NEWS
Cyber Security
Vol. 4 | Issue 12
December 2019

Page 2 | Page 3 | Page 4 | Page 5 | News | Reader Suggestion | Challenge | Closing

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 begin this newsletter I want to take a minute and talk about physical security and why it is important to cybersecurity. Physical security is often a second thought when it comes to information security. When it is thought of it is typically only in reference to security of server rooms, network closets, and computers. These are very important but basic security of a building is just as important.

Most organizations invest lots of money to protect against unauthorized access to sensitive areas. While there are several methods to limit physical access to an area, card access systems and cameras are most commonly used. These devices work well, but not if people forget to practice basic security in the workplace and bypass the systems. It is easy to understand the need to restrict access to sensitive areas like server rooms and network closets. However, employees often ignore policy and procedure for access to a building or areas within a building. They never stop to question and verify a person's credentials or if they are authorized unescorted access to an area. How many times have you seen someone open a card access entry door for someone but never verify they have a badge authorizing them entry? How many times have you been the person holding the door but not verifying the person?

This happens for a variety of reasons. Sometimes it is because the employee believes they remember seeing a person in the area before, so they must be authorized. Maybe the person is delivering a package and their hands are full so they cannot badge in. Maybe the person is a new janitor who is having trouble getting in to clean the building. Maybe the person is an employee who forgot to bring their access badge to work that day. Or maybe the person holding the door is just trying to be helpful. Whatever the reason, these are security concerns and violations and endanger an organization. If policy and procedure say you have to badge into an area, then everyone needs to badge in at all times. Even if you believe the person is authorized to be in the area, how can you be sure if they do not have their access card? How do you know the person didn't have their access revoked to the area and they are trying to gain unauthorized access? The best policy is to have the person contact their supervisor and be escorted or have them go to the security office for a temporary badge.

There are numerous stories of malicious people trying to gain access to restricted areas. People believe these things only happen from spies and terrorists trying to gain access to restricted areas on military bases and government buildings. Every organization is at risk from unauthorized access. Uniforms are easy to obtain, and fake credentials are easy to create. It would be very easy for a malicious person to obtain a janitor, UPS, FedEx, or even police uniform and try to social engineer their way into a building or into a restricted area. Vigilance is the only protection an organization has.

For a more detailed explanation on why physical security is so important, I encourage you to read a paper by David Hutter published by the SANS Institute. The paper is Physical Security and Why It Is Important.

Cybersecurity 202 / RIPlace

The Cybersecurity 202: U.S. officials fret about hacking by a new generation of nations

(by **Joseph Marks | November 26**)

THE KEY

As if digital threats from the main U.S. cyberspace adversaries weren't enough, U.S. officials and researchers are increasingly worried about hacking dangers posed by a slew of other nations including Vietnam, Qatar, and the United Arab Emirates.

The fears are upending a half decade during which U.S. cybersecurity worries focused on four main adversaries - Russia, China, Iran and North Korea. And they're signaling that cyberspace is about to get far more complicated and dangerous.

"The threshold for entry to have a cyber program has dropped so low because you don't need to figure out how to build your own program. You can just buy it as a service and that worries me," a senior FBI cybersecurity official told reporters during a roundtable discussion.

In some cases the nations are developing hacking capabilities in-house, such as Vietnam, where government-backed hackers are reportedly stealing information from rival governments and companies in key sectors including the auto industry to gain a competitive advantage. In other cases, as with Qatar and the UAE, they're contracting with private companies that sell hacking tools and services to law enforcement, and using them to spy on journalists and dissidents.

The most obvious problem is that more nations hacking leads to more hacking victims - including in the United States.

Click **HERE** to read the article.

New ransomware technique evades most updated security protection and Windows 10

(by **Cyware | November 26, 2019**)

- The technique dubbed RIPlace, required only a few lines of code to elude inbuilt ransomware protection features.
- It is even effective against systems that are timely patched and run modern antivirus solutions.

