Cyber Security NEWS
Vol. 5 | Issue 3
March/April 2020

TXDPS Cyber Security Newsletter

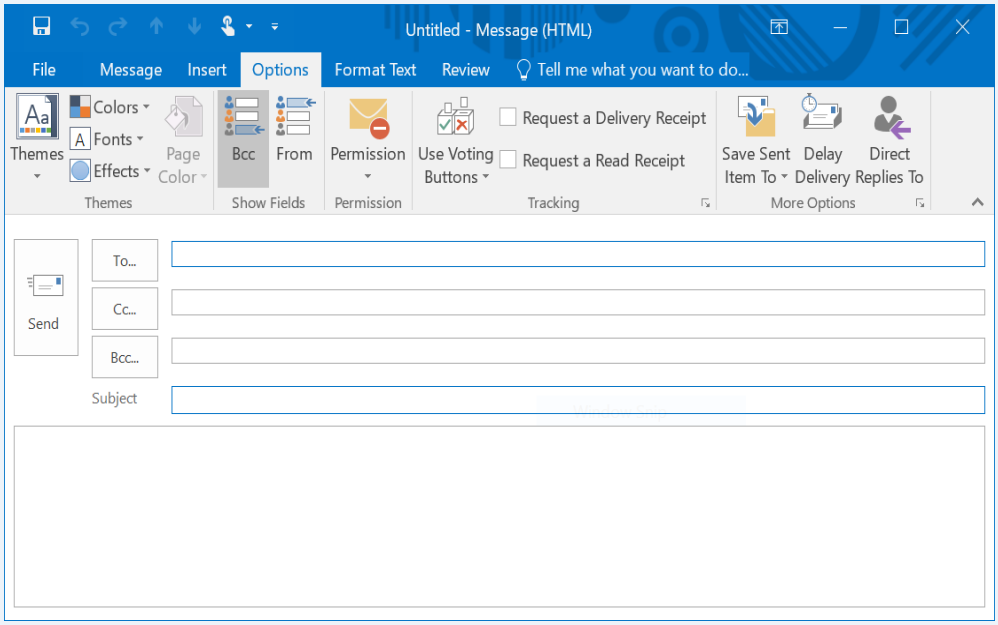
TXDPS Cyber Security welcomes you to the March/April TXDPS Cybersecurity Newsletter.

To start the newsletter, we want to let all DPS readers know about a change in the law regarding Cybersecurity Awareness Training. House Bill 3834, which passed in the last Legislative session, amended Texas Government Code 2054 mandating annual Security Awareness Training for all state employees and contractors (2054.519, Cyber Security Training Requirement). The new law requires all state employees and contractors who have access to the DPS information system or computer to complete a cybersecurity awareness training program every year.

It was recently observed users sometimes send emails outside the Agency which have a large number of email recipients. While this is not really a security risk, it could be a business or privacy risk. Blind Carbon Copy is a perfect way to send to everyone while still protecting their email addresses.

What is blind carbon copy and why is it important? Blind carbon copy, also referred to as Bcc, is a way of sending an email to multiple people without them knowing who else is receiving the message. It is especially useful when sending bulk email messages because it would not reveal all the other recipients and would prevent the dreaded mistake of a recipient replying to all.

If the Bcc field is not available when creating a new message, it can be enabled by clicking the "Options" tab and then the "Bcc" button within the "Show Fields" section.

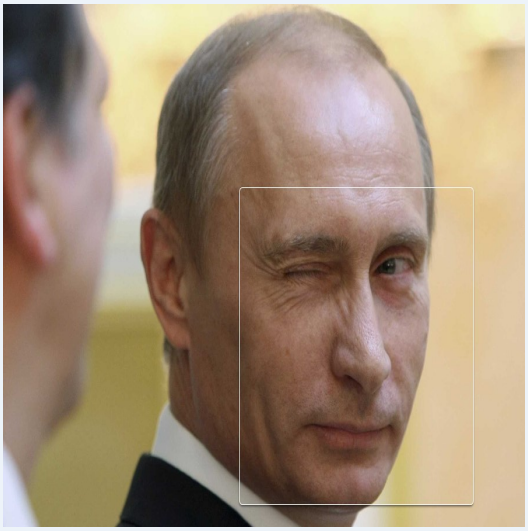


If you want more information about how to use Outlook or other Microsoft Office products, I would suggest you search on YouTube. **HERE** is a link for Outlook 2010 on YouTube. You can also learn more about other Office products for free at **Cybrary**. The site is free but will require you to register. Once you do, click on "Courses" and you can search for LOTS of different types of computer training.

