Cyber Security NEWS
Vol. 5 | Issue 1
January 2020

TXDPS Cyber Security Newsletter

TXDPS Cyber Security welcomes you to this month's TXDPS Cybersecurity Newsletter. In this publication we have provided information you will find relevant and useful. We encourage you to forward this newsletter to everyone you know to spread the cyber education.

To start the newsletter I 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 a computer to complete a cybersecurity awareness training program every year.

The DPS policy required all employees and contractors complete security awareness training every two years, but with the change in the law, everyone will now have to complete it yearly. What this means is in order to comply with the new law, starting this month we will be resetting everyone's SANS security awareness training account. So expect between now and June to receive an email notification your training account has been reset and you must complete security awareness training. Per DPS policy, you have 30 days to complete the training. If you do not complete it during that time, you will receive a reminder followed by email notifications to supervisor and then division chiefs if training is not completed by the 35th and 40th days, respectively. If you have questions, you can email me directly at kirk.burns@dps.texas.gov and I will be happy to answer them for you.

The next thing I want to talk about are some great tips I came across recently for travelers. The 11 tips, along with a link to the article, are listed below. People are often oblivious to the cyber dangers they encounter while traveling, and these tips might keep you from being compromised or having your identity stolen. The advice is relevant for daily use, but even more so if you are traveling.

- Reset all of your frequently used passwords
- Be cautious of travel websites
- Don't use public charging stations
- Be aware of shoulder surfing
- Avoid public Wi-Fi hotspots
- Keep your devices close to you and keep an eye out for stolen devices
- Avoid social media and out-of-office messages before your trip
- Back up files before you go
- Ensure your software is up to date
- Disable Bluetooth connectivity
- If traveling abroad, know your rights and the local laws.

While I do not agree with the reasoning behind all of the tips, they are good to consider when traveling. A more detailed explanation of the tips can be found HERE.

ToTok / Phishing

Popular messaging app is reportedly a United Arab Emirates spying tool

(by **Brendan Morrow** | **December 23, 2019**)

A popular chat app called ToTok is actually a spying tool used by the United Arab Emirates government, *The New York Times* reports.

ToTok is described as being a secure messaging app and has been downloaded millions of times on the Google and Apple stores, and it was even recently among the most popular social apps in the United States, although most users are located in the Emirates, the *Times* says. But it's reportedly "used by the government of the United Arab Emirates to try to track every conversation, momement, relationship, appointment, sound, and image of those who install it on their phones."

The firm behind the app, the *Times* reports, is "most likely a front company" associated with a cyberintelligence and hacking firm that's under FBI investigation. U.S. officials have reportedly informed some allies about the app.

"Instead of paying hackers to gain access to a target's phone...ToTok gave the Emirati government a way to persuade millions of users to hand over their most personal information for free," the *Times* writes.

Click **HERE** to read the article.

How do phishing techniques work? Researchers shine a light on some clever phishing techniques

(by **Cyware** | **December 12, 2019**)

- By using traffic generators, phishers ensure that the redirector page is the top search result for certain keywords or for very specific terms so as to guide users to the actual phishing page.
- User can easily avoid disasters by closely inspecting the page's URL to avoid common phishing pages.

The year 2019 saw a rise in phishing activity reaching new levels of creativity and sophistication. According to Microsoft, phishing attempts grew from under 0.2 percent of all emails analyzed worldwide in January 2018, to around 0.6 percent in October 2019.

Meanwhile, the Redmond-based tech giant also noted that the number of ransomware, crypto-mining, and other malware infections has gone down from the previous records. The company has published a blog where it reviewed three of the more clever phishing attacks it observed and traced this year.

Hijacking search results

- Phishers manipulate legitimate URLs through harmless-looking redirectors to compromise websites, which leads to phishing.
- They also move hijacked web traffic to websites they control.
- By using traffic generators, phishers ensure that the redirector page is the top search result for certain keywords or for very specific terms.
- Phishers would then send emails to victims linking the Google search result for the specific term.