Researchers of an end-point security solution firm recently stumbled upon a new technique that allows a ransomware to encrypt files on Windows systems without drawing the attention of existing anti-ransomware products.

The backstory

After discovering the technique, researchers from the firm got in touch with Microsoft, security vendors, law enforcement and regulatory authorities, and others.

- Nyotron told BleepingComputer that they tested RIPlace against over a dozen vendors including Microsoft, Symantec, Sophos, McAfee, Carbon Black, Kaspersky, Trend Micro, Cylance, SentinelOne, Crowdstrike, PANW Traps, and Malwarebytes.
- Only a handful of security vendors have acknowledged the issue, despite dozens being impacted.
- Only Kaspersky and Carbon Black modified their software to prevent this technique from the above-mentioned names.

Click **HERE** to read the article.

SDK / Bluetooth

Two third-party SDKs allowed secret harvesting of Twitter and Facebook user data

(by **Catalin Cimpanu** for **Zero Day | November 26, 2019 -12:44 GMT**)

Facebook and Twitter are investigating a report from security researchers about two third-party software development kits (SDKs) that allowed app makers to access and collect user data without authorization.

An SDK is a software library that app developers embed in their code to automate certain operations, and spare themselves from writing that specific code by hand and losing precious time.

SDKs are very popular in the modern app development ecosystem, but using an SDK also implies surrendering some of your app's control to a third-party entity.

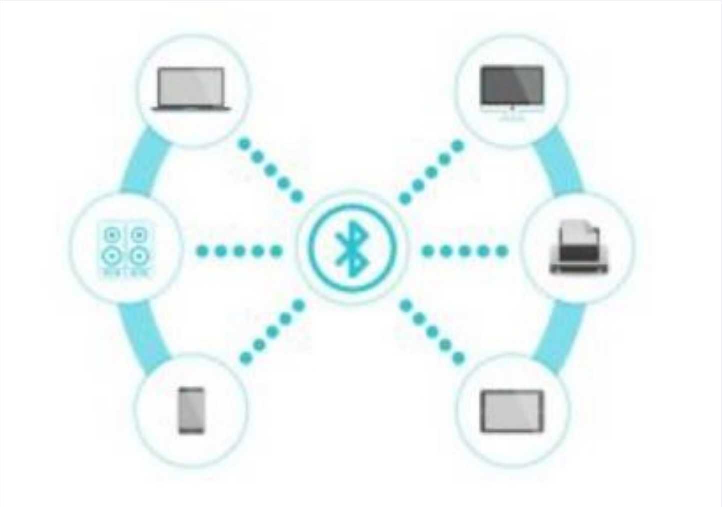
TWITTER ISSUE

On Monday, November 25, Twitter disclosed that they've received a report about an SDK made by data analytics platform OneAudience. The company offers a mobile SDK for Android and iOS apps that collects data on an app's users to provide additional insights for app makers about their audience.

Click **HERE** to read more.

How Bluetooth can be an attack gateway

(by **John Stock | 2019011-26 9:49:37Z**)



Recent data indicates there are 26.6 billion IoT devices currently in use in 2019 and this figure is set to rise significantly to 75 billion by 2025. While these IoT devices offer a range of benefits, contributing to more intelligent enterprises, they also create new security risks that work around antivirus protections.

For instance, one threat which is often overlooked is Bluetooth. While most people think of Bluetooth as a harmless technology that facilitates wireless connections between devices, it can actually create significant security risks when not managed properly, especially when users forget to add in authentication measures.

Connectivity comes with risk

Initially developed in 1998, Bluetooth is a wireless communication protocol that connects devices together. Whether using the latest wireless headphones, connecting phones to car handsfree systems or transferring files to colleagues, Bluetooth has proven to be a convenient tool in this wireless age. So much so, it has now established itself as standard technology, built within nearly every device or computer system on the market. However, like any piece of tech, convenience exposes vulnerabilities and security risks, causing endless headaches for the modern security professional.

