NEWS CYBER SECURITY
Vol. 6 | Issue 10
October 2021

Page 2 | Page 3 | Page 4 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

Can you believe Halloween is on the way? And the holidays are almost here! Happy October, everybody.

October is a special month for us because it's Cybersecurity Awareness Month (CSAM), a global effort to help everyone stay safe and protected when using technology whenever and however you connect.

And this year, DPS has pledged its commitment to CSAM by signing up as a 2021 Champion, officially joining that global effort to promote cyber awareness. The Cybersecurity Awareness Month Champions Program is a collaborative effort among businesses, government agencies, colleges and universities, associations, nonprofit organizations, and individuals committed to the Cybersecurity Awareness Month theme of "Do Your Part. #BeCyberSmart."

More than ever before, technology plays a part in almost everything we do. Connected devices have been woven into society as an integral part of how people communicate and access services essential to their well being. Despite these great advances in technology and the conveniences this provides, recent events have shown us how quickly our lives and businesses can be disrupted when cyber criminals and adversaries use technology to do harm. Cybersecurity Awareness Month aims to shed light on these security vulnerabilities, while offering actionable guidance surrounding behaviors anyone can take to protect themselves and their organizations. Everyone has a responsibility to do their part in securing our interconnected world.

We want to help you, your family, friends, and our community stay safe all year long, too. We encourage you to sign up as an individual Cybersecurity Awareness Month Champion. After signing up, you'll receive a toolkit of free resources, including simple online safety habits and steps you can take to #BeCyberSmart.

Throughout this month, we will also be sharing weekly content developed by a Digital Forensics Expert describing how she secures her home, while providing practical advice on how to keep your family safe online with a focus on proper device usage and limits for all age groups.

You can access the #SecureTheFamily series we'll be using here: https://www.sans.org/mlp/secure-the-family/#watch-videos..

Please feel free to share those resources with your family and friends!

Cyber Risk Management

For this month's highlight of cyber risk controls, we are taking a closer look at Cyber Security Awareness; the one we just mentioned that gets an entire month of global attention and focus because of its importance in preventing breaches.

In fact, Verizon's 2021 Data Breach Investigations Report (DBIR) top finding states that 85% of breaches involved a human element; a mix of accidental disclosures and hasty clicks. Mitigating human risk through cyber security awareness adds another layer of protection to our security posture.

Attackers today rarely bother trying to attack businesses through technological means only. Today's attackers typically target people as an easy way into protected networks. They take advantage of people's natural curiosity, propensity to react to urgency, and willingness to help somebody in need. They also capitalize on lack of awareness.

That's where you come into the picture. When DPS employees are cyber security aware, it means we all understand what cyber threats are, the potential impact a cyber-attack will have on our agency, and the steps required to reduce risk and prevent cyber-crime infiltrating our online workspace. And, of course, all of this translates to our technology resources and sensitive data in our homes.

Our goal with our cyber awareness program isn't just to meet state compliance. It's to empower DPS staff to partner with Cyber to fulfill our potential as a united front. Being cyber aware is another way we can team up to protect and serve our customers and fellow Texas residents. It's an old adage in this space that "users are the last line of defense." But, we genuinely aim for our staff to be Cyber's best asset of cyber defense.

Often, it's just simple awareness that is the key to that level of protection and prevention.

With that in mind, and as part of our involvement in CSAM, we've invited a speaker from the Department of Homeland Security's Cybersecurity Infrastructure and Security Agency (CISA) to offer a **virtual Lunch and Learn** on **October 13th at 12:30p**.

So mark your calendars and save the date! This 30 minute chat will be via WebEx, and we'll have some time to ask him cyber-related questions. More details (including the link to join) to follow.

Here's a quick snippet from the bio of our guest speaker, Ernesto Ballesteros:

Mr. Ballesteros is the Cybersecurity Advisor for the Capital Region of Texas, as well as the Cybersecurity State Coordinator of Texas, for the Department of Homeland Security's (DHS) Cybersecurity Infrastructure and Security Agency (CISA).

Prior to joining CISA, Mr. Ballesteros served the State of Texas, as the State Cybersecurity Coordinator and Chairman of the Texas Cybersecurity Council, at the Texas Department of Information Resources (DIR), where his primary charge was to "oversee cyber matters" for the State of Texas.

