Vol. 3 | Issue 12

Cyber Security NEWS

December 2018

Hello everyone and welcome to this month's TXDPS Cyber Newsletter.

Merry Christmas and Happy Holidays to everyone. Hope everyone had a great Thanksgiving and that you are enjoying your time with friends and family this holiday season.

While this is supposed to be a time of Peace and Goodwill towards everyone, it is also the time when criminals and grifters are most active. These unscrupulous people prey on the kindheartedness of people during the holiday season. You need to be wary of people trying to pick-pocket you in malls as well as be aware of scams that pretend to be for a good cause. Extra vigilance will help keep you and your loved ones safe. This includes while shopping online.

In last month's newsletter I included a tutorial from our operations section on how to encrypt email to keep your communications secure. This month I want to post some information about Two Factor Authentication (also known as 2FA) and how this can better protect you. On Wednesday 12 December 2018 at 5 pm, DPS activated 2FA to access DPS Webmail. **To clarify, the 2FA for DPS email is only for accessing email when NOT on TLE and when NOT using a VPN. You will not have to use 2FA when connected to the DPS network.** Employees should have seen the email sent out about this new procedure. If you missed the emails, don't worry…..I included it in the next couple of pages. :)

Because of data breaches, use of insecure passwords, reusing passwords, etc, the standard use of a username and password is no longer enough to safely authenticate you online. 2FA is a much better way to authenticate you and protect you from people trying to steal your money, identities, etc while online. It is fast becoming the industry standard for online authentication for businesses and websites. The following articles will educate you on what 2FA is, how it is used, and why you should be using it as much as possible.

- What Is Two-Factor Authentication (2FA)?
- Here Are All The Sites You Should Enable Two Factor Authentication on (And The Ones You Should Yell At)
- Two Factor Auth (2FA)

Stay vigilant when you are shopping and while online this holiday season. Be very careful of anything that sounds too good to be true. Remember it is a bad idea to post your location or notify people you are out of town on social media. Criminals look for these types of notifications to target houses to break into. A little paranoia is rarely a bad thing when it comes to security. Be safe, Merry Christmas and Happy Holidays from me and your Cybersecurity team.

2FA Procedure

Outlook Web Access (OWA) Multifactor Authorization Enrollment/Registration Procedure

Audience: Any User accessing Outlook Web Access (DPS Webmail) outside of a DPS network (**i.e. not on TLE and not using a VPN to connect to TLE**)

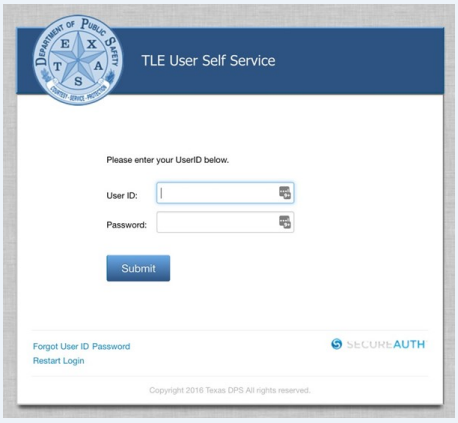
Purpose: This document lays out the step by step procedure for current Outlook Web Access users to migrate to the new Advanced Authentication for Outlook Web Access.

The process steps in this document are summarized below:

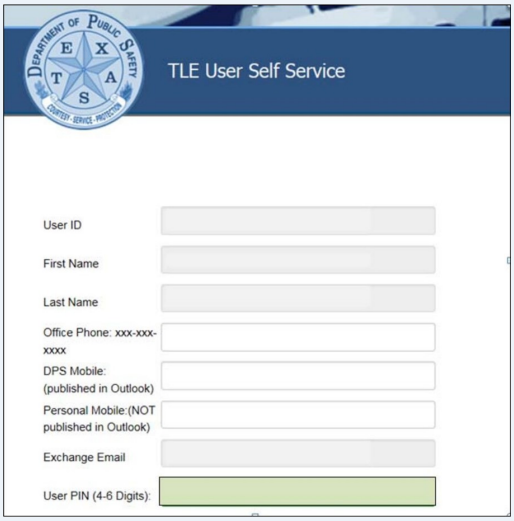
Update User Information

Users will first either verify or enter appropriate information at https://tleidupdate.tle.dps. You will have the opportunity to add/update your personal **and/or work mobile phone number** and **provide answers to several knowledge based questions**. This is critical information to have in order for the multifactor authentication process to work.