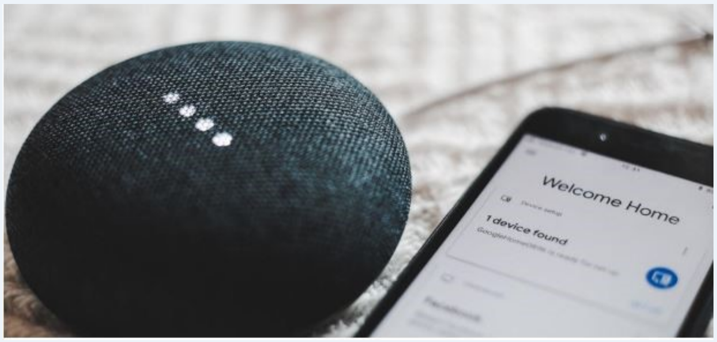
Sophisticated hackers with sinister intent have exploited several Bluetooth flaws to steal data or install malware, whether that be via Bluetooth chips, targeting mobile devices or even navigating through car entertainment systems. Some of the most high-profile Bluetooth attacks include:

Click **HERE** to read more.

FBI / Passwords

FBI recommends that you keep your IoT devices on a separate network

(by **Catalin Cimpanu** for **Zero Day | December 6, 2019 - 0334 GMT)**



The FBI says owners of IoT (Internet of Things) devices should isolate this equipment on a separate WiFi network, different from the one they're using for their primary devices, such as laptops, desktops, or smartphones.

'Your fridge and your laptop should not be on the same network,' the FBI's Portland office said in a weekly tech advice column. 'Keep your most private, sensitive data on a separate system from your other IoT devices,' it added.

The same advice - to keep devices on a separate WiFi network or LAN - has been shared in the past by multiple IT and security experts.

The reasoning behind it is simple. By keeping all the IoT equipment on a separate network, any compromise of a 'smart' device will not grant an attacker a direct route to a user's primary devices - where most of their data is stored. Jumping across the two networks would require considerable effort from the attacker.

However, placing primary devices and IoT devices on separate networks might not sound that easy for non-technical users. The simplest way is to use two routers.

The smarter way is to use 'micro-segmentation,' a feature found in the firmware of most WiFi routers, which allows router admins to create virtual networks (VLANs). VLANs will behave as different networks; even they effectively run on the same router. A good tutorial on how you can create VLANs on your routers is available here.

Click **HERE** to read more.

44 million Microsoft users reused passwords in the first three months of 2019

(by **Catalin Cimpanu** for **Zero Day | December 5, 2019 - 1542 GMT**)

The Microsoft threat research team scanned all Microsoft user accounts and found that 44 million users were employing usernames and passwords that leaked online following security breaches at other online services.

The scan took place between January and March 2019.

Microsoft said it scanned user accounts using a database of over three billion leaked credentials, which it obtained from multiple sources, such as law enforcement and public databases.

The scan effectively helped Microsoft identify users who reused the same usernames and passwords across different online accounts.

PASSWORD RESETS HAVE ALREADY TAKEN PLACE

The 44 million total included Microsoft Services Accounts (regular user accounts), but also Azure AD accounts.

'For the leaked credentials for which we found a match, we force a password reset. No additional action is required on the consumer side,' Microsoft said.

'On the enterprise side, Microsoft will elevate the user risk and alert the administrator so that a credential reset can be enforced.' it added.

The OS maker has been a staunch advocate and promoter of multi-factor authentication (MFA) solutions.

Click **HERE** to read more.

Dexphot / Stolen Cards

Microsoft says new Dexphot malware infected more than 80,000 computers

(by **Catalin Cimpanu** for **Zero Day | November 26, 2019 - 1700 GMT**)

Microsoft security engineers detailed today a new malware strain that has been infecting Windows computers since October 2018 to hijack their resources to mine cryptocurrency and generate revenue for the attackers.

A new malware strain has infected 80,000 Windows computers since October 2018.

Named Dexphot, this malware reached its peak in mid-June this year, when its botnet reached almost 80,000 infected computers.