Click **HERE** to read the article.

VegaLocker / Tesla

New VegaLocker ransomware variant targets healthcare and IT sectors

(by **Cyware** | **December 12, 2019**)

- It was being used in targeted attacks against healthcare and other tech companies in U.S., Canada, and Europe.
- The threat actors are believed to have dropped the ransomware through Remote Desktop servers that are publicly exposed to the Internet.

Cybercriminals have developed a new ransomware variant called Zeppelin. It is being used to target healthcare and Tech companies in U.S., Canada, and Europe. The ransomware is reportedly a new variant of the VegaLocker/Buran Ransomware.

Backstory of the ransomware family

Beginning its journey as VegaLocker, the ransomware evolved into a Ransomware-as-a-Service (RaaS) on Russian hacker forums under the name Buran in May 2019. Affiliates who joined the RaaS would earn 75 percent of the ransom payment, while the Buran operators would earn 25 percent. The latest variant of this ransomware family is now Zeppelin.

Click **HERE** to read more.

3 crashes, 3 deaths raise questions about Tesla's Autopilot

(by **Tom Krisher** | **January 3, 2020**)

Three crashes involving Teslas that killed three people have increased scrutiny of the company's Autopilot driving system just months before CEO Elon Musk has planned to put fully self-driving cars on the streets.

On Sunday, a Tesla Model S sedan left a freeway in Gardena, California, at a high speed, ran a red light and struck a Honda Civic, killing two peope inside, people said.

On the same day, a Tesla Model 3 hit a parked firetruck on an Indiana freeway, killing a passenger in the Tesla.

And on Dec. 7, yet another Model 3 struck a police cruiser on a Connecticut highway, though no one was hurt.

The special crash investigation unit of the National Highway Traffic Safety Administration is looking into the California crash. The agency hasn't decided whether its special-crash unit will review the crash that occurred Sunday near Terre Haute, Indiana. In both cases, authorities have yet to determine whether Tesla's Autopilot system was being used.

NHTSA also is investigating the Connecticut crash, in which the driver told police that the car was operating on Autopilot, a Tesla system designed to keep a car in its lane and a safe distance from other vehicles. Autopilot also can change lanes on its own.

Tesla has said repeatedly that its Autopilot system is designed only to assist drivers, who must still pay attention and be ready to intervene at all times. The company contends that Teslas with Autopilot are safer than vehicles without it, but cautions that the system does not prevent all crashes.

Even so, experts and safety advocates say a string of Tesla crashes raises serious questions about whether drivers have become too reliant on Tesla's technology and whether the company does enough to ensure that drivers keep paying attention. Some critics have said it's past time for NHTSA to stop investigating and to take action, such as forcing Tesla to make sure drivers pay attention when the system is being used.

Click **HERE** to read more.

WhatsApp / Apple Watch

Police Tracked a Terror Suspect—Until His Phone Went Dark After a Facebook Warning

(by **Morningstar (Provided by Dow Jones)** | **Jan 2, 2020)**

A team of European law-enforcement officials was hot on the trail of a potential terror plot in October, fearing an attack during Christmas season, when their keyhole into a suspect's phone went dark.

WhatsApp, Facebook Inc.'s popular messaging tool, had just notified about 1,400 users - among them the suspected terrorist - that their phones had been hacked by an "advanced cyber actor." An elite surveillance team was using spyware from NSO Group, an Israeli company, to track the suspect, according to a law-enforcement official overseeing the investigation.

A judge in the Western European country had authorized investigators to deploy all means available to get into the suspect's phone, for which the team used its government's existing contract with NSO. The country's use of NSO's spyware wasn't known to Facebook. NSO licenses its spyware to government clients, who use it to hack targets.

On Oct. 29, Facebook filed suit against NSO - which has been enmeshed in controversy after governments used its technology to spy on dissidents - in federal court in California, seeking unspecified financial penalties over NSO's alleged hacking of WhatsApp software. It also sought an injection prohibiting NSO from accessing Facebook and WhatsApp's computer systems.