We are excited to hear what he has to share. We sincerely hope you'll grab some food, fire up WebEx and join us on October 13!

QR Codes

We've received a few questions about using QR codes, and while we've determined there isn't really a risk by us creating and using these for business purposes, there are some risks that come with the use of QR codes in general:

1. QR codes can be used for phishing just like links in an email. Since we don't know what a QR code links to until we scan it, it's easy to get tricked into going to an unwanted website.

   If QR codes are used by DPS to share information with the public (such as link to a DPS public webpage), the bad guys could also jump on this trend and start trying to phish the public with fake DPS QR codes, thereby damaging our reputation. There's really nothing we can do to stop this, but it's something we should be aware of.

2. Along the same lines, if QR codes are used internally, then we may become more comfortable scanning QR codes with our DPS mobile devices, which could lead to us to scanning a malicious QR code (basically the same as clicking on a malicious link in an email). We should be mindful to only scan trusted DPS QR codes with our DPS devices.

So what can we do to avoid malicious attacks via QR codes in general?

Check for signs of tampering
Particularly when scanning QR Codes from print materials in public places, it's possible that the original QR Code has been replaced with a sticker of the dangerous one. Double-check that the QR Code on the material looks original and fits with the design.

Verify the company and the given URL
This is one of the most important points that all QR Code users should double-check. Before scanning, think: Does this company look legitimate? Does the design look professional? Does the QR Code match? If this all checks out, once you've scanned the QR Code and are redirected to a website, use the same company verification process. Furthermore, it's extremely important to check the URL and see if it's composed in a strange manner or differs from the website graphics, or if it has two different names.

Avoid providing personal information if directed to another website
If the particular website you are directed to asks for any personal information, do not enter anything like login information, passwords, or credit card details. Many marketing campaigns may ask for your name and email or to make direct purchases, so in these cases, you have to decide for yourself whether or not it feels secure. Regardless of the context, if something seems fishy, don't do it.

In the News

Port of Houston Target of Suspected Nation-State Hack

(Associated Press | September 24, 2021)

A major U.S. port was the target last month of suspected nation-state hackers, according to officials.

The Port of Houston, a critical piece of infrastructure along the Gulf Coast, issued a statement Thursday saying it had successfully defended against an attempted hack in August and "no operational data or systems were impacted."

Cybersecurity and Infrastructure Security Agency Director Jen Easterly initially disclosed that the port was the target of an attack at a Senate committee hearing Thursday morning. She said she believed a "nation-state actor" was behind the hack, but did not say which one.

"We are working very closely with our interagency partners and the intelligence community to better understand this threat actor so that we can ensure that we are not only able to protect systems, but ultimately to be able to hold these actors accountable," she said.

Sen. Rob Portman, R-Ohio, said the hack was "concerning" and said the U.S. needed to "push back against these nation-state actors who continue to probe and to commit these crimes against our public and private sector entities."

The hack involved ManageEngine ADSelfService Plus, a password management program. Easterly's agency, the FBI and the U.S. Coast Guard issued a joint advisory last week warning that the vulnerability in the software "poses a serious risk" to critical infrastructure companies, defense contractors and others.

Cybersecurity has become a key focus of the Biden administration. A devastating wave of cyberattacks has compromised sensitive government records and at times led to the shutdown of the operations of energy companies, hospitals and schools.

The SolarWinds espionage campaign, which the U.S. government said was conducted by Russian hackers, exposed the emails of 80% of the accounts used by the U.S. attorneys' offices in New York and affected several other departments. The Associated Press reported in June that suspected Chinese state hackers had recently targeted telecommunications giant Verizon and the country's largest water agency.

Full Story: https://www.securityweek.com/port-houston-target-suspected-nation-state-hack

A Few More Cyber News Stories:

Phone scammers use COVID-19 vaccine appointments to try tricking victims into downloading malware
https://www.cyberscoop.com/phone-scammers-use-covid-19-vaccine-appointments-to-try-tricking-victims-into-downloading-malware/

Hackers Are Going 'Deep-Sea Phishing,' So What Can You Do About It?
https://threatpost.com/hackers-deep-sea-phishing/174868/

Uber security alert scam spoofs real Uber number—Watch out!
https://blog.malwarebytes.com/malwarebytes-news/2021/09/beware-uber-scam-lures-victims-with-alert-from-a-real-uber-number

