Cyber Security NEWS
Vol. 4 | Issue 10
October 2019

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

Welcome to the TXDPS Cyber Newsletter

Hello everyone and welcome to this month's DPS Cybersecurity Newsletter. If you are a new reader, welcome. I hope you find the information provided relevant and useful. If you are a regular reader, thank you for continuing to read the newsletter and I encourage you to forward it on to anyone you know who needs some cyber education.

To begin this month's newsletter I want to address TXDPS readers and talk about the program Grammarly. There are several users throughout DPS who are using or want to use the program Grammarly. For those who do not know what Grammarly is, it is a cloud based program that can automatically detect grammar, spelling, punctuation, word choice and style mistakes in your writing. There are three ways the program can be used. You can either submit information to the website, use a browser extension or downloading the app to a computer. While this sounds like a wonderful program which can make the average user more efficient, there are dangers you need to be aware of. The following is an excerpt from the Grammarly website:

We collect this information as you use the Site, Software, and/or Services:

- *User Content. This consists of all text, documents, or other content or information uploaded, entered, or otherwise transmitted by you in connection with your use of the Services and/or Software.*
- *By uploading or entering any User Content, you give Grammarly (and those it works with) a nonexclusive, worldwide, royalty-free and fully-paid, transferable and sub licensable, perpetual, and irrevocable license to copy, store and use your User Content (and, if you are an Authorized User, your Enterprise Subscriber's User Content) in connection with the provision of the Software and the Services and to improve the algorithms underlying the Software and the Services.*

Certain data about the devices you use to connect with Grammarly and your use of the Site, Software, and/or Services are automatically logged in our systems, including:

- *Location information. This is the geographic area where you use your computer and mobile devices (as indicated by an Internet Protocol [IP] address or similar identifier) when interacting with our Site, Software, and/or Services.*
- *Log data. As with most websites and technology services delivered over the internet, our servers automatically collect data when you access or use our Site, Software, and/or Services and record it in log files. This log data may include the IP address, browser type and settings, the date and time of use, information about browser configuration, language preferences, and cookie data.*
- *Usage information. This is information about the Grammarly Site, Software, and/or Services you use and how you use them.*

What does this mean? It means the data collected could be very damaging to DPS. If you use Grammarly on any document that contains PII, HIPAA, CJI, TLP data or any other sensitive/protected data, per Grammarly's End User License Agreement they now possess a copy of the data and can use it how they wish (see bullet 2 above). And while unsubstantiated, there are reports from researchers which say that even having Grammarly loaded on devices gives it access to information not directly submitted to the program. If true, this means the program would have access to sensitive data not directly provided to the program.

As with all software, it is the business and data owners' responsibility to protect Agency data. While Grammarly provides a beneficial service, it also poses a greater than normal potential threat of leaked confidential data. Current DPS policy allows the use of Grammarly but it is strongly discouraged. The software is not on the Approved Software List because of the potential danger posed to DPS data. For those who wish to use the software, submit a request and one of our analyst will discuss the dangers of the software with you and give suggestions on how to safely use the software.

This and other important information can be found on the DPS Cybersecurity SharePoint site under General Information.

Ransomware / Fake Apps

Threat Level Increases in 2019 as Several Cities and Counties in US Respond to Ransomware Attacks by Paying Hefty Ransom

(by **CYWARE | 26 Sep 2019 @ 0300 GMT**)

Ransomware attacks are burgeoning across the cities and counties in the US. According to The U.S. Conference of Mayors, at least 22 such attacks have been noticed in the first half of 2019. This includes the counties of Fisher, Texas, Genesee and Michigan and the cities like Baltimore and Albany.

Cost of ransomware attacks

Few cities like Baltimore had strongly rejected the ransom by incurring the loss which amounted to nearly 10 times the ransom. However, there were few counties and cities that decided to pay the asked ransom to gain access to their infected systems.

Jackson County paid a sum of $400,000 in ransom to decrypt the data and regain access to their affected computer systems affected by the ransomware attack in March 2019. It was determined the County's infrastructure was infected using Ryuk ransomware.

The Lake City in Florida made several attempts to restore the affected networks before paying a ransom of roughly $480,000 to recover its encrypted data. The ransom was paid in the form of 42 Bitcoins to threat actors.