Since then, the number of daily infections has been slowly going down, as Microsoft claims it deployed countermeasures to improve detections and stop attacks.

A COMPLEX MALWARE STRAIN FOR A MUNDATE TASK

But while Doxphot's end goal was banal, the methods and techniques for its modus operandi stood out due to their high level of complexity, something that Microsoft also noticed.

'Dexphot is not the type of attack that generates mainstream media attention,' said Hazel Kim, a malware analyst for the Microsoft Defender ATO Research Team, referring to the malware's mundane task of mining cryptocurrency, rather than stealing user data.

'It's one of the countless malware campaigns that are active at any given time. Its goal is a very common one in cybercriminal circles - to install a coin miner that silently steals computer resources and generates revenue for the attackers.' Kim said.

Click **HERE** to read more.

Sale of 4 Million Stolen Cards Tied to Breaches at 4 Restaurant Chains

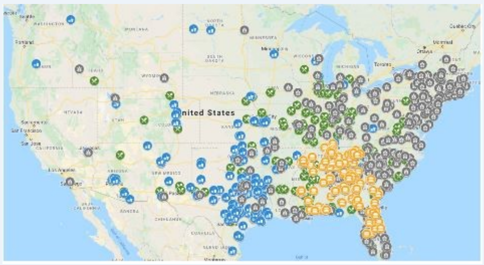
(by **Krebs**on**Security**)

On Nov. 23, one of the cybercrime underground's largest bazaars for buying and selling stolen payment card data announced the immediate availability of some four million freshly hacked debit and credit cards. KrebsOnSecurity has learned this latest batch of cards was siphoned from four different compromised restaurant chains that are most prevalent across the Midwest and eastern United States.

Two financial industry sources who track payment card fraud and asked to remain anonymous for this story said the four million cards were taken in breaches recently disclosed by restaurant chains **Krystal**, **Moe's**, **McAlister's Deli** and **Schlotzsky's**. Krystal announced a card breach last month. The other three restaurants are all part of the same parent company and disclosed breaches in August 2019.

KrebsOnSecurity heard the same conclusion from Gemini Advisory, a New York-based fraud intelligence company.

"Gemini found that the four breached restaurants, ranked from most to least affected, were Krystal, Moe's, McAlister's and Schlotzsky's," Gemini wrote in an analysis of the New World Order batch shared with this author. "Of the 1,750+ locations belonging to these restaurants, nearly 50% were breached and had customer payment card data exposed. These breached locations were concentrated in the central and eastern United States, with the highest exposure in Florida, Georgia, South Carolina, North Carolina, and Alabama."



Focus Brands (which owns Moe's, McAlister's, and Schlotzsky's) was breached between April and July 2019, and publicly disclosed this on August 23, Krystal claims to have been breached betweek July and September 2019, and disclosed this in late October.

Click **HERE** to read more.

More News

Your Smart TV could be spying on you, FBI warns

https://www.foxnews.com/tech/smart-tv-spying-fbi

Fin7 Cybergang Retools With New Malicious Code

https://threatpost.com/fin7-retools/149117/

Stealthy MacOS Malware Tied to Lazarus APT

https://threatpost.com/stealthy-macos-malware-lazarus-apt/150881/

New vulnerability lets attackers sniff or hijack VPN connections

https://www.zdnet.com/article/new-vulnerability-lets-attackers-sniff-or-hijack-vpn-connections/

DHS Chooses Bryan Ware, former AI entrepreneur, as assistant director for cybersecurity

https://www.cyberscoop.com/bryan-ware-dhs-assistant-director-cyber/?utm_campaign=CyberScoop%20-%20Editorial&utm_content=108015766&utm_medium=social&utm_source=twitter&hss_channel=tw-720664083767435264

New Facebook security program will warn presidential candidates of hacking attempts

https://www.cyberscoop.com/facebook-election-security-2020/?utm_campaign=CyberScoop%20-%20Editorial&utm_content=107997184&utm_medium=social&utm_source=twitter&hss_channel=tw-720664083767435264