CYBER
CHALLENGE

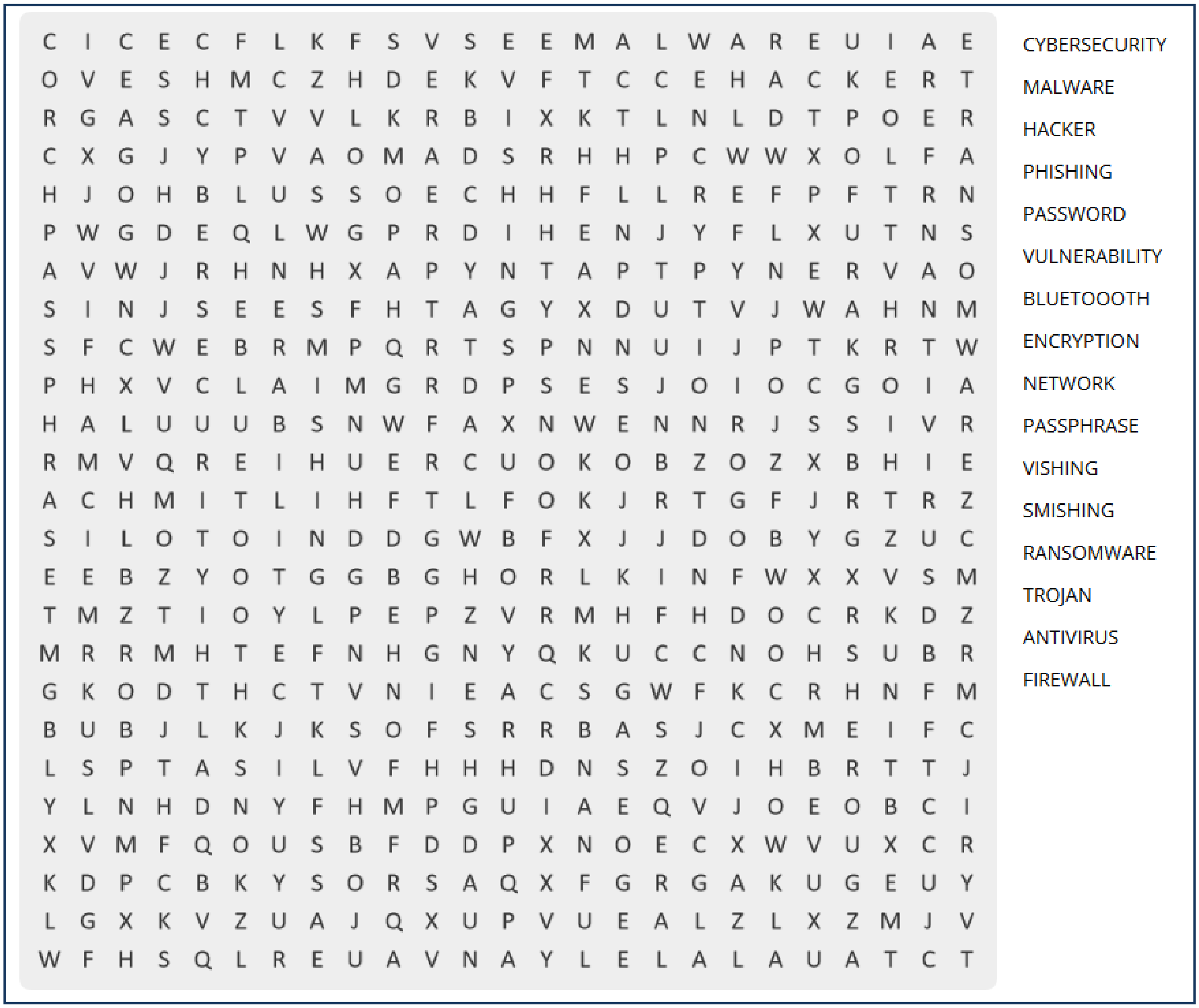
The Weakest Link

This Month's Challenge

For this month's challenge, let's tackle a good ol' Cyber Word Search.

Click on the word-grid image below to launch the website and get started. Once you locate a word, click and drag from the first letter in the word to the last letter and then release. The letters will be highlighted. If they match a word in the list, the outline will remain and the word will be crossed off the list.