Russia / Bernie

Russia is planning to interfere in 2020 presidential election

(by **Shannon Vavra and Sean Lyngaas | Feb 20, 2020**)



Russia is working to interfere in the 2020 presidential election, and appears to have a preference for President Donald Trump's candidacy, according to a briefing delivered to the House Intelligence Committee last week.

According to a report in the The New York Times, the briefing detailed evidence that Moscow is trying to duplicate its interference efforts from the 2016 presidential elections. A person familiar with the briefing told CyberScoop that, according to the briefing, Russia has a preference for Trump's candidacy and would continue to use messaging aimed at sowing discord among supporters of Democratic presidential candidates.

The briefing, delivered by the Office of the Director of National Intelligence's election security lead Shelby Pierson, reportedly upset Trump because he suspected Democratic committee members would use the information against him, according to the Times, and The Washington Post. Trump mistakenly thought that the information was supplied exclusively to Rep. Adam Schiff, D-Calif., despite the fact that multiple committee members from both parties were briefed.

Trump was so infuriated by the briefing that he lashed out at acting Director of National Intelligence Joseph Maguire, eventually removing him from his position. Earlier this week, Trump appointed Richard Grenell, the current U.S. Ambassador to Germany, to occupy the position until he nominates a permanent replacement, according to the Post.

Click **HERE** to read the article.

Sanders informed that Russia is trying to help his Campaign

(by **Shannon Vavra | Feb 21, 2020**)

U.S. officials have informed Sen. Bernie Sanders, I-VT., that Russia is trying to boost his presidential campaign as part of a broader effort to interfere in the 2020 presidential elections and the crowded Democratic field.

Sanders confirmed the news Friday, telling reporters in Nevada he had learned about Russia interference in his campaign approximately one month ago.

The news comes just a day after it was reported that Russia has a preference for President Donald Trump's candidacy in the 2020 presidential election, according to a U.S. intelligence community briefing delivered last week to the House Intelligence Committee. A person familiar with that briefing told CyberScoop that alongside Russia's preference for Trump's campaign, Russia will use messaging intended to spread discord among supporters of Demographic presidential candidates.

The alleged support for both Trump and Sanders could mean a repeat of Russian's actions in 2016. Russia operatives sought to boost both Trump and Sanders in the 2016 election, according to an indictment from Special Counsel Robert Mueller's investigation into Russian interference.

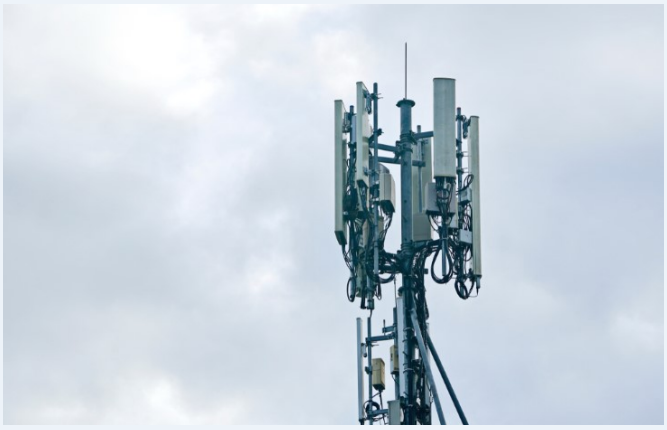
It was not clear whether the information provided to the Sanders Campaign came from the intelligence community. The office of the Director of National Intelligence declined to comment. The FBI did not immediately return request for comment.

Click **HERE** to read the article.

4G Mobile Network / Iran

Newly Discovered IMP4GT Attack Identified Targeting 4G Mobile Networks

(by **Cyware News** | **Feb. 27, 2020**)



A group of researchers from Ruhr-Universitat Bochum has demonstrated a new type of attack on 4G networks that can allow attackers to perform activities as a user. The flaw exists in the 4G mobile communication standard and exploits a security vulnerability in LTE.