France Not Ruling Out Response to Cyber Attack on Hospital

https://www.bloomberg.com/news/articles/2019-11-28/france-not-ruling-out-response-to-cyber-attack-on-hospital

Hacker's paradise: Louisiana's ransomware disaster far from over

https://arstechnica.com/information-technology/2019/11/hackers-paradise-louisianas-ransomware-disaster-far-from-over/

New Disney Plus Streaming Service Hit By Credential Stuffing Cyber Attack

https://www.cpomagazine.com/cyber-security/new-disney-plus-streaming-service-hit-by-credential-stuffing-cyber-attack/

Church's Chicken Restaurants Hit by Payment Card Breach

https://www.securityweek.com/churchs-chicken-restaurants-hit-payment-card-breach

Auditors Uncover Tens of Thousands of Critical Security Gaps At Energy Facilities

https://www.nextgov.com/cybersecurity/2019/11/auditors-uncover-tens-thousands-critical-security-gaps-energy-facilities/161539/

Smash-and-grab car thieves use Bluetooth to target cars containing tech gadgets

https://www.maritimecybersecurity.center/smash-and-grab-car-thieves-use-bluetooth-to-target-cars-containing-tech-gadgets/

More News

State-sponsored cyber attacks causing more damage

https://www.computerworld.com/article/3479970/state-sponsored-cyber-attacks-causing-more-damage.html

Dropbox Phishing Scam: Don't Get Fooled by Fake Shared Documents

https://www.thesslstore.com/blog/dropbox-phishing-scam-dont-get-fooled-by-fake-shared-documents/

Over 38 Million Healthcare Records Exposed in Breaches Over 2019

https://www.bleepingcomputer.com/news/security/over-38-million-healthcare-records-exposed-in-breaches-over-2019/

Anatomy Of A Scam: Nigerian Romance Scammer Shares Secrets

https://www.forbes.com/sites/ajdellinger/2019/11/25/anatomy-of-a-scam-nigerian-romance-scammer-shares-secrets/#ed0daa376385

Hackers target third-party payment processing page to phish victims

https://cyware.com/news/hackers-target-third-party-payment-processing-page-to-phish-victims-b15b55c0

Lights That Warn Planes of Obstacles Were Exposed to Open Internet

https://www.vice.com/en_au/article/7x5nkg/airplane-warning-lights-hacked

Silly Phishing Spotlight: Login to Unblock Microsoft Excel

https://www.bleepingcomputer.com/news/security/silly-phishing-spotlight-login-to-unblock-microsoft-excel/

Catch Says POS Malware Incident Might Have Exposed Customers' Data

https://www.tripwire.com/state-of-security/security-data-protection/catch-says-pos-malware-incident-might-have-exposed-customers-data/

The State of cybersecurity in the pharmaceutical industry

https://cyware.com/news/the-state-of-cybersecurity-in-the-pharmaceutical-industry-42835bac

Vistaprint left a customer service database unprotected, exposing calls, chats and emails

https://techcrunch.com/2019/11/25/vistaprint-security-lapse/?renderMode=ie11

TikTok accused in California lawsuit of sending user data to China

https://news.yahoo.com/tiktok-accused-california-lawsuit-sending-024206053.html

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 Lauren Christian:

PureLocker: New Ransomware-as-a-Service Being Used in Targeted Attacks Against Servers

This article is about a new and undetected ransomware threat is being used for targeted attacks against production servers of enterprise networks.

https://www.intezer.com/blog-purelocker-ransomware-being-used-in-targeted-attacks-against-servers/

FTC Provides Tips on Safeguarding Data Before Upgrading Mobile Phones

This article gives tips on how to protect your personal data when you upgrade your mobile phone.

https://www.us-cert.gov/ncas/current-activity/2019/11/19/ftc-provides-tips-safeguarding-data-upgrading-mobile-phones

RIPlace Evasion Technique

This is another article about RIPlace. It goes into more detail about how it is done.

https://www.nyotron.com/riplace

From David Evans:

