CYBER SECURITY NEWS

Vol. 5 | Issue 9

October 2020

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

Welcome to the TXDPS Cyber Security Newsletter!

We hope this month's newsletter finds you and your family well. Hopefully, those of you with kids in school have found a rhythm, and those with family and friends in education have found a source of encouragement and strength for them to plug into. Hang in there!

Can you believe it's already October? Or…maybe you're thinking it's *only* October. Either way…it's here. And that means so is National Cyber Security Awareness Month (NCSAM)!

Cyber Security Awareness month was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online. Since its original inception under leadership from the U.S. Department of Homeland Security and the National Cyber Security Alliance (NCSA), Cyber Security Awareness Month has grown exponentially, reaching consumers, small and medium-sized businesses, corporations, educational institutions and young people across the nation. Now in its 17th year, Cyber Security Awareness Month continues to build momentum and impact co-led by NCSA and the Cybersecurity and Infrastructure Agency (CISA).

CYBERSECURITY AWARENESS MONTH

So…what's this mean for you and DPS?

Well, for starters, you'll be hearing from us more often over the next few weeks. (Please, hold the applause.) We want to use this as an opportunity to share more information and make sure you feel more prepared to face the many cyber threats online while you're in the office or working from home, and in your every day life. We'll be providing tips for working from home more securely, giving you the heads up on some free cyber security webinars, and trying to do what we can to get you bought into the cyber awareness culture.

NCSAM also provides you the opportunity to make sure your friends and family feel confident about their preparedness as they continue to experience life more and more online. Partner with us to help spread awareness! Cyber Security Ambassador, anyone?

This month's theme, "**Do Your Part. #BeCyberSmart**", highlights the importance of empowering individuals (that's you!) and organizations to better protect their part of cyberspace in an increasingly connected world.

We look forward to doing just that. If you have any questions or ideas, please send them our way!

Cyber Risk Management

As a reminder, we introduced this section last month because we wanted to use this space to focus more on specific security controls that you may encounter when interacting with our Cyber team. Remember, a security control is simply a protective measure that is put in place to prevent or manage a security risk. We want you to know *why* we ask you to do the things we ask you to do.

Something you may have heard of when it comes to cyber security is a principle called "**Least Privilege**." The basic concept of least privilege is that we allow a user the least amount of access (or permissions) necessary for them to perform their assigned duties and nothing more. The goal is to minimize risk to our agency.

Most advanced attacks today rely on the exploitation of privileged credentials like admin rights. Meaning, if a user account has admin rights and is then hacked, the hacker has full access to otherwise restricted, critical systems. Limiting these rights to an as-needed basis reduces our cyber attack surface. The infamous Target breach of 70 million customer accounts happened because an HVAC contractor had too many permissions to their network. When that account was hacked, the hackers had free reign. Least privilege could have helped prevent this.

It also helps stop the spread of malware as many times, malware needs elevated rights to install itself and then spread agency-wide. And, least privilege protects you as the user from accidentally changing or unintentionally deleting information. Essentially, the least privilege approach narrows the scope of harm that can be caused by the unwanted or unauthorized use of network privileges.

Another control that goes hand-in-hand with least privilege is "**Separation of Duties**." Separation of duties means that no one person should be solely accountable for certain business operations; it's a system of checks and balances so one user doesn't own the entire process from start to finish. It is mostly put in place for two things: avoiding conflicts of interest that could result in abuse or fraud, such as an employee submitting and then approving their own report, and preventing control failures that could result in data theft or security breaches. And, again, this also protects us from accidental damage.

In both cases, the idea is to allow the right people to have the access that they need to do their jobs, but not enough access to bypass controls or run a process without oversight. These principles protect us from malicious attacks, whether outside or inside our network, and assists us in mitigating unintentional inside threats.

Cybercrime and the Pandemic

This global pandemic isn't going anywhere for a while it seems, and cyber-criminals continue to use this fact to their advantage. They have focused heavily on the issues related to the pandemic to launch attacks such as phishing, ransomware, and malware as well as exploit the increased reliance on home networks and IoT devices (e.g. smart thermostats, streaming devices, or any home appliance that connects to the Internet). In fact, ransomware alone has increased over 700% globally. In addition, malware developers also continue to target applications commonly used by remote employees, such as the Zoom video conferencing platform.

The pandemic has also exposed new cracks in organizations' cyber defenses, with a recent report finding just under half of businesses have experienced at least one "business impacting cyber-attack" related to COVID-19 since April 2020. For the most part, COVID-19 has exacerbated pre-existing cyberthreats.

