NEWS
Cyber Security
Vol. 4 | Issue 5
May 2019

Page 2 | Page 3 | Page 4 | Page 5 | More News | Reader Articles | Challenge | Closing

Welcome to the TXDPS Cyber Newsletter

Hello everyone and welcome to this month's cybersecurity newsletter. I hope you find this month's newsletter relevant and interesting. Before you start reading the articles, I want to take a few minutes and talk about a problem one of our users notified me about. He has had several phishing attempts to his DPS cell phone. This is actually known as Vishing but it works exactly the same way as Phishing, just via a phone instead of through email. Phishing and Vishing are both forms of Social Engineering. For those who don't remember what Social Engineering is from previous newsletters, or maybe this is the first time you have heard the term, Social Engineering is a non-technical hacking technique. It is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Social Engineering is probably the most dangerous form of hacking because it does not require any technical expertise. All it requires is the individual be personable and able to convince the victim to divulge information without the victim realizing they are doing so. Many techniques are used to do this but the most common is to try to scare the victim and convince them they need to provide the information being requested.

Unlike email phishing scams, vishing isn't easy to prevent. Email servers can be "trained" to look for certain things in an email and automatically block them from getting to a user. But how do you determine if an incoming phone call is legitimate or not? How do you know the call you are receiving is not from your utility company, a corporation, a police department, etc? And why is it so difficult to be sure? The reason an individual and phone company cannot be sure is because it is very easy to spoof a phone number to look like it originates from a legitimate source. So unfortunately there really is not an easy way to determine the legitimacy of an incoming phone call or text. This also means there is no way to effectively block fraudulent calls or text. The best defense is knowledge and a little skepticism. The old saying "If it seems to good to be true" then it probably is. Before giving information or clicking on a link in the text, look up the phone number (never trust one given to you) to the organization contacting you and call them. See if they did contact you. If so, now you know it is safe to provide the information because YOU contacted them through a verified number so now you know you aren't talking to someone Vishing you.

Here are some great videos that show you exactly what Vishing is and how it is done:

Hack Attack—Vishing   Credit Card Vishing Scam   Phone Scams   Vishing a Business

Smishing and Vishing   Three Vishing Calls   Protect Yourself   Vishing From a Hacker

"Vishing" phone calls come from attackers who appear to be calling from a local number and claim to be from government agencies such as the IRS or police or services such as credit card companies, but the intent is the same as phishing — trying to steal your money.

Cyber Command / Phishers

Cyber Command has redeployed overseas in effort to protect 2020 elections

(by **Shannon Vavra** on **May 7, 2019**)

U.S. Cyber Command is still working overseas with allies to try preventing election interference, Brig. Gen. Timothy Haugh, the commander of Cyber Command's cyber national mission force said Tuesday.

As part of the military's operation to defend the U.S. midterm elections in 2018, an operation known internally in the Department of Defense as "Synthetic Theology," Cyber Command deployed cyberwarriors to Ukraine, North Macedonia, and Montenegro to help defend those countries' networks, and to collect intelligence on adversaries. Cyber Command has since "redeployed" out of "some of those" countries, Haugh said during a reporters' roundtable at the Integrated Cyber Center and Joint Operations Center in Fort Meade, Maryland.

Haugh did not specify in which countries Cyber Command has ongoing operations right now in preparation for 2020, but said these kinds of partnerships will continue to grow.

"When we look to do partnerships overseas … we want to do that anywhere where there's a potential adversary that would also target our electoral systems," Haugh said.

The effort is meant to complicate possible election interference originating in countries like Russia, which the U.S. intelligence community has determined sought to interfere in the 2016 presidential election. Investigators also found that hackers infiltrated state election infrastructure ahead of last year's midterm elections, and a steady stream of account takedowns have demonstrated how suspected government propagandists still are using social media to manipulate public opinion. By working with the countries affected by this problem now, the logic goes, Cyber Command can gain an insight into what the U.S. might expect next year.

Click **HERE** to read the article.

Facebook, Instagram Are Phishers' Favorite Social Platforms

(by **DARK Reading** on **5/2/2019**)

Cloud companies continue to represent the most phishing URLs, but social media saw the most growth in Q1 2019.