What is affected? According to researchers, the attack termed as IMP4GT attack impacts all devices that communicate with LTE. This includes smartphones, tablets, and some loT devices.

How does the attack happen? There are two variants of the attack. They can be conducted in uplink and downlink direction.

With the uplink impersonation, the attacker impersonates a victim asking for TCP/IP connection from a network. Later, it uses arbitrary IP services to generate traffic and associates them with the victim's IP address.

The downlink impersonation allows an attacker to establish a TCP/IP connection to the phone that bypasses any firewall mechanism of the LTE network.

Bottom Line: The only way to mitigate the risk of exploitation is to change the hardware. The Bochum-based team is attempting to close the security gap in the latest mobile communication standard 5G, which is currently rolled out.

Click **HERE** to read more.

Multinational Attack Campaign By Iranian APT Group Targets Government Organizations

(by **Cyware News** | **Feb. 27, 2020**)

A new credential-stealing malware dubbed Forelord was found targeting potential victims via spear-phishing emails. Meanwhile, the researchers have attributed the campaign to a known Iranian advanced persistent threat (APT) group.

What happened? The phishing email scam was reportedly observed between mid-2019 and mid-January 2020.

The email campaign targeted organizations in Turkey, Jordan, Iraq, as well as global government organizations and some unknown entities in Georgia and Azerbaijan.

The malware is named ForeLord because once the malware connects to the C2 servers, it receives a string of code that says "lordlordlordlord."

How does it work? In this campaign, researchers observed multiple emails using malicious attachments to gain initial access. Whereas, Cobalt Ulster is known for using a government agency, university or intelligence organization-related theme as a hook. The recent campaign used a more generic style, as per researchers.

Victims are asked to open a ZIP archive containing a malicious Excel file. Then an open request is made to enable-view the document. Once enabled, the malware disables the security controls and the malicious code runs in the victims' system. ForeLord drops several tools used to collect critical information and credentials. It further tests those credentials on the network and creates a reverse SSL tunnel to provide an additional access channel for the hacked network.

Click **HERE** to read more.

Chinese Hackers / 2FA

Accused Chinese hackers abandon techniques after U.S. indictments

(by **CyberScoop (|Feb 26, 2020)**

U.S indictments against individual Chinese soldiers accused of hacking various American targets have deterred those military personnel from conducting the same kinds of hacks again, according to the co-founder of a firm known for investigating nation-state activity.

Digital infrastructure associated with alleged hackers charged in 2014, 2017 and 2018 essentially evaporated when charges in each case were made public, said Dmitri Alperovitch, who co-founded CrowdStrike, during a keynote speech Wednesday during the RSA security conference in San Francisco. Each of the groups known as APT1, APT3, or Buyosec and APT 10, respectively has been associated with Chinese intelligence services or the People's liberation Army.

"Everything associated with them disappeared," Alperovitch said during a conversation with reporters after the presentation. He cautioned that, while other Chinese groups largely have remained active, the specific groups named in the indictments "vanished" in a way that was "remarkable." Some of the alleged hackers may have been re-assigned to other units that had not been publicly identified, and thus continued launching attacks on Beijing's behalf, Alperovitch suggested.

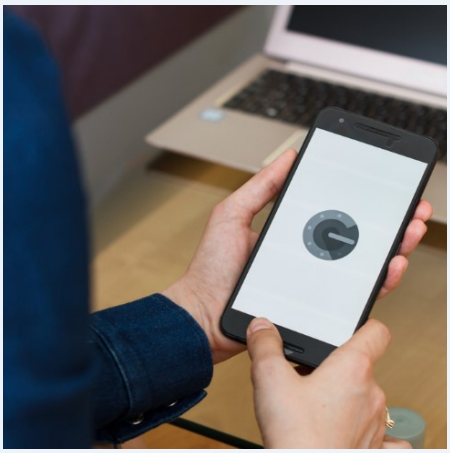
At the very minimum, he said, attackers had to "reset and re-tool." Even that would differentiate Chinese hackers from their counterparts in Russia and Iran, who tend to "ignore the indictments and move on," he said. Exactly why China changes its tactics, while other state-sponsored hackers continue without interruption, remains unclear.

Click **HERE** to read more.