Another city in Florida, Riviera Beach met with the same fate on June 2019. The city which was locked out of its systems and email services since May 29, 2019, decided to pay more than $600,000 to a ransomware gang to recover its data. Apart from this, the City's officials also spent $941,000 for new computer systems and other hardware. This step was taken to rebuild its IT infrastructure following the incident.

Click **HERE** to read the article.

Fake Apps Sneak Gambling Into iOS and Android App Stores

(by **Ionut Ilascu | September 27, 2019 @ 11:14 AM**)

Gambling apps double-crossed the review systems in Google Play and the App Store by posing as a policy-abiding app. After bypassing the verification, the infringing functionality became available to users.

The apps made it into the Android official store in August but survived for a longer time in the iOS repository as some of them had been rated more than 100,000 times.

Bypassing the review systems

The App Store tightened its restrictions on apps with games that involve real money (lotteries, gaming, charity, digital commerce) and starting September 3, all such apps must include the code for this functionality in the binary, for Apple's review.

Similarly, Google accepts gambling apps in its Android store only in countries where they are legal (UK, France, and Ireland, for the moment).

Despite the restrictions, some developers managed to push apps that featured content that violates the policies of the two stores.

They created apps with functionality in agreement with the store requirements, such as weather tracking or entertainment. But they come with an API switch feature to control the availability of the illegal content in the app.

The accepted content is only a façade maintained until the app becomes available to users. Once it makes it to the store, the real content is loaded in a WebView. The real content is then delivered from a specific URL in a WebView.

Click **HERE** to read the article.

SIM Attack / Pedestrian-Safety

Researchers Disclose Another SIM Card Attack Possibly Impacting Millions

(by **Edward Kovacs** | **September 27, 2019**)

A new variant of a recently disclosed SIM card attack method could expose millions of mobile phones to remote hacking, researchers have warned.

Earlier this month, cyber telecoms security firm AdaptiveMobile Security disclosed the details of Simjacker, an attack method that involves sending specially crafted SMS messages to the targeted mobile phone.

The attack relies on the fact that these special messages are processed by the legacy S@T Browser present on many SIMs. An attack could issue commands to conduct various types of activities, including sending SMS messages, making phone calls, launching a web browser, and collecting information about the targeted device, regardless of operating system and manufacturer.

AdaptiveMobile estimates that the attack could work against over 1 billion mobile phones considering that the S@T Browser is present on SIM cards provided by mobile operators in more than 30 countries. The company also claimed that an unnamed organization that helps governments monitor individuals has been using this method for at least two years.

The Simjacker attack method that leverages the S@T Browser was also independently discovered by researchers at Ginno Security Lab, a non-profit cybersecurity organization. Ginno Security Lab has dubbed the method S@Tattack and recently published a blog post describing its findings.

However, Ginno Security Lab has also identified a second SIM card attack method, one that involves the Wireless Internet Browser (WIB), which SmartTrust created for SIM toolkit based browsing. This attack has been dubbed WIBattack.

Click **HERE** to read more.

New Cars' Pedestrian-Safety Features Fail in Deadliest Situations, Study Finds

(by **Ben Foldy** | **Oct 3, 2019 @ 11:38 am ET**)

New safety features being rolled out by auto makers to keep drivers from hitting pedestrians don't work at times in some of the most dangerous situations and frequently fail at night, according to a new study by AAA.

Testing performed by the association found that pedestrian-detection technology offered in four different models performed inconsistently and didn't activate properly after dark, when many roadway deaths occur.

The uneven performance highlights the challenges the auto industry faces as it looks to automate more of the car's driving functions and roll out new crash-avoidance technologies that rely on sensors and software to detect road hazards.

"Pedestrian fatalities are really becoming a crisis," said Greg Brannon, AAA's director of automotive engineering. While such pedestrian -detection systems have the potential to save lives, drivers shouldn't become overly reliant on them to prevent accidents, Mr. Brannon said.

Like other advanced safety features becoming more widespread, pedestrian-detection technology uses cameras, radar and other sensors to identify people in the vehicle's path and alert drivers to the danger ahead. If the driver doesn't react quickly enough, the car can brake for them.