Facebook phishing spiked 155.5% in the first quarter of 2019, pushing social media into the fourth most-popular category for phishing attacks. Instagram phishing URLs jumped 1,868%

Social media saw more growth than any other phishing category evaluated in the Vade Secure "Phishers' Favorites" report for the first quarter of 2019, which shares the 25 most impersonated brands for each quarter. This is the first time it published a global report after seeing little change in top brands for North America and Europe in the previous three quarters.

Facebook was the top spoofed brand in the first quarter of 2018, and then dropped for three straight quarters, falling to No. 7 in the fourth quarter of 2018. Researchers aren't sure why it's now again appealing to hackers. One reason could be the rise of social sign-on using Facebook accounts, which attackers could use to view and compromise other apps people have authorized for Facebook login. Another theory involves Facebook's dubious security practices.

Instagram is an interesting target because, as researchers point out, phishing attacks targeting the brand were "virtually nonexistent" for three straight quarters before spiking in 2019. In early March, a phishing campaign tried to trick victims into providing credentials in exchange for a "verified" Instagram badge; analysts think these incidents drove the increase.

Microsoft was the top spoofed brand in the first quarter of 2019. Researchers attribute the trend to the high value of Office 365 credentials, which give intruders access to the Office 365 platform and let them commit a range of attacks: suspended account claims, malicious links, and face OneDrive and SharePoint documents. PayPal came in second after phishing attacks rose 88% in the first quarter.

Click **HERE** to read the article.

Chinese hackers / Verizon

Chinese hackers found and repurposed elite NSA-linked tools

(by **Greg Otto** on **May 6, 2019**)

A hacking group with ties to Chinese intelligence has been using tools linked to the National Security Agency as far back as March 2016, according to research from security firm Symantec.

The tools include some released by the Shadow Brokers, a mysterious group that dumped computer exploits once used by the NSA on the open internet in April 2017. Symantec's research suggests that the Chinese-linked group, which the company calls "Buckeye," was using the same NSA-linked tools at least a year before they were publicly leaked.

According to Symantec, one of the tools used by Buckeye was DoublePulsar, a backdoor implant that allows attackers to stealthily collect information and run malicious code on a target's machine. DoublePulsar was used in conjunction with another tool, which Symantec calls Trojan.Bemstour, that took advantage of various Microsoft Windows vulnerabilities in order to secretly siphon information off targeted computers.

The Trojan.Bemstour exploit allowed attackers to remotely manipulate a machine's kernel, the core part of a computer's operating system that manages resources such as memory. When put into action, the exploit can pull sensitive information from a targeted machine or can be combined in conjunction with other vulnerabilities to take control of the kernel.

Click **HERE** to read more.

Financial crime outpaces espionage as top motivation for data breaches, Verizon report finds

(by **Jeff Stone** on **May 8, 2019**)

Seventy-one percent of the data breaches that occurred in the last year were financially motivated, according to Verizon's annual Data Breach Investigations Report. While there's been uptick in espionage targeting the manufacturing sector, the overwhelming majority of cybercrime still is carried out by hackers primarily interested in making a buck. Just ask the financial companies: For the first time last year, they reported more instances of fraud when a physical card was not used than when a card was present.

"It's not necessarily that attackers are changing their techniques, or even evolving," said Alex Pinto, head of security research at Verizon, of the findings. "It's that attackers are keen to go after whoever is the easiest target … and there was a very sharp uptick on financially motivated social engineering."

Verizon's DBIR has become a well-regarded barometer of threats, hacking techniques and other lessons culled from thousands of breaches voluntarily shared with the U.S. telecom giant by enterprises in various industries. This edition, the 12th, includes data from 41,686 security incidents, of which 2,013 were confirmed data breaches.

The objective, Pinto said, is to help security leaders better understand where hackers are most likely to attack, and stop a breach before it occurs.

Sixty-nine percent of the breaches were carried out by outsiders, according to Verizon. Most (52 percent) involved hacking, with 33 percent were social attacks and 28 percent could be blamed on malicious software. A mere 32 percent of the reported incidents involved phishing while espionage, the act of gaining some kind of strategic advantage, was the cause of 25 percent.

Click **HERE** to read .

Israel / DOE

WHAT ISRAEL'S STRIKE ON HAMAS HACKERS MEANS FOR CYBERWAR

(by **Lily Hay Newman** on **05.06.19 @ 04:43 PM)**

This weekend, violence between Israel and Gaza escalated to a degree not seen since 2014, with 25 Palestinians and four Israelis killed in the fighting. Decades into the entrenched tensions of the region, the incident overall was tragically unsurprising. But for cybersecurity professionals, one aspect particularly stood out: The Israeli Defense Force claimed that it bombed and partially destroyed one building in Gaza because it was allegedly the base of an active Hamas hacking group.