New Malware strain Steals Google Authenticator 2FA Codes From Under Your Nose

(by **Cyware News | Feb. 28, 2020**)

Security experts discovered a new Android malware variant that can extract and steal one-time passcodes (OTP) generated through Google Authenticator.



What happened? A team of researchers claimed to have spotted an authenticator OTP-stealing capability in Cerberus, a relatively new Android banking Trojan launched last year.

As per reports, current versions of the Cerberus banking Trojan possess several advanced capabilities. It abuses the accessibility privileges to steal 2FA codes. When the Authenticator app is opened, it can leak the interface content and can send it to the attacker's controlled server.

How does Authenticator work? Google launched the Authenticator mobile app in 2010 as an alternative to SMS-based one-time passcodes.

The app generates six to eight digits long unique codes that users must enter in login forms while attempting to access online accounts. Since Google Authenticator codes are generated on smartphones, online accounts of the users with 2FA layers are considered more secure than those protected by SMS-based codes.

This new feature for stealing 2FA codes is not yet live in the Cerberus version currently being advertised and sold on hacking forums. "We believe that this variant of Cerberus is still in the test phase but might be released soon," researchers presume.

Click **HERE** to read more.

Self Driving Cars / Google

Ethical hackers submitted more bugs to the Pentagon than ever last year

(by **Shannon Vavra** | **March 2, 2020**)

Outside security researchers alerted the Pentagon about more software vulnerabilities in its networks than ever before, according to statistics released by a Department of Defense unit focused on cyber operations.

The Defense Department's Cyber Crime Center(DC3) on Friday released its annual numbers from the Vulnerability Disclosure Program (VDP). In which the Pentagon asks ethical hackers, known as "white hats," to probe it's networks for weaknesses, then tell the government what they found. In all, the VDP processed 4,013 vulnerability reports, 2,836 of which led to mitigation activities, the DC3's Executive Director, Jeffrey Specht, said in the report. Eight percent of the submitted reports were critical or high severity, according to a statement.

"It was our busiest year to date with a staggering 21.7% increase of submitted reports from 2017," the DOD Cyber Crime center (DC3) report says.

The department has been working to uncover vulnerabilities with the help of white hat hackers for years. In 2016, the department launched "hack the Pentagon" a program that rewarded white hat hackers who initially uncovered nearly 140 vulnerabilities in five public websites, for a payout of nearly $150,000. The Defense Department's willingness to adopt bug bounties in 2016, then an emerging concept, has been credited with moving this kind of security testing into the mainstream.

Click **HERE** to read more.

DoppelPaymer Ransomware Used to Steal Data from Supplier to SpaceX, Tesla

(by **Elizabeth Montalbano** | **March 3, 2020**)

A company that provides custom parts to aerospace giants Lockheed Martin, SpaceX and Boeing, has been the target of an attack by an emerging type of ransomware that can both encrypt files and exfiltrate data.

Colorado-based Visser Precision said it was targeted by a cyber incident that involved the attacker accessing and stealing company data after a security researcher found some of the company's stolen files leaked online.

Brett Callow, a threat analyst at anti-malware security from Emsisoft, discovered the documents– a series of nondisclosure agreements Visser has with companies including SpaceX, Tesla, Honeywell, General Dynamics and others– on a hacker website and began alerting news outlets, according to published reports in Forbes and TechCrunch.

"The evolution of ransomware from simply keeping data unusable, to that plus threatening to release it, is insidious in its premise," Mike Jordan, vice president of research, shared assessments, said in an email to Threatpost. "Deciding whether to pay a ransomware extortionist always involves a financial calculus where you determine whether paying is cheaper than recovering the data on your own."

Click **HERE** to read more.