Car makers have started to advertise this technology more aggressively, and often it is marketed under different names. For instance, Toyota Motor Corp. offers its pedestrian-detection feature as part of a larger package of crash0-avoidance technologies, called Safety Sense. Honda Motor Co.'s suite of advanced safety features is called Honda Sensing, and it recently highlighted its pedestrian-detection system in a television ad.

Click **HERE** to read more.

Zuckerberg / Voting App

Attorney General Bill Barr Will Ask Zuckerberg To Halt Plans For End-To-End Encryption Across Facebook's Apps

(by **Ryan Mac** and **Joseph Bernstein** | **October 3, 2019 @ 3:28 pm ET)**

Attorney General Bill Barr, along with officials from the United Kingdom and Australia, is set to publish an open letter to Facebook CEO Mark Zuckerberg asking the company to delay plans for end-to-end encryption across its messaging services until it can guarantee the added privacy does not reduce public safety.

A draft of the letter, dated Oct. 4, is set to be released alongside the announcement of a new data-sharing agreement between law enforcement in the US and the UK; it was obtained by BuzzFeed News ahead of its publication.

Signed by Barr, UK Home Secretary Priti Patel, acting US Homeland Security Secretary Kevin McAleenan, and Australian Minister for Home Affairs Peter Dutton, the letter raises concerns that Facebook's plan to build end-to-end encryption into its messaging apps will prevent law enforcement agencies from finding illegal activity conducted through Facebook, including child sexual exploitation, terrorism, and election meddling.

"Security enhancements to the virtual world should not make us more vulnerable in the physical world," the letter reads. "Companies should not deliberately design their systems to preclude any form of access to content, even for preventing or investigating the most serious crimes."

The letter calls on Facebook to prioritize public safety in designing its encryption by enabling law enforcement to gain acess to illegal content in a manageable format and by consulting with governments ahead of time to ensure the changes will allow this access. While the letter acknowledges that Facebook—which owns Facebook Messenger, WhatsApp, and Instagram—captures 99% of child exploitation and terrorism-related content through its own systems, it also notes that "mere numbers cannot capture the significance of the harm to children."

Click **HERE** to read more.

FBI investigating alleged hacking attempt into mobile voting app during 2018 midterms

(by **Kevin Collier** | **October 2, 2019 @ 0001 GMT**)

(CNN) - The FBI is investigating after someone allegedly tried to hack into West Virginia's mobile voting app during the 2018 midterm elections.

One or more people allegedly attempted to hack into Voatz, an experimental app that lets voters who are active military or registered to vote abroad cast their votes from their phones, Mike Stuart, the US attorney for the Southern District of West Virginia, announced Tuesday.

Stuart said in a statement that "there was no intrusion and the integrity of votes and the election system was not compromised," but that an investigation had begun, was "ongoing and no legal conclusions whatsoever have been made regarding the conduct of the activity or whether any federal laws were violated."

West Virginia is the only state that currently allows for the system, though it's been used and is being considered in several cities and counties across the country.

"We just noticed a certain group of people from a certain part of the country tried to access the system. We stopped them, caught them and reported them to the authorities," Voatz co-founder and CEO Nimit Sawhney told CNN.

"Somebody downloaded, registered and then tried to tamper with it, do something. We caught unauthorized activity, and they immediately got stopped," Sawhney said. He said he did not think the culprit was a sophisticated nation-state hacker looking to disrupt the election. Because Sawhney caught the activity last October, and elections are considered critical infrastructure, he felt he needed to report the incident to the FBI.

Click **HERE** to read more.

Google / iPhone Cable

A new Google tool will tell you if your passwords have been hacked

(by **Chris Smith** | **October 2, 2019**)

Google on Wednesday announced new tools meant to enhance user privacy across its products, such as Google Maps incognito mode, YouTube history deletion, and privacy management via Google Assistant. But Google also announced a feature that should enhance your security online by telling you which passwords may have been compromised during security breaches targeting various sites, and advising immediate action.

The feature is hardly new, and Google Chrome isn't the only browser that can help you with password security by offering information about past data breaches that may have affected a certain account. But Google will now include the feature in its password manager app. That means, of course, you'd have to use Google's password manager to save your passwords in order to take advantage of the feature, rather than going for dedicated password managers like 1Password or LastPass.

In addition to informing you about breaches, the password manager will also prevent you from using bad passwords, like "password," or "123456," which is something that people are still doing:

Click **HERE** to read more.