The assault seems to be the first true example of a physical attack being used as a real-time response to digital aggression—another evolution of so-called "hybrid warfare." That makes it a landmark moment, but one that analysts caution must be viewed in the context of the conflict between Israel and Palestine, rather than as a standalone global harbinger.

What Happened?

This is a very good question, but one that still lacks clear answers. IDF said in a tweet on Sunday that "We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed." But IDF has not provided any other details about the nature of the alleged cyberattack, and it is unclear from current IDF statements why Israel would choose to retaliate for an assault that it claims to have successfully fended off.

Click **HERE** to read more.

'Denial of service' attack caused grid cyber disruption: DOE

(by **Blake Sobczak** on **Thursday, May 2, 2019**)

A recent cyber disruption to the U.S. grid involved a "denial of service condition" at a Western utility, according to a Department of Energy official.

On March 5, an unidentified power company fell victim to a "cyber event" that interfered with operations but stopped short of causing blackouts, according to a DOE filing this week.

A DOE official confirmed yesterday that the event "did not impact generation, the reliability of the grid or cause any customer outages."

But the denial-of-service attack was significant enough for the utility to file an electric disturbance report with DOE—the same forms reserved for major interruptions like storms, physical attacks or fuel shortages (Energywire, April 30).

Denial-of-service, or DOS, cyberattacks overwhelm target networks with bogus traffic, making it difficult for victim computers to operate normally. Distributed-denial-of-service (DDOS) attacks harness the power of hacked "botnets" of computers to throw at hackers' targets, while rarer telephony-denial-of-service (TDOS) events seak to block incoming and outgoing calls.

In December 2015, suspected Russian hackers used stolen login credentials and a TDOS attack to hit three distribution utilities in Ukraine, briefly cutting the lights to about a quarter-million people in a first-of-its-kind cyberattack (Energywire, July 18, 2016).

The March event doesn't appear to be part of such a coordinated hacking campaign, based on the limited information disclosed by DOE and several organizations in the anonymous utility's service area of Utah, Wyoming and Southern California. Still, a malicious cyberevent wasn't previously known to have interfered with U.S. grid operations, making the March 5 disclosure significant.

Click **HERE** to read more.

Microsoft / Dell

Microsoft pushes open-source software kit to election agencies, voting-tech vendors

(by **Sean Lyngaas** on **May 6, 2019**)

Election officials around the U.S. could soon have access to an open-source software development kit from Microsoft that is intended to make voting more secure and transparent.

The software kit, called ElectionGuard, will allow third parties to validate election results and voters to ensure their ballots were correctly counted, according to Microsoft. Each voter would get a unique code to track the encrypted version of his or her vote to confirm that it was not altered.

“It will not be possible to ‘hack’ the vote without detection,” Tom Burt, a Microsoft corporate vice president, asserted in a blog post Monday. He touted the kit’s use of homomorphic encryption, which will allow votes to be counted without decrypting the data, as a feature that will protect votes individually and collectively.

The software, which will be available starting this summer to election agencies and vendors, is meant to supplement, rather than replace, paper ballots. Its code will be posted to GitHub, and can be layered onto existing voting software for added integrity.

The tech giant plans to have ElectionGuard ready for piloting in the 2020 elections—a vote that federal, state, and local officials are already preparing to secure. Last month, FBI Director Christopher Wray said protecting the 2018 U.S. midterm elections from foreign meddling was a “dress rehersal for the big show” of the 2020 presidential contest.

Click **HERE** to read more.

Pre-Installed Software Flaw Exposes Most Dell Computers to Remote Hacking

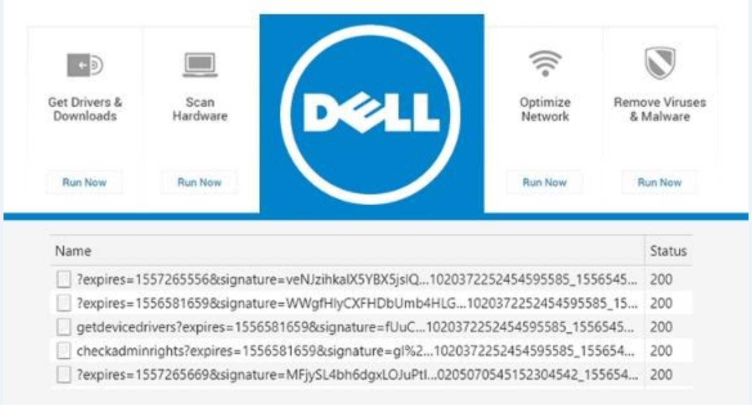
(by **Mohit Kumar** on **May 02, 2019**)

If you use a Dell computer, then beware - hackers could compromise your system remotely.