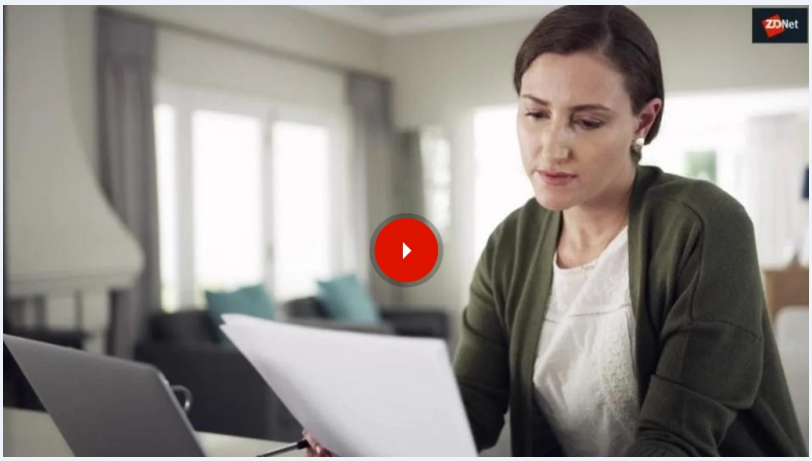
More News

Working from home? Switch off Amazon's Alexa (say lawyers)

(By **Chris Matyszczyk** | **March 24, 2020)**

Those not used to working from home must be going through several stages of spiritual discomfort.

Yes, ZDNet's more experienced hands can help you acclimatize to the new working style, now that the COVID-19 pandemic has disrupted modern working life..



Yet some professionals may not be so able to deal with life sans their office perks. Lawyers, for example.

Many are used to sitting in their enclosed chambers, closing their doors and holding vital conversations about lawyerly matters. There, they feel secure.

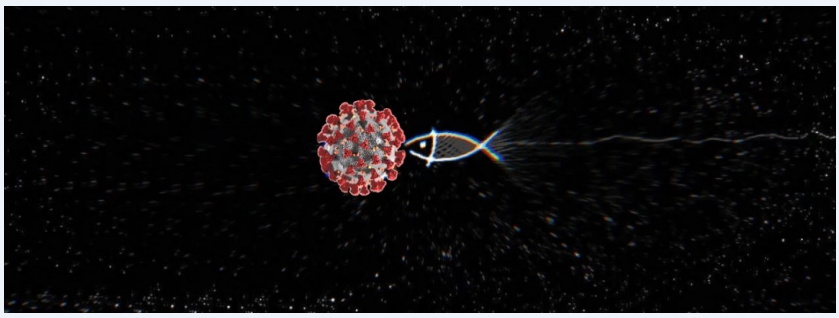
Working in their homes, they worry who may be spying on them. Alexa, for example, and her band of vastly intelligent speakerpersons.

Bloomberg reports that famed UK law firm Mishcon de Reya -- motto: "It's Business. But It's Personal." (seriously) -- is telling its fine employees to mute or even totally disable domestic smart speakers for confidential business calls.

Click **HERE** to read more.

Phishing Attack Says You're Exposed to Coronavirus, Spreads Malware

(By **Lawrence Abrans** | **March 29, 2020)**



A new phishing campaign has been spotted that pretends to be from a local hospital telling the recipient that they have been exposed to the Coronavirus and that they need to be tested.

With the Coronavirus pandemic affecting all corners of the world, we continue to see phishing actors try to take advantage of the fear and anxiety it is provoking to scare people into opening malicious email attachments.

In a new low, a threat actor is pretending to be from a local hospital telling the recipient that they have been in contact with a colleague, friend, or family member who has tested positive for the COVID-19 virus.

```
Dear XXX

You recently came into contact with a colleague/friend/family member who has COVID-19 at
Taber AB, please print attached form that has your information prefilled and proceed to
the nearest emergency clinic.

Maria xxx
The Ottawa Hospital General Campus
501 Smyth Rd, Ottawa, ON K1H 8L6, Canada
```

Click **HERE** to read more.

More News

NHS Outplays Ransomware; Six Attacks Record since Massive Wannacry Infection

https://cyware.com/news/nhs-outplays-ransomware-six-attacks-recorded-since-massive-wannacry-infection-b1c4a103

The UK Enacts Law to Fortify Security Posture of loT Devices in the Country

https://cyware.com/news/the-uk-enacts-law-to-fortify-security-posture-of-iot-devices-in-the-country-651d2213

Researcher Finds Over 60 Vulnerabilities in Physical Security Systems

https://www.securityweek.com/researcher-finds-over-60-vulnerabilities-physical-security-systems

Ashley Madison cyber-breach: 5 years later, users are being targeted with 'sextortion' scams

https://www.cnbc.com/2020/01/31/ashley-madison-breach-from-2015-being-used-in-sextortion-scams.html