NSO said it is vigorously defending itself against the lawsuit, without elaborating.

Technology companies such as Facebook and Apple Inc. over recent years have strengthened the security of their systems to the point where even the tech companies themselves can't provide law-enforcement agencies with messages created on their own systems.

Click **HERE** to read more.

He told police he was stabbed for being Jewish. Then his Apple Watch caught him in a lie.

(by **Bisma Parvez** | **2:25 p.m. ET Jan. 2, 2020**)

A 26-year-old man faked his own stabbing at the West Bloomfield synagogue where he worked and then reported he was attacked because of his Jewish faith, authorities say.

Now Sean Samitt is facing a felony charge of filing a false police report, according to West Bloomfield Police.

Police said Samitt's Apple Watch helped them solve the case.

Samitt was arrested on Dec. 20 and arraigned the same day before Magistrate Julie Nelson-Klein at the 48th District Court in Oakland Country on one count of falsely reporting a felony, a crime punishable up to four years. According to authorities, his $7,500 bond was posted by Samitt's mother.

On Thursday, he appeared at the 48th District Court for a probable cause hearing. He is expected to appear for the preliminary examination on Jan. 14.

Samitt reported he was attacked and stabbed in the abdomen by an unknown man in the parking lot at the Temple Kol Ami, where he worked as a cantorial soloist, which is a music director.

He reported the crime on Dec. 15, telling police that he was confronted about 7 p.m. as he was leaving work by a white male in his late 30's to early 40's.

Sammitt said that the alleged attacker shouted, "You Jews!" and said "too many immigrants are here," according to the police report obtained by the Free Press through a Freedom of Information Act request.

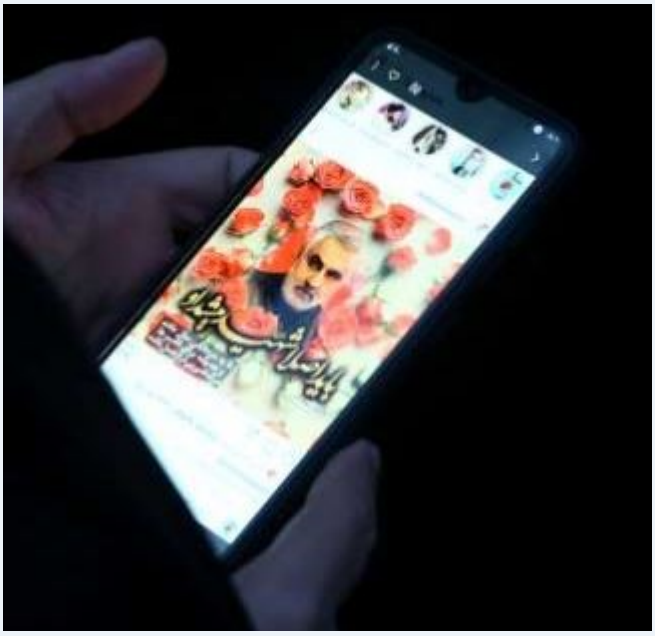
Samitt told officers that he was punched in the chest and abdomen during the encounter and he feared for his life, the report said. He said he escaped by kneeing the attacker in the groin and pushing him away, then drove himself to Henry Ford Hospital where a security staff called local authorities about the attack.

Click **HERE** to read more.

Iran / Apple

U.S. Officials Brace for Cyber-Attack Retaliation From Iran

(by **Alyza Sebenius** and **William Turton** | **4 Jan 2020**)



Iranian officials are likely considering a cyber-attack against the U.S. in the wake of an airstrike that killed one of its top military officials.

Former U.S. officials and security experts said there is precedent for such concerns amid years of tit-for-tat cyber-attacks between the two countries. As recently as June, after the U.S. sent additional troops to the Middle East and announced further sanctions on Iran, cyber-attacks targeting U.S. industries and government agencies increased, the Department of Homeland Security said at the time.