Scammers try a new way to steal online shoppers' payment-card data

Thieves have devised a new way to steal payment-card data from online shoppers - or at least it's new to the researcher who found it.

https://arstechnica.com/information-technology/2019/11/scammers-try-a-new-way-to-steal-online-shoppers-payment-card-data/

Cyber Challenge

Cyber Challenge

Last Month's Challenge

Congratulations to everyone who was able to solve last month's challenges. There were 8 questions and one of them was tricky because I double encoded the message. 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 8 of 8 Challenges	
Erich Neumann @ 0930 on 18 Nov	Justin Whittington @ 1115 on 18 Nov	Faye Krueger @ 1115 on 18 Nov
Deborah Wright @ 1801 on 18 Nov	Rene Hess @ 0243 on 19 Nov	David Evans @ 1031 on 19 Nov
	James Kimani @ 2113 on 3 Dec	
	Completed 7 of 8 Challenges	
	Kevin Borth @ 0706 on 18 Nov	
	Completed 6 of 8 Challenges	
Debra Lewis @ 1506 on 19 Nov	Lynni Ward @ 1232 on 20 Nov	

1. I am a network that is constructed using public wires - usually the Internet - to connect remote users or regional offices to a company's private, internal network. What am I? **VPN**
2. I was a computer virus written by a high school student originally intended to be a prank. I was the first large-scale computer virus outbreak in history. What am I called and who wrote me? **Elk Cloner, Richard Skrenta**
3. I was the first computer system to be infected by the virus in question 2. What computer system am I? **Apple II**
4. I am considered the first real mobile malware. I was released in 2004 and spread via Bluetooth. My target was the Symbian operating system which was the primary OS used on smartphones at the time. What is my name? **Cabir**
5. I am an IoT botnet that launched the largest DDoS attack ever in October 2016. I attacked the service provider Dyn and took down a huge portion of the Internet. Some of the companies effected were Twitter, the Guardian, Netflix, Reddit and CNN. What is my name? **Mirai**
6. I am a type of software designed to protect computers from malware. When I find malware I remove it from the computer. What am I? **Anti-Virus software**
7. I am a security concept incorporated into home routers where a unique code on a computer is used by the router to identify the computer. If the computer is on the router approved list, it is allowed to communicate on the network. What am I? **MAC security**
8. This challenge was a hexadecimal code. When you decoded it you got a base-64 code. When you decoded that you got this: I am a cybersecurity model designed to guide policies for information security within an organization. I share a name with a U.S. Government agency. What am I? **CIA Triangle**

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

2. V nz n pbqr vawrpgvba grpuavdhr hfrq gb nggnpx qngn-qevira nccyvpngvbaf. Fgngrzragf ner vafregrq vagb n svryq gb rkcybvg n frphevgl ihyarenovyvgl va na nccyvpngvba fbsgjner. Jung nz V?

3. &#73;&#32;&#97;&#109;&#32;&#97;&#32;&#99;&#111;&#109;&#112;&#117;&#116;&#101;&#114;&#32;&#115;&#101;&#99;&#117;&#114;&#105;&#116;&#121;&#32;&#109;&#101;&#99;&#104;&#97;&#110;&#105;&#115;&#109;&#32;&#115;&#101;&#116;&#32;&#116;&#111;&#32;&#100;&#101;&#116;&#101;&#99;&#116;&#44;&#32;&#100;&#101;&#102;&#108;&#101;&#99;&#116;&#44;&#32;&#111;&#114;&#44;&#32;&#105;&#110;&#32;&#115;&#111;&#109;&#101;&#32;&#109;&#97;&#110;&#110;&#101;&#114;&#44;&#32;&#99;&#111;&#117;&#110;&#116;&#101;&#114;&#97;&#99;&#116;&#32;&#97;&#116;&#116;&#101;&#109;&#112;&#116;&#115;&#32;&#97;&#116;&#32;&#117;&#110;&#97;&#117;&#116;&#104;&#111;&#114;&#105;&#122;&#101;&#100;&#32;&#117;&#115;&#101;&#32;&#111;&#102;&#32;&#105;&#110;&#102;&#111;&#114;&#109;&#97;&#116;&#105;&#111;&#110;&#32;&#115;&#121;&#115;&#116;&#101;&#109;&#115;&#46;&#32;&#32;&#87;&#104;&#97;&#116;&#32;&#97;&#109;&#32;&#73;&#63;&#32;