NSA Releases Guidelines to Improve Cloud Security

https://cyware.com/news/nsa-releases-guidelines-to-improve-cloud-security-d252da0d

New Report Shows Employee at Large Organization Send Over 130 Emails Every Week to the Wrong Person

https://cyware.com/news/new-report-shows-employees-at-large-organization-send-over-130-emails-every-week-to-the-wrong-person-65759a59

Weaponized Data Breaches: Fueling a Global Cyber Cold War

https://www.infosecurity-magazine.com/opinions/weaponized-data-breaches-war

Iranian Hackers Target U.S. Reserch Organization in Ongoing Campaign

https://www.securityweek.com/iranian-hackers-target-us-research-organization-ongoing-campaign

FBI investigating Israeli spyware vendor involvement in possible hacks: report

https://thehill.com/policy/technology/technology/480825-sources-say-fbi-investigating-israeli-spyware-vendor-involvement

Please don't fall for these surprisingly badly written phishing scam emails

https://www.zdnet.com/article/please-dont-fall-for-these-surprisingly-bad-phishing-scam-emails/

Microsoft Azure Flaws Could Have Let Hackers Take Over Cloud Servers

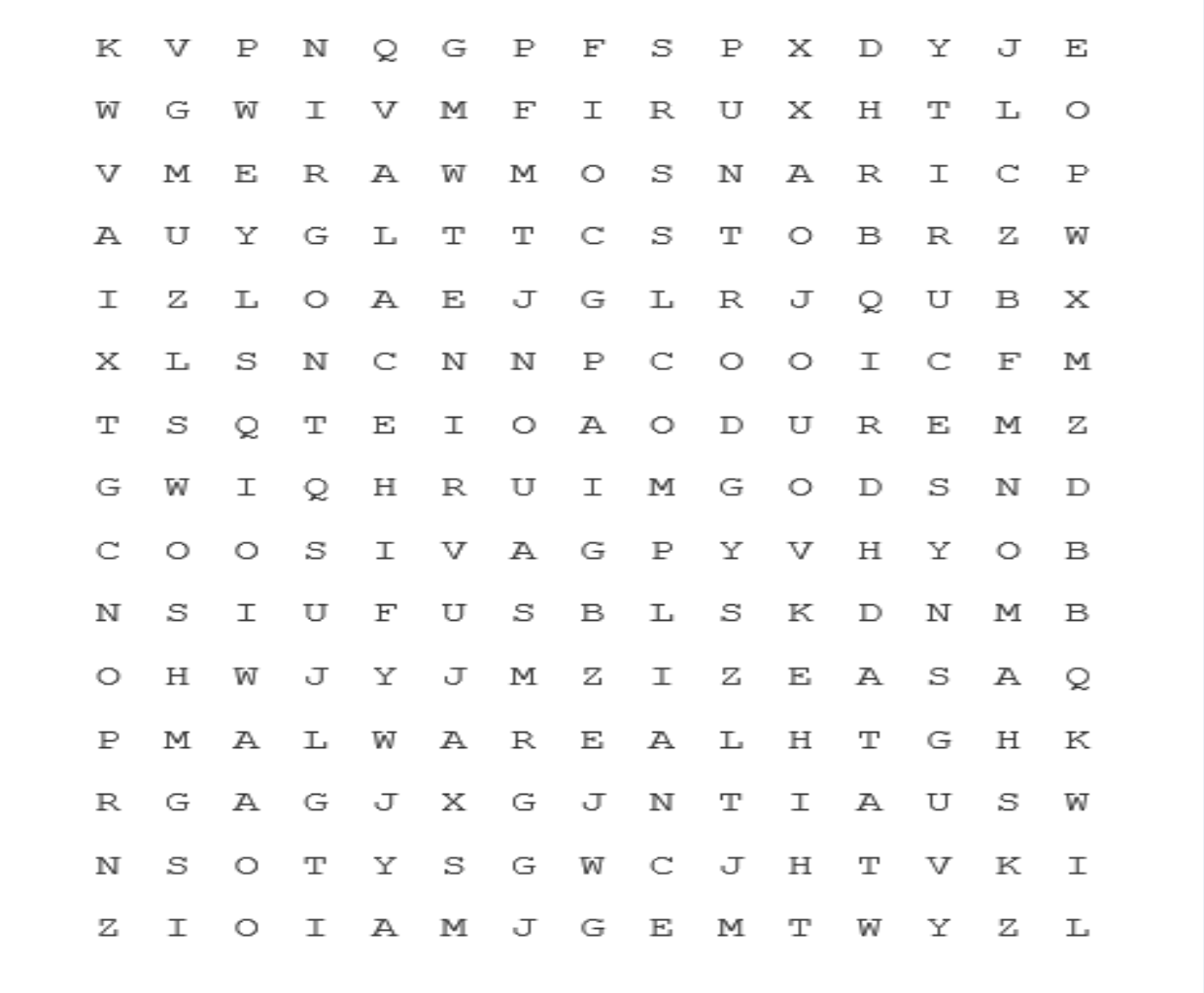
https://thehackernews.com/2020/01/microsoft-azure-vulnerabilities.html