In a tweet after the airstrike on Thursday, Christopher Krebs, director of the U.S. Cybersecurity and Infrastructure Security Agency, repeated a warning from the summer about Iranian malicious cyber-attacks, and urged the public to brush up on Iranian tactics and to pay attention to critical systems, particularly industrial control infrastructure.

The airstrike in Baghdad killed Qassem Soleimani, a major general in the Iranian Islamic Revolutionary Guard, who led proxy militias that extended the country's power across the Middle East. The strike ordered by U.S. President Donald Trump was in response to "an imminent threat," according to Secretary of State Michael Pompeo.

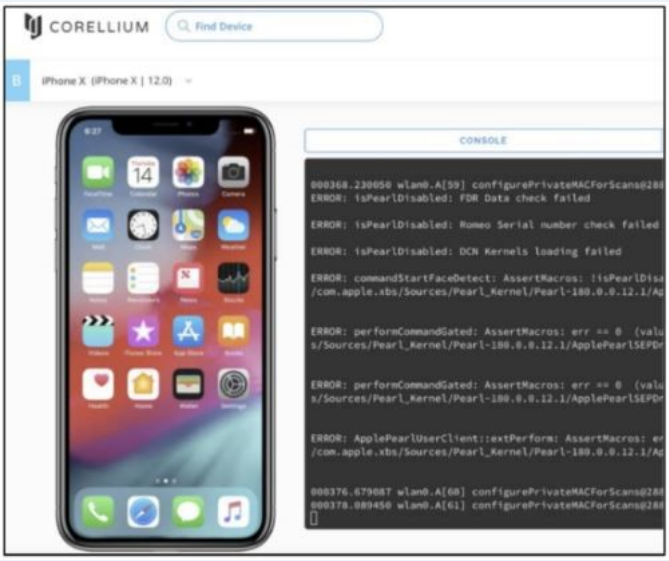
By midday, shares of cybersecurity companies were mostly up, even as the broader market was down amid uncertainty created by the airstrike. Just before 1 p.m. eastern time, shares of CrowdStrike Inc. were up 3.7% and FireEye Inc., 2.7%.

Click **HERE** to read more.

Apple targets jailbreaking in lawsuit against iOS virtualization company

(by **Jon Brodkin** | **1/3/2020, 2:30 PM**)

Apple has expanded a lawsuit against an iOS virtualization company, claiming that its actions facilitate jailbreaking and violate the Digital Millennium Copyright Act (DMCA) prohibition on circumvention of copyright-protection systems.



Apple sued Corellium, a company that sells access to virtual machines that run copies of the operating system used in iPhones and iPads, in August 2019. We detailed the initial allegations in a previous article; Apple said that Corelliium sells "perfect replicas" of iOS without a license from Apple and markets its software as "a research tool for those trying to discover security vulnerabilities and other flaws in Apple's software." But instead of aiding good-faith security research, Corellium " encourages its users to sell any discovered information on the open market to the highest bidder," Apple alleged.

The first version of Apple's lawsuit accused Corellium of copyright infringement. A new version filed on December 27 alleges both copyright infringement and "unlawful trafficking of a product used to circumvent security measures in violation of 17 U.S.C. § 1201," a statute that's part of the DMCA. Apple argued that Corellium gives users the ability to jailbreak iOS for either benign or malicious purposes.

Click **HERE** to read more.

More News

Microsoft, Dropbox and LinkedIn are the biggest targets for phishing attacks

https://www.businessinsider.in/tech/news/microsoft-dropbox-and-linkedin-are-the-biggest-targets-for-phishing-attacks/articleshow/72492998.cms

Maze Ransomware Demands $6 Million Ransom From Southwire

https://www.bleepingcomputer.com/news/security/maze-ransomware-demands-6-million-ransom-from-southwire/

Cybersecurity: This password-stealing hacking campaign is targeting governments around the world

https://www.zdnet.com/article/cybersecurity-this-password-stealing-hacking-campaign-is-targeting-governments-around-the-world/