Legit-Looking iPhone Lightning Cables That Hack You Will Be Mass Produced and Sold

(by **Joseph Cox** | **Sep 30 2019, 4:52pm**)

Their creation has been successfully fully outsourced to a factory, the security researcher behind the cables said.

Soon it may be easier to get your hands on a cable that looks just like a legitimate Apple lightning cable, but which actually lets you remotely take over a computer. The security researcher behind the recently developed tool announced over the weekend that the cable has been successfully made in a factory.

"I've completely torn the cable apart to make sure there aren't any production stoppers. Gotta make sure it's up to par!," the security researcher MG told Motherboard in an online chat.

MG is the creator of the O.MG Cable. It charges phones and transfers data in the same way an Apple cable does, but it also contains a wireless hotspot that a hacker can connect to. Once they've done that, a hacker can run commands on the computer, potentially rummaging through a victim's files, for instance.

After demoing the cable for Motherboard at the DefCon hacking conference this summer, MG said "It's like being able to sit at the keyboard and mouse of the victim but without actually being there."

At the time, MG was selling the handmade cables at the conference for $200 each. Now that production process has been streamlined.

"After months of work, I am now holding the very first fully manufactured #OMGCable," MG tweeted on Saturday.

"I'm just being super transparent about the process," MG told Motherboard. "[Mostly] everyone who manufactures something is going to keep it quiet up until release day when they unveil the entire thing and it's ready for sale or they at least have a sale date."

Click **HERE** to read more.

More News

New PDFex attack can exfiltrate data from encrypted PDF files

https://www.zdnet.com/article/new-pdfex-attack-can-exfiltrate-data-from-encrypted-pdf-files/

Malvertiser exploited two browser bugs to show over one billion malicious ads

https://click.email.sans.org/?qs=1cbd2695fcf87a2735de1b21ac66e19d2636b4d10a8cf76a4f5d3ac0c99f694bcde2b817b620349619ffb5d4a658d75da3688faa58639189

Senate Passes Bill Aimed At combating Ransomware Attacks

https://threatpost.com/senate-passes-bill-aimed-at-combating-ransomware-attacks/148779/

NSA launches new cyber defense directorate

https://www.washingtonpost.com/national-security/nsa-launches-new-cyber-defense-directorate/2019/09/30/c18585f6-e219-11e9-be96-6adb81821e90_story.html

Attackers are increasingly using the Open Document (ODT) file type to bypass anti-virus detection

https://blog.talosintelligence.com/2019/09/odt-malware-twist.html

New Research from Absolute Underscores Educational Organizations Vulnerable to Cyber Attacks

https://finance.yahoo.com/news/research-absolute-underscores-educational-organizations-120000673.html

Outlook for Web Bans 38 More File Extensions in Email Attachments

https://thehackernews.com/2019/09/email-attachment-malware.html

Skidmap malware buries into the kernel to hide illicit cryptocurrency mining

https://www.zdnet.com/article/skidmap-malware-buries-into-the-kernel-to-hide-cryptocurrency-mining/

Canadian Centre for Cyber Security Releases Advisory on TFlower Ransomware Campaign

https://cyware.com/news/canadian-centre-for-cyber-security-releases-advisory-on-tflower-ransomware-campaign-388cae50/

Accused Capital One hacker pleads not guilty to all charges

https://www.cyberscoop.com/capital-one-hacker-not-guilty-paige-thompson/

Hit by ransomware? Victims of these four types of file-encrypting malware can now retrieve their files for free

https://www.zdnet.com/article/hit-by-ransomware-victims-of-these-four-types-of-file-encrypting-malware-can-now-retrieve-their-files-for-free/

More News

Researchers Discover New Downloader that Uses Microsoft SQL for Delivering Malware

https://cyware.com/news/researchers-discover-new-downloader-that-uses-microsoft-sql-for-delivering-malware-c5f51bb8

Exclusive - Hacker Steals Over 218 Million Zynga 'Words with Friends' Gamers Data

https://thehackernews.com/2019/09/zynga-game-hacking.html

Baltimore IT department uses 'mind-boggling,' outdated data storage method, audit finds

http://www.baltimoresun.com/politics/bs-md-ci-audit-it-20190927-23hrwbtdyzcu7lmmwdqzbmzja4-story.html