Bill Demirkapi, a 17-year-old independent security researcher, has discovered a critical remote code execution bulnerability in the Dell SupportAssist utility that comes pre-installed on most Dell computers.

Dell SupportAssist, formerly known as **Dell System Detect**, checks the health of your computer system’s hardware and software.

The utility has been designed to interact with the Dell Support website and automatically detect Service Tag or Express Service Code of your Dell product, scan the existing device drivers and install missing or available driver updates, as well as perform hardware diagnostic tests.



Name	Status
□ ?expires=1557265556&signature=veNJzihkalX5YBX5jslQ...10203722524545955855_1556545...	200
□ ?expires=1556581659&signature=WWgfHlyCXFHDbUmb4HLG...1020372252454595585_15...	200
□ getdevicedrivers?expires=1556581659&signature=fUuC...1020372252454595585_1556545...	200
□ checkadminrights?expires=1556581659&signature=gl%2...1020372252454595585_155654...	200
□ ?expires=1557265669&signature=MFjySL4bh6dgxLOJuPtl...0205070545152304542_155654...	200

If you are wondering how it works, Dell SupportAssist in the background runs a web server locally on the user system, either on port 8884, 8883 8886, or port 8885, and accepts various commands as URL parameters to perform some-predefined tasks on the computer, like collecting detailed system information or downloading a software from remote server and install it on the system.

Though the local web service has been protected using the “Access-Control-Allow-Origin” response header and has some validations that restrict it to accept commands only from the “dell.com” website or its subdomains, Demirkapi explained ways to bypass these protections in a blog post published Wednesday.

As shown in the video, Demirkapi demonstrated [PoC code] how remote hackers could have easily downloaded and installed malware from a remote server on affected Dell computers to take full control over them.

Click **HERE** to read more.

More News

AMC accidentally exposed data on 1.6 million subscribers

https://www.engadget.com/2019/05/03/amc-sundance-now-shudder-subscriber-exposed-database/

Google manually reviewed a million suspected terrorist videos on YouTube

https://www.engadget.com/2019/05/02/google-youtube-terrorist-videos-manual-review/

Why older employees are less likely to get tricked by phishing attacks

https://www.techrepublic.com/article/why-older-employees-are-less-likely-to-get-tricked-by-phishing-attacks/

Evil Clippy Can Bypass Antivirus Products to Infect Microsoft Office

https://news.softpedia.com/news/evil-clippy-can-bypass-antivirus-products-to-infect-microsoft-office-525889.shtml

International "Malvertiser" Extradited from the Netherlands to Face Hacking Charges in New Jersey

https://www.justice.gov/opa/pr/international-malvertiser-extradited-netherlands-face-hacking-charges-new-jersey

AT&T, Verizon, Sprint and T-Mobile get sued for reportedly selling your location data

https://news.yahoo.com/t-verizon-sprint-t-mobile-172726883.html

Hackers steal card data from 201 online campus stores from Canada and the US

https://www.zdnet.com/article/hackers-steal-card-data-from-201-online-campus-stores-from-canada-and-the-us/

Home routers are open to attacks, as Huawei 'backdoor' shows

https://www.foxnews.com/tech/home-routers-are-open-to-attacks-as-huawei-backdoor-shows

Millions of Chinese-made devices, including baby monitors, vulnerable to hacking: study

https://www.foxnews.com/tech/devices-baby-monitors-vulnerable-hacking-study

Facebook contractors categorize your private posts to train AI

https://www.engadget.com/2019/05/06/facebook-privacy-content-labeling/

Hackers exploiting unpatched Chrome bug to target 500M iPhone users

https://www.hackread.com/hackers-exploite-unpatched-chrome-bug-iphone-users/?fbclid=IwAR33RL8bF0e_VjvapfC08teis7SAg5PdC4b4btsRp3xwbLLBB6JzjIV11jo