Cyberattack Impacts MTSA Facility Operations

https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf

Landry's Restaurant Chain Discloses Payment Security Incident

https://www.darkreading.com/landrys-restaurant-chain-discloses-payment-security-incident/d/d-id/1336708

Wyze Labs data breach exposes 2.4 million, includes PHI

https://www.scmagazine.com/home/security-news/data-breach/wyze-labs-data-breach-exposes-2-4-million-includes-phi/

Army Follows Pentagon Guidance, Bans Chinese-Owned TikTok App

https://www.military.com/daily-news/2019/12/30/army-follows-pentagon-guidance-bans-chinese-owned-tiktok-app.html

Microsoft seizes 50 websites used by North Korean hackers to gather intelligence

https://www.cyberscoop.com/microsoft-north-korea-lawsuit-website-seizing/

RavnAir Group update on cyber-attack - update for 12/28/19

https://www.flyravn.com/ravn-news/ravnair-group-update-on-cyber-attack-update-for-12-28-19/

New Orleans Ransomware Attack Update: City to Raise Cyber Insurance to $10M

https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/new-orleans-cyber-insurance-plan/

Senator Wyden Asks Avast Antivirus Why It Sells Users' Browsing Data

https://www.vice.com/en_us/article/v744v9/senator-ron-wyden-asks-avast-selling-users-browsing-data

More News

Intel CPU flaw lets attackers manipulate voltage and leak secrets

https://cyware.com/news/intel-cpu-flaw-lets-attackers-manipulate-voltage-and-leak-secrets-6a839991

Hackers allegedly emptied brokerage accounts with a simple email scam - here's how to protect yourself

https://www.cnbc.com/2019/12/11/how-to-protect-your-brokerage-account-from-email-scams.html

Report: aviation industry playing catch up on cybersecurity

https://fcw.com/articles/2019/12/11/aviation-cyber-report-johnson.aspx

Connected Children's Toys aren't Cybersafe: Researchers Reports Several Serious Vulnerabilities

https://cyware.com/news/connected-childrens-toys-arent-cybersafe-researchers-reports-several-serious-vulnerabilities-6209841a

How Congress wants to help sync military cyber

https://www.defensenews.com/congress/2019/12/11/how-congress-wants-to-help-sync-military-cyber/

Vulnerabilities Spotted in Blink Home Security Cameras

https://cyware.com/news/vulnerabilities-spotted-in-blink-home-security-cameras-16383da0

Experian expects deepfake content to create geo-political confusion in 2020

https://securityboulevard.com/2019/12/experian-expects-deepfake-content-to-create-geo-political-confusion-in-2020/

Exclusive: Bitdefender Finds Security Hole in Wemo Smart Plug

https://in.pcmag.com/ifttt/134319/exclusive-bitdefender-finds-security-hole-in-wemo-smart-plug

Smart Krampus - 3PC Malware Targets iPhone Users

https://threatpost.com/krampus-3pc-malware-iphone-users/151043/

The little-known ways mobile device sensors can be exploited by cybercriminals

https://blog.malwarebytes.com/iot/2019/12/the-little-known-ways-mobile-device-sensors-can-be-exploited-by-cybercriminals/

U.S. government limits exports of artificial intelligence software

https://www.reuters.com/article/usa-artificial-intelligence/us-government-limits-exports-of-artificial-intelligence-software-idUSL1N2980M0

Reader Suggested Articles

Below are some articles suggested by readers that are informative and useful. Thank you to everyone who sent me these articles. I found them very interesting and hope readers will also.