Cyber Challenge

Word Search

Definitions of Cyber

We've decided to add something new to the Newsletter. We created a word search covering important terms of Cyber Security. Good luck and remember you can always email us for hints if you need them. Please use a drawing utensil and email us (GRP_Cyber_Ops@dps.texas.gov) a screenshot of the completed version! From this month forward, we will keep a count of members completing the challenges and display the winner on the next months Newsletter!



BOTS	CLOUD	COMPLIANCE
DATA	ESPIONAGE	LOSS
MALWARE	PHISHING	PROTECTION
RANSOMWARE	SECURITY	VULNERABILITY

Cyber Challenge

This Month's Challenges

As for this month's challenges, I decided to make two challenge questions. We will begin with an easy question. After that, I provided a link that will quiz your knowledge on cyber crypto. Good luck & remember you can always email me (Patrick.Thomas2@dps.texas.gov) for hints if you need help. Please email me your answers after figuring out the challenges and I will add you to next months Newsletter!

First Challenge:

I've done research into what the five most common ways to be hacked are, what are the top five most common ways to be hacked? (5 Answers)

Second Challenge

The final challenge is a Polybius challenge that is much more difficult than the previous one I have provided. Please refer to the link to figure out the final question below. Final Question

What is the **1st** word in the secret code?

For security reasons convert your **answer into a number** using this Polybius square:

	1	2	3	4	5	6
1:	A	B	C	D	E	F
2:	G	H	I	J	K	L
3:	M	N	O	P	Q	R
4:	S	T	U	V	W	X
5:	Y	Z	1	2	3	4
6:	5	6	7	8	9	0

For Example:

hi = 2223

bye = 125115

23 = 5455

GOOD LUCK with the challenges.

</Closing Comments>

We realize your time is valuable, but education should never end and being aware of cyber issues/dangers are key to protecting not only yourself but the agency. We hope you have enjoyed reading this newsletter and it has given you things to think about.

To close this month's newsletter I want to provide (10) practices for cybersecurity.

1. Clicking without Thinking Is Reckless
2. Stick to your own devices
3. Be aware of your surroundings
4. Keep track of your digital footprint
5. Keep up with Updates
6. Connect Securely
7. Secure Your Mobile Device
8. Beware Social Engineering
9. Back Up Your Data
10. You're not immune

The link to an explanation of what these practices mean can be found HERE.

As we close out this newsletter, I want to thank our readers and let me know if you would like anything to be added for an upcoming edition. Feel free to email me at GRP_Cyber_Ops@dps.texas.gov or call at (512) 424-2329. Our team needs to keep all of DPS up to date with the latest cyber-security trends. Continuing our knowledge with the latest technologies is an important way to reduce risk and potential breaches to not only DPS but also your personal lives. Thank you for reading this edition of the newsletter. Please let me know if you enjoyed the word search. I may continue to use this periodically to keep our readers engaged with cyber terminology.

We hope you enjoyed the newsletter. Please pass it on to others you know so we can spread the knowledge. The better educated everyone is on cyber issues the safer everyone is. You can see previous issues of the newsletter at this public facing TXDPS website:

http://www.dps.texas.gov/InformationTechnology/Cyber/index.htm

Good luck with the Cyber Challenges. Again, If you have suggestions on how the newsletter could be improved, please let me know.

Best,

David

And as always, **THANK YOU FOR YOUR CYBER VIGILANCE.**