Treasury Targets Assets of Russian Financier who Attempted to Influence 2018 U.S. Elections

https://home.treasury.gov/news/press-releases/sm787

TalkTalk hacker Elliott Gunton: Cryptocurrency auctioned by police

https://www.bbc.com/news/uk-england-norfolk-49880630

Former U.S. Army contractor sentenced to prison for destroying IT system

https://www.cyberscoop.com/army-contractor-sentenced-federated-it/

Cisco warning: These routers running IOS have 9.9/10-severity security flaw

https://www.zdnet.com/article/cisco-warning-these-routers-running-ios-have-9-910-severity-security-flaw/

GAO Identifies Significant Cybersecurity Risks in US Electric Grid

https://cyware.com/news/gao-identifies-significant-cybersecurity-risks-in-us-electric-grid-f8e1700b

Percentage-Based URL Encoding Used by Phishers to Evade Detection

https://www.tripwire.com/state-of-security/security-data-protection/percentage-based-url-encoding-used-by-phishers-to-evade-detection/

Wipers Disguised as Ransomware Have Become a New Weapon for Cybercriminals

https://cyware.com/news/wipers-disguised-as-ransomware-have-become-a-new-weapon-for-cybercriminals-d9e2187f/

Do Not Install iOS 13, United States Department of Defense Says

https://news.softpedia.com/news/do-not-install-ios-13-united-states-department-of-defense-says-527485.shtml

Hackers tried to steal Airbus secrets via contractors: report

https://finance.yahoo.com/news/hackers-tried-steal-airbus-secrets-080551636.html

Reader Suggested Articles

Below are some articles suggested by readers. I hope you find them informative and useful. Thank you ladies for sending me these articles.

From Lauren Meadows:

- https://www.bleepingcomputer.com/news/microsoft/how-to-enable-ransomware-protection-in-windows-10/

How to Enable Ransomware Protection in Windows 10

Windows Defender includes a security feature called "Ransomware Protection" that allows you to enable various protections against ransomware infections. This feature is disabled by default in Windows 10, but with ransomware running rampant, it is important to enable this feature in order to get the most protection you can for your computer.

From Deborah Wright:

- https://www.geekwire.com/2019/amazon-capital-one-face-lawsuits-massive-hack-affects-106m-customers/

Amazon and Capital One face legal backlash after massive hack affects 106M customers

A group of angry customers filed a lawsuit against Capital One this week following the hack that affected more than 106 million people. And they aren't stopping there; the group also named Amazon Web Services, Capital One's cloud provider, alleging the tech giant is also culpable for the breach.

- https://techcrunch.com/2019/08/09/aws-ebs-cloud-backups-leak/2019/08/09/aws-ebs-cloud-backups-leak/

Hundreds of exposed Amazon cloud backups found leaking sensitive data

How safe are your secrets? If you used Amazon's Elastic Block Storage snapshots, you might want to check your settings.

New research just presented at the DefCon security conference reveals how companies, startups and governments are inadvertently leaking their own files from the cloud.

Cyber Challenge

Last Month's Challenge

Congratulations to everyone who was able to solve last month's challenges. I provided ten questions which I thought were interesting and were intended to educate while being fun to solve. Below are the readers who submitted answers along with how many they got correct. Congratulations to these readers because a few of the questions were not easy.

	Completed all 10 Challenges	
Deborah Wright @ 1952 on 10 Sept	Andrew Lott @ 0658 on 11 Sept	Debra Lewis @ 1148 on 11 Sept
Kymberly Hernandez @ 1222 on 11 Sept	Faye Krueger @ 1020 on 12 Sept	Crystal Kaatz @ 1022 on 12 Sept
David Evans @ 1338 on 12 Sept	Scott Smith @ 1625 on 12 Sept	Dariela Maldonado @ 2208 on 12 Sept
Rebekah Lloyd @ 0704 on 13 Sept	Rene Hess @ 0409 on 14 Sept	Kelly Patterson @ 1020 on 16 Sept
Bryce Stringer @ 1157 on 25 Sept	Mercedez-Faye A Wallace-Morrison @ 0840 on 1 Oct	James Kimani @ 1342 on 4 Oct

Completed 8 of 10 Challenges
Cynthia Baughman @ 0946 on 11 Sept

Completed 5 of 10 Challenges
Anne Kirsch @ 1454 on 11 Sept

Completed 4 of 10 Challenges
Michelle Pugh @ 1727 on 10 Sept

Last month's questions and answers can be found on the next page.