From Deborah Wright:

Snatch ransomware reboots PCs in Windows Safe Mode to bypass antivirus apps

This ransomware is a newer strand which will reboot a computer to be able to bypass antivirus software and is capable of stealing files from the network and not just from the infected computer.

https://www.zdnet.com/article/snatch-ransomware-reboots-pcs-in-windows-safe-mode-to-bypass-antivirus-apps/

Phishing Attack Hijacks Office 365 Accounts Using OAuth Apps

This article talks about a unique way of compromising an email account.

https://www.bleepingcomputer.com/news/security/phishing-attack-hijacks-office-365-accounts-using-oauth-apps/

From Bernie Acre:

Ransomware attack teaches value of prevention to East Greenwich town government

Any cyber-attack is costly, but ransomware can be far more expensive. Most organizations are unwilling to fund preventative measures because of the lack of tangible metrics on prevention. However, organizations learn the hard way that the cost of preventative measures, no matter how much, are FAR cheaper than post-event.

https://securityboulevard.com/2019/12/ransomware-attack-teaches-value-of-prevention-to-east-greenwich-town-government/

From David Morgan:

Pentagon document lays out battle plan against zombies

Not that the Pentagon actually expects a zombie apocalypse, but they are ready if there is. :) The military has to plan for all types of things from natural disasters to catastrophic attacks. This is a fun way to exercise those principles.

https://www.cnn.com/2014/05/16/politics/pentagon-zombie-apocalypse/index.html

Cyber Challenge

Last Month's Challenge

Congratulations to everyone who was able to solve last month's challenges. The original version of the questions can be found in last month's newsletter. I have provided the actual question with the type of encoding I used and the answer below. The people listed below are those who contacted me with the answers. If you were unable to solve them I would strongly encourage you to look at the answers below and then look at last month's questions again and see if you can figure them out. You can find the answers to the challenges below.

	Completed 5 of 5 Challenges	
Deborah Wright @ 1429 on 10 Dec	Faye Krueger @ 1446 on 10 Dec	Kelly Patterson @ 1516 on 10 Dec
Steven Campbell @ 1517 on 10 Dec	Kimberly Avila @ 1603 on 10 Dec	Erich Neumann @ 1618 on 10 Dec
Rene Hess @ 1735 on 12 Dec	Devin Mathews @ 1029 on 12 Dec	Justin Wittington @ 1041 on 16 Dec
Jodie Tullos @ 1052 on 16 Dec	David Evans @ 0934 on 17 Dec	
	Completed 4 of 5 Challenges	
Stephanie Davidson @ 1155 on 11 Dec	Luis Zayas @ 0948 on 19 Dec	
	Completed 2 of 5 Challenges	
	Carl Weeks @ 1056 on 11 Dec	
	Completed 1 of 5 Challenges	
Kristen Poirier @ 1255 on 11 Dec	Roman Baca @ 1300 on 11 Dec	Haley Yaklin @ 1715 on 16 Dec

1. I am a specific type of network attack accomplished by sending a TCP packet to a device designed to turn on all flags. What is the name of this kind of attack? (encoded using Roman Numerals) **Christmas Tree or XMAS Attack**
2. I am a code injection technique used to attack data-driven applications. Statements are inserted into a field to exploit a security vulnerability in an application software. What am I? (encoded using ROT13) **SQL Injection**
3. I am a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. What am I? (encoded using HTML) **Honeypot**
4. I am a free and open-source packet analyzer. I am used for network troubleshooting, analysis, software and communications protocol development, and education. What am I? (encoded using morse code) **Wireshark**
5. I am a Linux distribution developed by Mati Aharoni and Devon Kearns designed for digital forensics and penetration testing. What am I? (encoded using Octal) **Kali Linux**

Cyber Challenge

This Month's Challenges

For this month's challenges I decided to use some different types of encoding for the challenges. Good luck and remember you can always email me for hints if you need them.

1. 49 20 61 6d 20 74 68 65 20 70 61 72 74 20 6f 66 20 74 68 65 20 6b 65 79 20 70 61 69 72 20 74 68 61 74 20 69 73 20 66 6f 75 6e 64 20 69 6e 20 61 20 62 72 6f 77 73 65 72 e2 80 99 73 20 74 72 75 73 74 65 64 20 72 6f 6f 74 20 43 41 2e 20 20 57 68 61 74 20 61 6d 20 49 3f