More News

DHS Sets List of National Critical Functions, Marking Shift from CI Sectors

https://www.meritalk.com/articles/dhs-sets-list-of-national-critical-functions-marking-shift-from-ci-sectors/

A curious case of Bloomberg's Huawei scoop

https://www.axios.com/curious-case-bloombergs-huawei-scoop-5ea156bc-0fa6-42e0-8ece-41a0e9619fcd.html

Cybersecurity pros could work for multiple agencies under bill passed by Senate

https://www.fedscoop.com/federal-rotational-cyber-workforce-program-passes-senate/

U.S. cyber spies unmasked many more American identities in 2018—U.S. report

https://news.yahoo.com/u-cyber-spies-unmasked-many-more-american-identities-201214748.html

Self-taught Belgian bloke cracks cryto conundrum that was supposed to be uncrackable until 2034

https://www.theregister.co.uk/2019/04/30/cryptography_conundrum_cracked/

Microsoft Hackers Stealing Bitcoin from Compromised Accounts

https://news.softpedia.com/news/microsoft-hackers-stealing-bitcoin-from-compromised-accounts-525833.shtml

Windows 10 Security Feature Makes Chromium Browsers Three Times Slower

https://news.softpedia.com/news/windows-10-security-feature-makes-chromium-browsers-three-times-slower-525836.shtml

50,000 companies running SAP installations open to attack via publicly released exploits

https://www.helpnetsecurity.com/2019/05/02/misconfigured-sap-installations/

Apple Claims Parental Control Apps Removed Due to Use of MDM

https://www.securityweek.com/apple-claims-parental-control-apps-removed-due-use-mdm

Exposed database holds sensitive data on over 80 million US households

https://www.engadget.com/2019/04/29/database-exposes-80-million-us-households/

Slack to investors: we might be the target of organized crime, nation-sponsored hackers

https://securityboulevard.com/2019/04/slack-to-investors-we-might-be-the-target-of-organized-crime-nation-sponsored-hackers/

Data breach of unknown entity exposes private data of 80 million U.S. households

https://www.digitaltrends.com/computing/data-breach-exposes-data-of-80-million-us-households/

Reader Suggested Articles

Below are readers suggestions for this month. Hopefully you will find the articles as interesting as I did.

From Erich Neumann:

Over 80% of All Phishing Attacks Targeted U.S. Organizations

- https://www.bleepingcomputer.com/news/security/over-80-percent-of-all-phishing-attacks-targeted-us-organizations/

25% of Phishing Emails Sneak into Office 365: Report

- https://www.darkreading.com/cloud/25--of-phishing-emails-sneak-into-office-365-report/d/d-id/1334397

New Super-Secure Wifi Is Actually Full of Security Holes

- https://gizmodo.com/new-super-secure-wifi-is-actually-full-of-security-hole-1833967122

6 Ways Attackers Are Still Bypassing SMS 2-Factor Authentication

- https://www.securityweek.com/6-ways-attackers-are-still-bypassing-sms-2-factor-authentication

From Deborah Wright

GODADDY TAKES DOWN 15,000 SPAMMY ‘SNAKE OIL’ SUBDOMAINS

- https://www.wired.com/story/godaddy-spam-takedown-subdomains-snake-oil/

Microsoft admits expiring-password rules are useless

- https://www.cnet.com/news/microsoft-admits-expiring-password-rules-are-useless/

Security baseline (DRAFT) for Windows 10 v1903 and Windows Server v1903

- https://blogs.technet.microsoft.com/secguide/2019/04/24/security-baseline-draft-for-windows-10-v1903-and-windows-server-v1903/

Ransomware disables Cleveland airport’s email systems, information screens

- http://www.scmagazine.com/home/security-news/ransomware-disables-cleveland-airports-email-systems-information-screens/

More than 1,500 feds applied for first Cyber Reskilling Academy cohort

- https://www.fedscoop.com/cyber-reskilling-academy-1500-applicants/

All You Need to Know about the Cyber Retraining Academy

- https://www.infosecurity-magazine.com/news-features/all-you-need-cyber-retraining/

A MYSTERIOUS HACKER GROUP IS ON A SUPPLY CHAIN HIJACKING SPREE

- https://www.wired.com/story/barium-supply-chain-hackers/

Feds Bust Up Dark Web Hub Wall Street Market

- https://krebsonsecurity.com/2019/05/feds-bust-up-dark-web-hub-wall-street-market/