Cyber Challenge

Last Month's Challenge Answers

Here are the questions and answers for last month's challenges:

1) I am a bundle of programs that is designed to bombard users with advertisements. The main aim behind it is to redirect the user's search requests to advertising websites and collect marketing data. What am I?

ANSWER: Adware

2) I am a specific type of malware designed to infect several Internet-connected devices such as PCs, mobiles, servers and IoT devices. I am often referred to as a small robot. What type of malware am I?

ANSWER: Botnet

3) While I am a vast network of websites and portals that are not categorized by search engines, I am a smaller section where lots of illegal activities occur. What am I?

ANSWER: Dark Web

4) I am a non-malicious surprise embedded in a program or media which is entertaining and accessible to anyone. I am often found in video games and even in movies. I am an intentional joke intended to be amusing to everyone who finds me. What am I?

ANSWER: Easter Egg

5) I am a fraudulent Wi-Fi hotspot or access point that appears to be legitimate but is setup to eavesdrop on wireless communications. I am the wireless equivalent of a phishing scam. What am I?

ANSWER: Evil Twin

6) I am the measure of difficulty an attacker has to guess in order to crack the average password using a system. The lower I am the easier it is to guess a password. The higher I am the more difficult it is to guess a password. What am I?

ANSWER: Entropy

7) I am a thing that is designed to record everything you do on your computer, phone, tablet, etc. I record every interaction and can either send that data on my own to a remote location or wait to have it requested. I can be either software or hardware. What am I?

ANSWER: Keylogger

8) I am a sort of Phishing which has become a major threat to all e-commerce websites. I redirect a user to a fake site which appears to be a genuine one. A user enters all their credentials into the duplicate site considering it to be a legitimate site. What type of phishing attempt am I?

ANSWER: Pharming

9) I am a term used to describe a new hacker/cracker. I do not have enough skill to write my own exploits and often have no idea how the exploit works. I use scripts developed by other hackers to cause the mischief I create. I am called what?

ANSWER: Script Kiddie

10) I am an industry best practice and the best protection an organization has to recover from ransomware. Ransomware can happen no matter how vigilant an organization is. However, if I have been done and tested, an organization is often able to recover very quickly with little to no cost to the organization. What am I?