2. LXXIII XXXII XCVII CIX XXXII XCVII XXXII CIX CI XCVII CX CXV XXXII CXVI CXI XXXII XCVII XCIX XCIX CI CXV CXV XXXII XCVII XXXII XCIX CXI CIX CXII CXVII CXVI CI CXIV XXXII CXV CXXI CXV CXVI CI CIX XXXII CXI CXIV XXXII CI CX XCIX CXIV CXXI CXII CXVI CI C XXXII C XCVII CXVI XCVII XXXII CXVI CIV XCVII CXVI XXXII XCVIII CXXI CXII XCVII CXV CXV CI CXV XXXII CXVI CIV CI XXXII CXV CXXI CXV CXVI CI CIX CXV XXXII XCIX CXVII CXV CXVI CXI CIX XCVII CXIV CXXI XXXII CXV CI XCIX CXVII CXIV CV CXVI CXXI XXXII CIX CI XCIX CIV XCVII CX CV CXV CIX CXV XLVI XXXII XXXII LXXIII XXXII XCVII CIX XXXII CXI CII CXVI CI CX XXXII CXVII CXV CI C XXXII CXIX CIV CI CX XXXII XCVII XXXII CIV XCVII XCIX CVII CI CXIV XXXII XCIX CXI CIX CXII CXIV CXI CIX CV CXV CI CXV XXXII XCVII XXXII CXV CXXI CXV CXVI CI CIX XXXII CXV CXI XXXII CXVI CIV CI CXXI XXXII XCIX XCVII CX XXXII CI XCVII CXV CV CVIII CXXI XXXII CIII XCVII CV CX XXXII XCVII XCIX XCIX CI CXV CXV XXXII XCVII CIII XCVII CV CX XLVI XXXII XXXII LXXXVII CIV XCVII CXVI XXXII XCVII CIX XXXII LXXIII LXIII

3. 01001001 00100000 01100001 01101101 00100000 01110100 01101000 01100101 00100000 01110100 01101000 01101001 01110010 01100100 00100000 01110011 01110100 01100101 01110000 00100000 01101001 01101110 00100000 01110100 01101000 01100101 00100000 01001001 01101110 01100011 01101001 01100100 01100101 01101110 01110100 00100000 01010010 01100101 01110011 01110000 01101111 01101110 01110011 01100101 00100000 01010000 01110010 01101111 01100011 01100101 01110011 01110011 00101110 00100000 00100000 01010111 01101000 01100001 01110100 00100000 01100001 01101101 00100000 01001001 00111111

4. SG93IG1hbnkgc3RlcHMgYXJlIHRoZXJlIGluIHRoZSBSaXNrIE1hbmFnZW1lbnQgRnJhbWV3b3JrIGFuZCB3aGF0IGlzIHN0ZXAgdGhyZWU/

5. 123 143 141 155 155 145 162 163 040 155 141 171 040 162 145 147 151 163 164 145 162 040 141 040 167 145 142 040 141 144 144 162 145 163 163 040 164 150 141 164 040 154 157 157 153 163 040 154 151 153 145 040 151 164 040 142 145 154 157 156 147 163

</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 some best practices for cybersecurity.

- Check Emails for Signs of Phishing
- Be Cautious of Vishing Calls
- Know the Signs of SMShing
- Use a Strong Password
- Practice Social Media Safety
- Update Devices to Prevent Ransomware
- Practice Mobile Security
- Ensure the Devices in Your Home Are Secure
- Use Cloud Security to Protect Your Company's Data
- Be Aware of In-Person Social Engineering

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

In closing I want to let everyone know this will probably be the last newsletter I produce for DPS. I have been offered a job at a different state agency and will most likely take the position. The person who will be taking over the newsletter has been identified and you can expect to start to receive the newsletter from him next month. It is likely I will eventually startup a newsletter where I am going, so if you would like to be on that email list please let me know before the end of the month.

I have greatly enjoyed working here at DPS and producing this newsletter. I know I am leaving the agency in good hands and do not expect the quality of the newsletter to slip in my absence.

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. If you have suggestions on how the newsletter could be improved, please let me know.

Kirk

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