Firefox 66.0.4 Released With Fix for Disabled Addons

- https://www.bleepingcomputer.com/news/software/firefox-6604-released-with-fix-for-disabled-addons/

Cyber Challenge

Cyber Challenge

Last Month’s Challenge

Here are the people who completed last month’s challenges:

Deborah Wright @ 0007 on 8 April 2019	Erich Neumann @ 0523 on 8 April 2019	Faye Krueger @ 1101 on 8 April 2019
Rene Hess @ 1709 on 9 April 2019	Jared Crouse @ 0426 on 11 April 2019	James Taylor @ 2020 on 15 April 2019

Last month’s cyber challenge was to find three messages hidden in the newsletter and then decipher them. The messages are all cryptograms and the first one can be found on the first page. The message was:

P OS O FCNM IOQYCNAZB WMEC AV UMGCN OWWOUJ PQ TKPUK O UONCVRRM WONYCWCI IPYPWOR SCBBOYC PB WNOQBSPWWCI WA VAAR ECAERC PQWA URPUJPQY AQ O RPQJ WA PQBWORR SORTONC AN CDEABC BCQBPWPFC IOWO. TKOW OS P?

Once you decrypt it you get:

I am a very dangerous type of cyber attack in which a carefully targeted digital message is transmitted to fool people into clicking on a link to install malware or expose sensitive data. What am I?

The answer to the question is: **phishing**.

The second message was on the fourth page:

K EH E RJVGC RMER KGLBSLVZ TUDVJ TJKHKGESZ MKIETAKGY RMKJC-OEJRU MBHV BJ PBJA TBHOWRVJZ RB HKGV NBJ TJUORBTWJJVGTU. PMER EH K TESSVC?

Once you decrypt it you get:

I am a trend that involves cyber criminals hijacking third-party home or work computers to mine for cryptocurrency. What am I called?

The answer to the question is **cryptojacking**.

The last message can be found on the fifth page:

O NJ N MHHZ MTNM NZZHIU SUQKU MH YQBQAY NWNOAUM JNA-OA-MTQ-JOYYZQ NMMNFLU HA HDQA IOBO AQMIHKLU. O DKHCOYQ NA QAFKEDMQY MSAAQZ BKHJ MTQ FHJDSMQK MH NA QAY DHOAM UHJQITQKQ QZUQ HA MTQ DZNAQM. ITNM NJ O FNZZQY?

Once you decrypt it you get:

I am a tool that allows users to defend against man-in-the-middle attacks on open wifi networks. I provide an encrypted tunnel from the computer to an end point somewhere else on the planet. What am I called?

The answer to the question is **VPN**.

For those of you who didn’t attempt or were unable to complete last month’s challenges, I encourage you to look for the hidden messages and see if you can now solve the challenges. If you need assistance, email me.

This month’s challenge is on the next page. Remember, if you have difficulties solving the challenges you can always email me for hints.

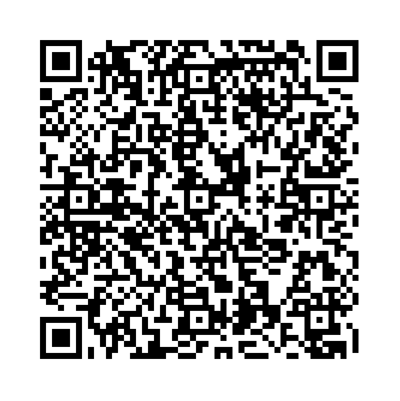
Cyber
Challenge

Cyber Challenge

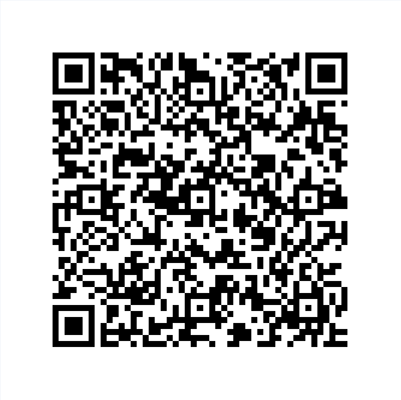
This Month's Challenge

As you can see below, this month's challenge is six QR Codes. Each code contains a question. To complete the challenge you will need to extract the question from each QR code, determine the answers, and then email them to me. Good luck. Email me if you have any questions or need hints.