4. .. / .- -- / .- / ..-. .-. . . / .- -. -.. / --- .--. . -. ... --- ..- .-. -.-. . / .--. .- -.-. -.- . - / .- -. .- .-.. -.-- --.. . .-. / / .. / .- -- / ..- ... . -.. / ..-. --- .-. / -. . - .-- --- .-. -.- / - .-. --- ..- -... .-.. . ... --- --- - .. -. --. --..-- / .- -. .- .-.. -.-- ... . --..-- / ... --- ..-. - .-- .- .-. . / .- -. -.. / -.-. --- -- -- ..- -. .. -.-. .- - .. --- -. ... / .--. .-. --- - --- -.-. --- .-.. / -.. . ...- . .-.. --- .--. -- . -. - --..-- / .- -. -.. / . -.. ..- -.-. .- - .. --- -. / / .-- .... .- - / .- -- / .. ..--..

5. 111 40 141 155 40 141 40 114 151 156 165 170 40 144 151 163 164 162 151 142 165 164 151 157 156 40 144 145 166 145 154 157 160 145 144 40 115 141 164 151 40 101 150 141 162 157 156 151 40 141 156 144 40 104 145 166 157 156 40 113 145 141 162 156 163 40 144 145 163 151 147 156 145 144 40 146 157 162 40 144 151 147 151 164 141 154 40 146 157 162 145 156 163 151 143 163 40 141 156 144 40 160 145 156 145 164 162 141 164 151 157 156 40 164 145 163 164 151 156 147 56 40 40 127 150 141 164 40 141 155 40 111 77 40

</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.

The list below was posted in last month's newsletter, but I felt it was important to share it again to remind people of ways to stay safe this holiday. There are unscrupulous people who wait for the holiday season to swindle people out of their money and/or steal their identity. These tips will hopefully keep you and your family safe from identity theft and scams.

- **Shop at websites you trust** - Shop from reputable sites. Be wary of going to random sites you see links to.
- **Check out the business** - What do its customer reviews say? Does it have a history of scam reports or complaints at the Better Business Bureau? Take it one step further by contacting the business. If there's no email address, phone number, or address for a brick-and-mortar location, that could be a signal that it's a fake company.
- **Beware rock-bottom prices** - Black Friday, Cyber Monday, and other big sales along the way have become a tradition of holiday shopping. The website may exist only to get your personal information.
- **Avoid public Wi-Fi** - Bottom line: it's never a good idea to shop online or log in to any website while you're connected to public Wi-Fi.
- **Use a VPN** - If you must shop online on public Wi-Fi, consider installing and using a VPN on all mobile devices and computers before connecting to any Wi-Fi network.
- **Create strong passwords**
- **Check out website security** - That small lock icon in the corner of your URL bar tells you that the web page you're on has privacy protection installed.
- **Watch out for email scams** - It might be tempting to open an email that promises a "special offer." Clicking on emails from unknown senders and unrecognizable sellers could infect your computer with viruses and malware. Delete them, don't click on any links, and don't open any attachments from people you are unfamiliar with.
- **Don't give out too much information** - It isn't really paranoia if they are out to get you
- **Pay with a credit card** - Most major credit cards offer $0 liability for fraudulent purchases.
- **Check your statements**
- **Mind the details** - Keep the receipt, order confirmation number, and postal tracking number in a safe place. If you have a problem with the order, this information will help the merchant resolve the problem.
- **Take action if you don't get your goods**
- **Report the company**
- **Make a resolution** - The holiday season doesn't last forever. Make a New Year's resolution to shop safely online.

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.**