out and disable Amazon Sidewalk. If you have a Ring device, go to the control center on the app or their website. If you have an Echo device, go to settings in the Alexa app. (Detailed instructions can be found in the linked article below.)

(From Amazon): *However, disabling means missing out on Sidewalk's connectivity and location related benefits. You also will no longer contribute your internet bandwidth to support community extended coverage benefits such as locating pets and valuables with Sidewalk-enabled devices*."

Full story: Amazon Sidewalk

Amazon Sidewalk Information: Amazon Sidewalk FAQs

A Few More Cyber News Stories:

SolarWinds Hack: Nation-state attackers could have launched supply chain attack nine months before previously thought

Full Story

Biden's Cybersecurity Executive Order Puts Emphasis on the Wrong Issues:

Full Story

100M Android Users Hit By Rampant Cloud Leaks:

Full Story

Microsoft, Google Clouds Hijacked for Gobs of Phishing:

Full Story

Cyber Challenge

Game Time!

This Month's Challenge

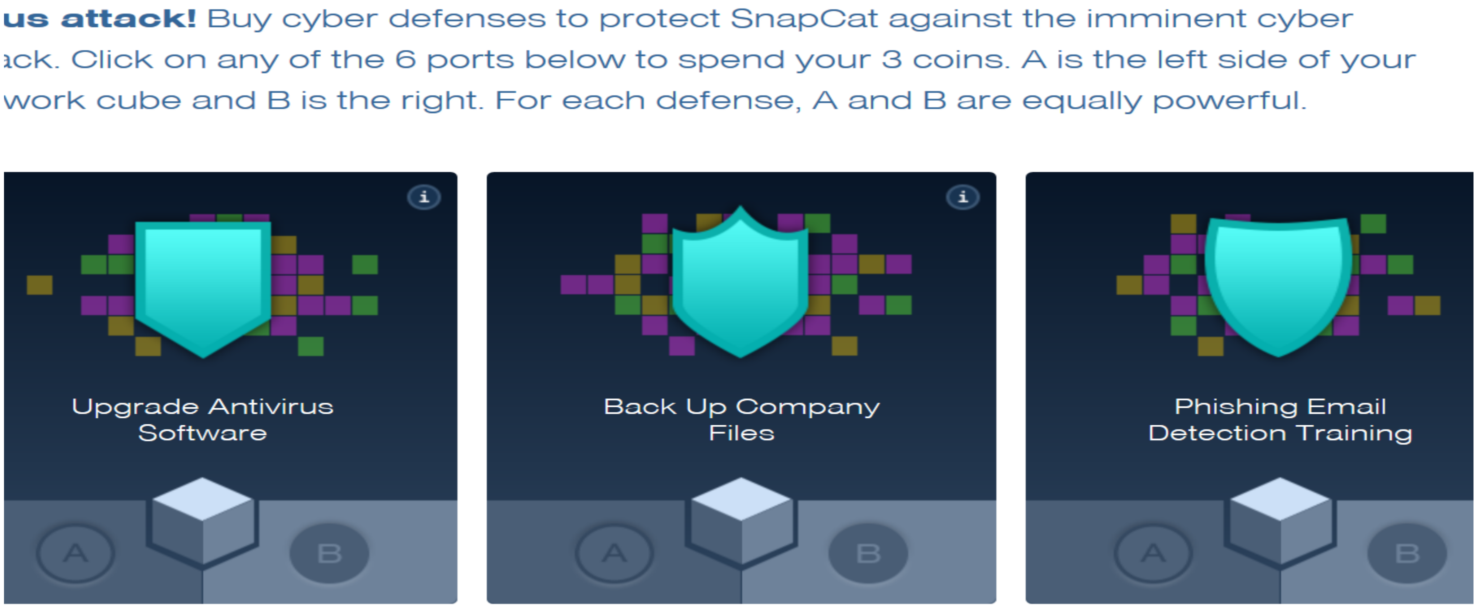
For this month's challenge, as the CTO of a start-up social networking company (options include the cleverly named Einstagram, SnapCat, WattsAmp, and Phasebook), you'll be in charge of cybersecurity during increasingly sophisticated attacks. Bolster your defenses to fend off foes in varying challenges that involve password and code cracking, and more.

The idea: Take cybersecurity into your own hands. In this Lab, you'll defend a company that is the target of increasingly sophisticated cyber attacks. Your task is to strengthen your cyber defenses and thwart the attackers by completing a series of cybersecurity challenges. You'll crack passwords, craft code, and defeat malicious hackers.

The goal: We want to see how well employees at DPS can identify numerous cyber security attacks!

Good luck! (Click the link below to get started. Estimated total time to complete: 30 minutes)

https://www.pbs.org/wgbh/nova/labs/lab/cyber/



us attack! Buy cyber defenses to protect SnapCat against the imminent cyber ıck. Click on any of the 6 ports below to spend your 3 coins. A is the left side of your work cube and B is the right. For each defense, A and B are equally powerful.

Please let us know how you did, so we can include you in next month's newsletter!

Feel free to check-out the other cyber security-related content on the PBS NOVA Labs website.

</Closing Comments>

As we close this month’s newsletter, we’d like to give a quick shout out to those of you who submitted your completed challenges from last month! We fully appreciate you taking a few minutes out of your day to engage with us!

A big THANK YOU to:

- Faye K.
- Vikki G.
- Sharon H.
- Victoria M.
- Debra L.
- Lillie P.
- Lance J.
- Eddy H.
- Lisa S.
- Kirbie W.

If we missed you, let us know!

In closing I want to remind everyone that Cyber Security’s deadline is coming up for reporting our annual training compliance to DIR. I would like to remind users to help us out and make sure you get your training completed. If anyone is due or overdue they will receive an email notification. If you didn’t see an email from us then you’re probably fine, but if you’d like to check your training status feel free to reach out to (GRP_Security_Awareness_Training).

Directions on how access the SANS Cyber Security Awareness Training.

1) Visit the DPS Services page using Firefox or Edge
2) Click on the Cyber Training Tab
3) Type in your username and password you normally use signing into your computer
4) Finally, click on the SANS Cyber Security Awareness Training icon from your home screen dashboard
5) Complete all of the training modules!

Thank you for swinging by and checking out this month’s newsletter! I’d like to reiterate I’m always open to feedback, either regarding this newsletter, our awareness training, or anything related to cyber security awareness here at DPS. If you have ideas to share, please continue to send them our way (Grp_Security_Awareness_Training).

Share and Connect

Newsletter Archive