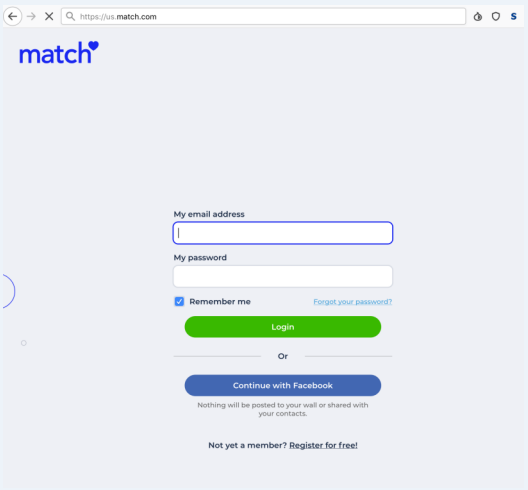
ANSWER: Backups

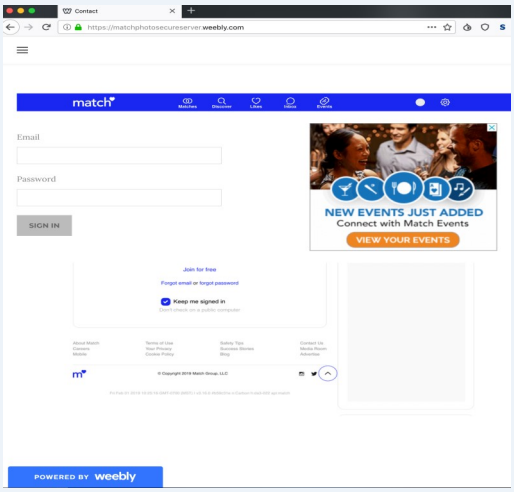
Cyber Challenge

This Month's Challenges

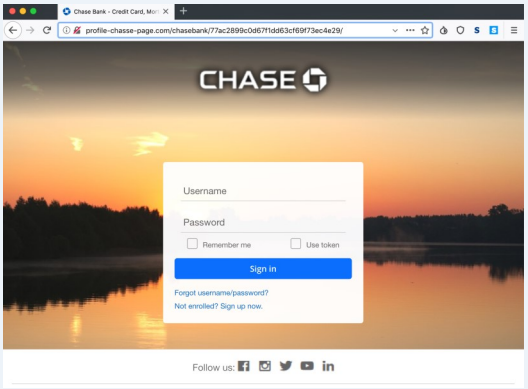
This month the challenges are based on identifying phishing attempts. The first two challenges are to identify the phishing website, and how you determined it was. The third is to identify if it is a phishing site or not and why. There is a hidden 4th challenge. Remember you can always ask for hints. Good luck with the challenges.

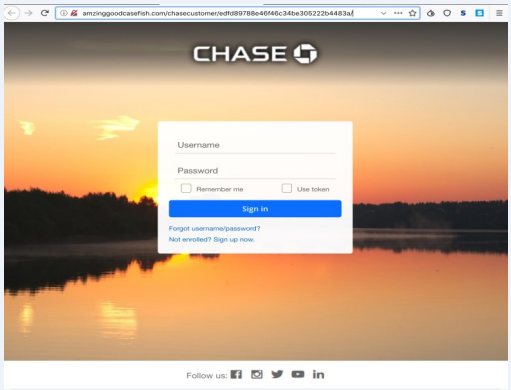
1)



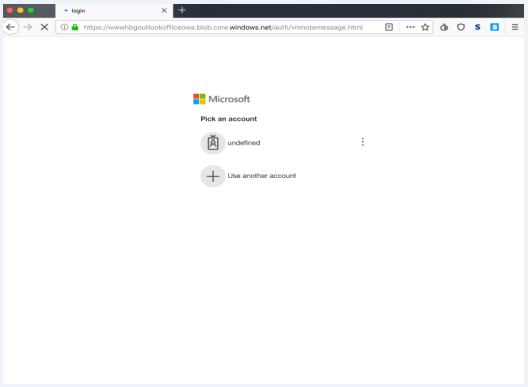


2)





3)



</Closing Comments>

As always, thank you for taking the time to read the newsletter. I 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. I hope you have enjoyed reading this newsletter and it has given you things to think about.

In closing I was asked by one of our CID Agents, Erich Neumann, to warn people about a targeted phishing scam he has been investigating. The scam seems to be targeting Texas state agency heads. We have noticed it at DPS but other state agencies might be unaware and should be watching for this scam. Here is what Erich provided me:

The e-mails come from myoffic@sc.rr.com, myofice@sc.rr.com, myoffice1@dc.rr.com, myoffice@bak.rr.com, do@sc.rr.com, or doo@sc.rr.com, though the sender's name is spoofed to display as the agency head in question. In the case where the scammers were successful and a loss was sustained the recipient noticed the non-agency return address but assumed it was a personal e-mail address.

The body of the e-mail is always the same, indicating probable use of a script to generate them:

[recipient],I need to update my pay check direct deposit information for my next paycheck. Please can we handle it

now ?

Thanks

[Name of Agency Head]

Sent from my iPhone

There is no space between the comma and the I, and no comma after "Thanks" and the recipient is always addressed by first name only in the body of the message. The "Sent from my iPhone" is just as likely to be intended as a way to allay concerns over the fact that the e-mails are not formatted as they would be when sent via internal e-mail as they are an actual indication of the source device. Responses also receive similarly identical apparently automatically generated e-mails in return, but any subsequent messages appear to be actually written by the scammers as by this point the responses need to be specific to the e-mail thread in question and they've already got the target on the hook.

So far there hasn't been any supposed sender who hasn't been an agency head, apparently leveraging their authority in combination with using the target's first name to lure in the recipient.

It would appear that DPS is well protected as the attempts here, at least so far, have failed. Other agencies have not been so lucky, and many others have been targeted, so I'm interested in pushing this out to other agency IT/Cyber people to be aware of as well.

Again thank you for taking the time to read 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

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.

Kirk

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