Speaking to *Infosecurity Magazine*, a global cybersecurity researcher at Bitdefender explained that he expects cyber-criminals to continue leveraging the COVID-19 pandemic to launch attacks throughout the rest of 2020. "If during the first half of 2020 cyber-criminals have been exploiting the pandemic with messages promising miracle cures and medical devices or equipment meant to protect users from infection, during the second half we'll likely see attackers exploiting the economic and social aftermath of the pandemic," he said.

"Spam or fraudulent messages will likely exploit the way both private and public companies have changed their interaction with users. For example, messages claiming to be from financial institutions asking customers to update their personal and financial data or promising financial relief, because they can no longer do it in person in light of COVID-19 restrictions."

Hackers aim to exploit vulnerable situations, and the global disruption brought on by COVID-19 is no different.

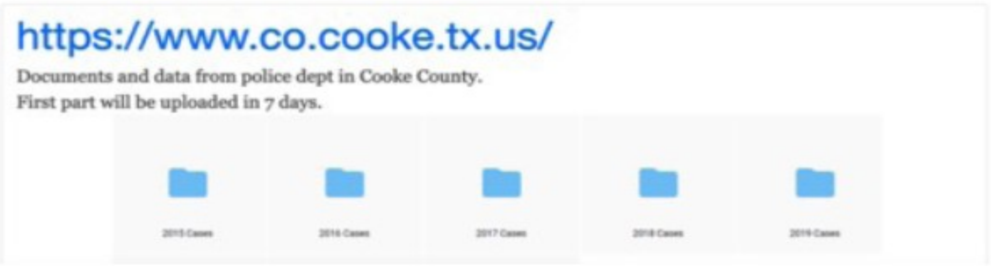
Please continue to use good cyber hygiene, slow down before clicking links and opening attachments in email, and report anything suspicious to our Cyber team.

Think before clicking.

In the News

Cyberattacks Targeting State and Local Government Increase by 50%

(By Stu Sjouweman | September 24th, 2020)



https://www.co.cooke.tx.us/

Documents and data from police dept in Cooke County.
First part will be uploaded in 7 days.

Screenshot from Happy Blog, an auction website for data exfiltrated by ransomware - in this case featuring data stolen from Cooke County, TX.

via BlueVoyant's *State and Local Government Security Report*

State, local, tribal, and territorial government agencies and municipalities are under attack. Observations and data from security vendor BlueVoyant highlight the attacks and the results. We've long known that state and local government has been a target. But new data from BlueVoyant's *State and Local Government Security Report* makes the case that it's only getting worse.

According to the report:

- Monthly attacks have risen 50% since 2017
- Ransoms rose from $30,000 in 2017 to over $1,000,000 in 2019
- 555 compromised email accounts across only 38 analyzed data breaches
- 95K incidents of inbound targeting of SLTT in just 6 months

The bad guys realize government is expected to always be running so we are the perfect target to take out with ransomware. Government agencies also do business with countless companies with money changing hands, making us a prime target for fraud.

From the report, "Over the last few years, attacks against municipalities have risen in frequency and cost. These attacks are driven by pervasive ransomware strains, which hold governments to ransom for larger and larger sums and often exfiltrate sensitive data whether they are paid or not. The rise in attacks is also often driven by ease of access. State and local governments are rapidly improving their cybersecurity posture to secure their systems and protect against persistent adversaries. However, they suffer from differences in funding and preparedness, a lack of standardized policies, and systems that are digitizing faster than their security and infrastructure can keep up."

Source: https://blog.knowbe4.com/cyberattacks-targeting-state-and-local-government-increase-by-50

A Few More Cyber News Stories:

iPhone 12 scam pretends to be Apple "chatbot" – don't fall for it!
https://nakedsecurity.sophos.com/2020/09/24/sms-phishing-scam-pretends-to-be-apple-chatbot-dont-fall-for-it/

Lame-duck versions of TikTok and WeChat are definitely a problem, security experts say
https://www.cyberscoop.com/tiktok-wechat-ban-security-issues/

Seven out of ten CISOs fear that cyberwarfare is an impending threat
https://www.itsecurityguru.org/2020/09/25/seven-out-of-ten-cisos-fear-that-cyberwarfare-is-an-impending-threat/