Send me a snapshot of your completed puzzles! Good luck.



```
C I C E C F L K F S V S E E M A L W A R E U I A E
O V E S H M C Z H D E K V F T C C E H A C K E R T
R G A S C T V V L K R B I X K T L N L D T P O E R
C X G J Y P V A O M A D S R H H P C W W X O L F A
H J O H B L U S S O E C H H F L L R E F P F T R N
P W G D E Q L W G P R D I H E N J Y F L X U T N S
A V W J R H N H X A P Y N T A P T P Y N E R V A O
S I N J S E E S F H T A G Y X D U T V J W A H N M
S F C W E B R M P Q R T S P N N U I J P T K R T W
P H X V C L A I M G R D P S E S J O I O C G O I A
H A L U U U B S N W F A X N W E N N R J S S I V R
R M V Q R E I H U E R C U O K O B Z O Z X B H I E
A C H M I T L I H F T L F O K J R T G F J R T R Z
S I L O T O I N D D G W B F X J J D O B Y G Z U C
E E B Z Y O T G G B G H O R L K I N F W X X V S M
T M Z T I O Y L P E P Z V R M H F H D O C R K D Z
M R R M H T E F N H G N Y Q K U C C N O H S U B R
G K O D T H C T V N I E A C S G W F K C R H N F M
B U B J L K J K S O F S R R B A S J C X M E I F C
L S P T A S I L V F H H H D N S Z O I H B R T T J
Y L N H D N Y F H M P G U I A E Q V J O E O B C I
X V M F Q O U S B F D D P X N O E C X W V U X C R
K D P C B K Y S O R S A Q X F G R G A K U G E U Y
L G X K V Z U A J Q X U P V U E A L Z L X Z M J V
W F H S Q L R E U A V N A Y L E L A L A U A T C T
```

CYBERSECURITY
MALWARE
HACKER
PHISHING
PASSWORD
VULNERABILITY
BLUETOOOTH
ENCRYPTION
NETWORK
PASSPHRASE
VISHING
SMISHING
RANSOMWARE
TROJAN
ANTIVIRUS
FIREWALL

</Closing Comments>

As we close this month's newsletter, we'd like to give a quick shout out to those of you who took the time to engage with our cyber challenge. We fully appreciate you taking a few minutes out of your day to engage with us. Please keep doing so; and get others to join you.

A big THANK YOU to:

Wendy S.

Ms. Wendy was the only brave soul to submit a poster this month. Scroll one more page to check it out. Thanks so much! It was great!

Last month, I asked for your "I was scammed" horror stories, and y'all had some doozies! Thank you for sharing. Here are a few stories from your DPS coworkers.

"I was in the mix of the millions of people whose information was breached with T-Mobile. I was walking with a friend and my phone kept buzzing which was odd, I usually don't get evening emails, and within a 30 minute time span, my email was used to log into Netflix, the email and phone number changed and charged through PayPal for the connection. I am still scratching my head on how they were able to see the code as my email account never asked for a two-step verification when signing in. Nonetheless, I removed my payment method off of PayPal and submitted a fraudulent charge as well as change my email password. Since then, my email has been spotted on the dark web but nothing more has been detected at this time."

"My scam story - I still don't understand what this was or how it happened. I received a phone call while I was shopping in Central Market. The caller asked me if my name was [my name], I said yes. He asked me if I recently bought a train ticket to a specific destination. I said, 'no I did not.' He replied, 'just as we thought this was fraudulent charge.' This was about 10 years ago so I don't remember all the questions, but I only replied 'yes' or 'no' to them, trying to be smart about the call from a stranger. By the time I reached the register, my checking account was emptied. The call was from an odd 4 digit number. Never answer a call from strange numbers!!"

How's that for some October spook? I'll be sharing the others soon. Be safe out there!

I'm looking forward to sharing some cool stuff in the coming weeks for Cybersecurity Awareness Month. As always, let me know if you have any feedback to share. Thanks for what you do!

-Eric Posadas

TIPS TIPS TIPS

CHECK FOR ACCURACY BEFORE YOU SEND

YOUR PRIVACY IS CRITICAL, KEEP IT!

BEWARE OF SCAMMERS

ELIMINATE FAKE ACCOUNTS

RESEARCH TO GET THE FACTS

Secure your passwords

Always check before opening unknown files

Follow ALL your Cyber Security Training Officer's tips

Each one

Teach one

You'll be glad you did !!!