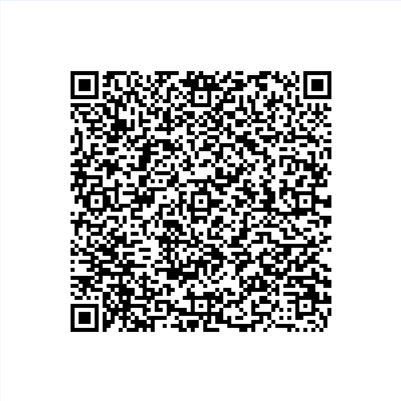
1)



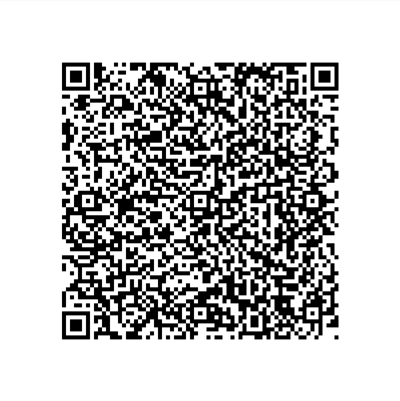
2)



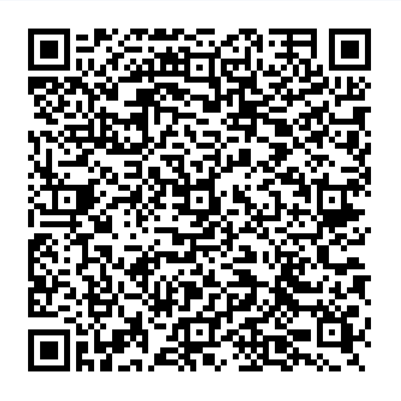
3)



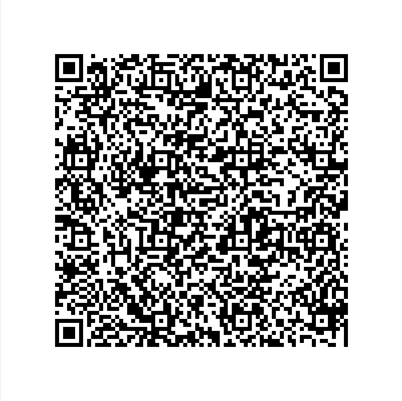
4)



5)



6)



For those who have no idea how to get started, there are several free QR Readers you can download to your phone. I suggest you try one of them to scan each picture and retrieve the hidden message.

</Closing Comments>

Thank you for taking the time out of your day to read the newsletter. As always, I hope you found this month's newsletter informative, interesting, and useful. Remember, you can only defend against threats when you are knowledgeable about them. I realize cybersecurity is not the most liked topic, but it is important to understand the dangers you and your family face when online and how your actions and the actions of others can affect the Agency and your personal life.

As a closing thought, there is a quote I heard once but cannot remember where or when. That quote is "You may not care about Cybersecurity, but Cybersecurity cares about you." I wanted to include this quote in the newsletter because I often hear people say they do not worry about cybersecurity because there is "no reason why anyone would want to hack me." Or I hear, "I do not have anything a hacker would want." These are very naïve statements. All the person is doing is deluding themselves into believing they do not need to worry about security updates, anti-virus updates, application updates or even being aware of cybersecurity issues. My question to you is; Have you ever said or thought something like this? These beliefs not only endanger the user, and everyone else.

A weak link in any system is where a malicious actor will attack. This is true in both the physical as well as the digital world. It is also true for both personal and business computers, cell phones, tablets, IoT devices, etc. Everything I listed is nothing more than a specialized computer. Not protecting them endangers yourself, the department, and whatever network these device attach to. So if you do believe there is no reason someone would want to compromise your cell phone, computer, smart TV, Alexa, Echo, Ring, etc; remember that YOU are exactly who a malicious actor is looking for.

If you have questions or would like more information about these things, email me and I will be happy to talk to you more about it.

Kirk

As a reminder, feel free to share this and previous newsletters with friends and family. The better educated everyone is on cyber issues the safer everyone is. You can see previous issues of the website at this public facing DPS site:

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

Again, I hope you enjoyed the newsletter and good luck with the Cyber Challenges. If you have suggestions on how the newsletter could be improved, please let me know.

And as always,

THANK YOU FOR YOUR CYBER VIGILANCE.