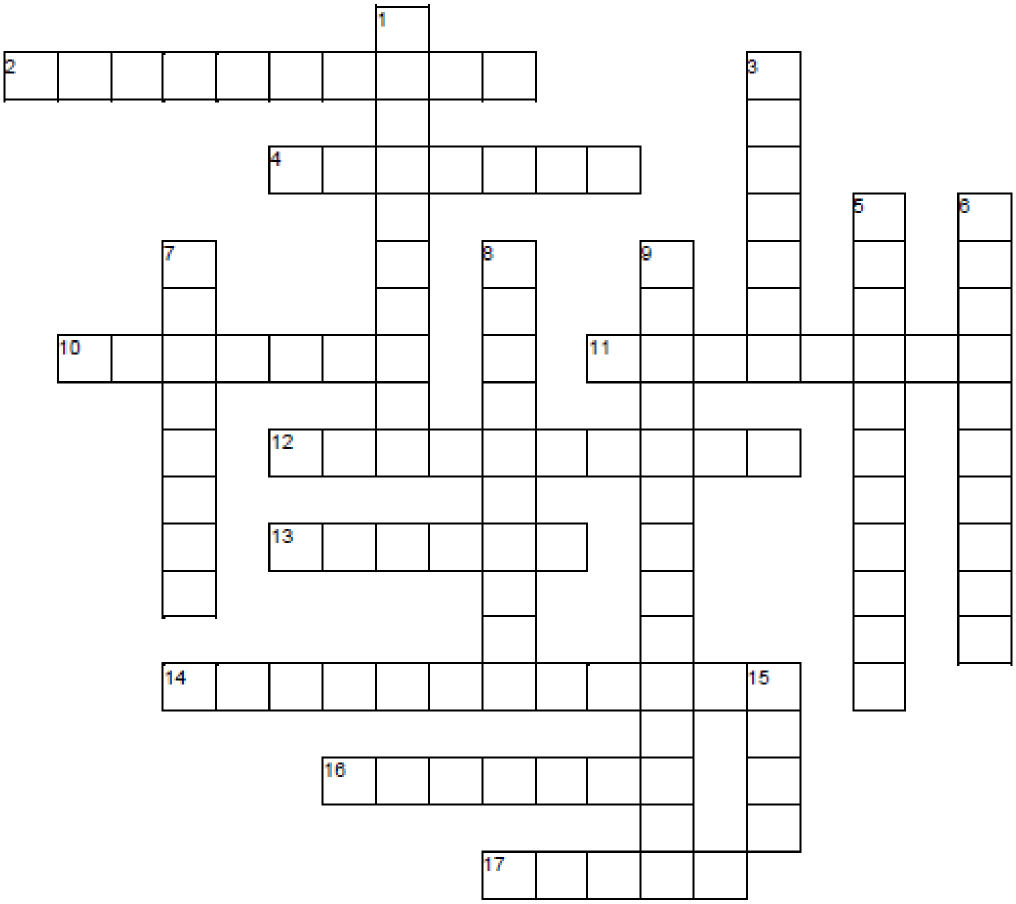
Cyber

Crossword Puzzle

This Month's Challenge

For this month's challenge, let's get back to puzzle solving. Let's see how much of that cyber awareness training stuck with you after watching all those videos! I admit, I borrowed this from a 3rd-party, and a few answers will make you wrinkle your nose a bit. But most of them are spot on and great to keep in mind! If you get stuck, ask me for a hint!

Everyday Security



Across

2. when our information is compromised
4. often hidden in e-mail attachments
10. take sensitive conversations somewhere ______
11. you have one of these for each account
12. meant for specific employees only
13. what to do when you see something wrong
14. information not meant for sharing
16. everyone must use their own ______
17. how you should destroy hard copies

Down

1. people who enter behind you
3. keeps your computer defended
5. what the criminals want
6. required to access data
7. scams in your inbox
8. the digital threat
9. how much data should you see?
15. do this to your computer when you walk away

</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 all who submitted an answer!

If we missed you, let us know!

Last month, I provided some resources to help you have cyber security chats with your kiddos. I'd like to do the same this month as children are continuing to attend school, visit friends and move more daily activities online.

Living Security is an Austin-based cyber security awareness company, and they'll be delivering a series of free webinars as part of their *Family First* initiative. "Family First is designed to help you with the information you need, the steps you should take and provide the tools you need to protect the children in your lives. In partnership with leading technology companies across the world, our goal is to help make cybersecurity easy to understand, memorable and impactful." Register here: https://livingsecurity.com/family-first/

Living Security's Family First Series

3 VIDEOS TO WATCH WITH YOUR FAMILY & SHARE

3 EXPERT WEBINARS TO DISCUSS THE LATEST RISKS ONLINE

RESOURCES TO HELP YOU KEEP YOUR FAMILY SAFE

Thank you for swinging by and checking out this month's newsletter! I continue to learn more and more about this agency as I find my footing here and fully appreciate all that you do. 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.

And, as always, thank you for what you do for DPS and for your cyber vigilance!

- Eric Posadas