Navigate to https://tleidupdate.tle.dps. Log in with your DPS ACID and password.



This will direct you to the page where you will fill out your contact information. You will also choose and answer several security questions



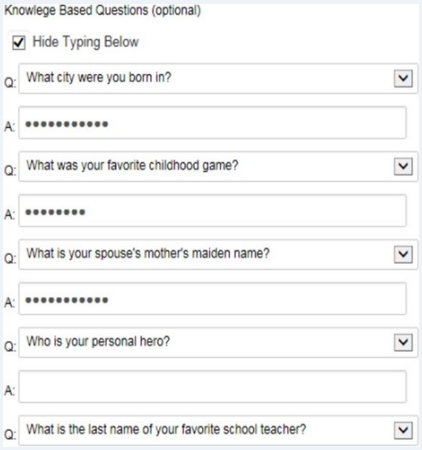
2FA

Verify/Enter phones that can receive texts or messages – Use format: XXX-XXX-XXXX

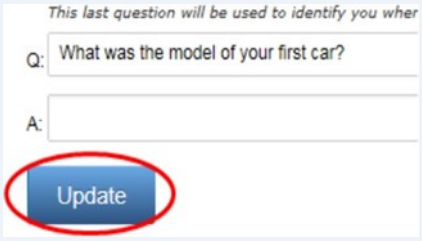
- Office Phone
- DPS Mobile – should be DPS issued phone – this number will be published in Outlook
- Personal Mobile – will not be published in Outlook

Answer at least 3 of the Knowledge Based Questions

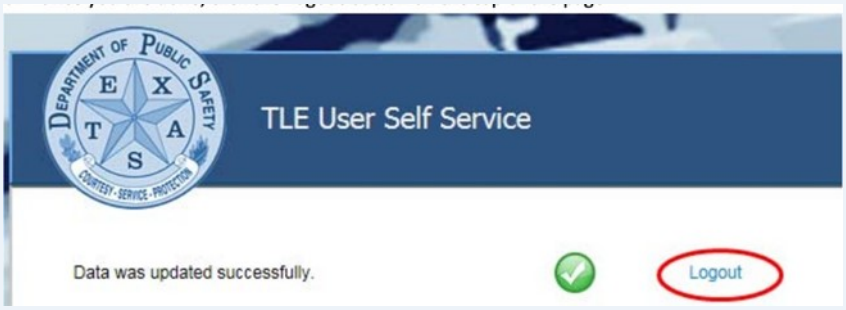
- **Note: Three must be answered even though it states that they are optional**



Once you are done, click on the Update button to continue



Once you are done, click the Logout button on the top of the page



It may take up to 24 hours for information to go live.

Worst Cyber Attacks

The worst cyber attacks of the past 10 years

(by **Jade Scipioni** | Published December 04, 2018 | **Personal Finance** | **FOXBusiness)**

While news of Marriott's and Quora's massive data breaches have made the media rounds over the last weeks - - affecting a combined 600 million users - - the breaches still pales in comparison to others, especially Yahoo's breach in 2016 that exposed 3 billion users.

Over the last 10 years, there have been eight major cyber attacks that compromised data of more than 100 million people.

Here are the top cyber attacks over the last decade.

1. Yahoo!

Impact: 3 billion user accounts

In September 2016, the internet giant announced it had been the victim of the biggest data breach in history. The company said the attack compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. Then a couple months later, it revealed a different group of hackers compromised 1 billion accounts.

2. Marriot - Starwood Hotels

Impact: 500 million/guests/accounts

On November 30, 2018, the hotel empire revealed a security breach with its Starwood Hotel brands that may have compromised the data of as many as 500 million guests.

3. Adult Friend Finder

Impact: More than 412.2 million accounts

In October 2016, the website said hackers were able to gain access to more than 20 years of data on its six databases that included names, email addresses and passwords.

4. Under Armour - MyFitnessPal

Impact: 150 million user accounts

In February 2018, the sports apparel brand Under Armour disclosed that a hacker gained access of email addresses and login information to 150 million users of its food and nutrition website, MyFitnessPal.

5. eBay

Impact: 145 million users

In May 2014, eBay announced that hackers got into the company network using the credentials of three corporate employees and had complete inside access for 229 days, during which time they were able to collect personal information of all of its 145 million users.

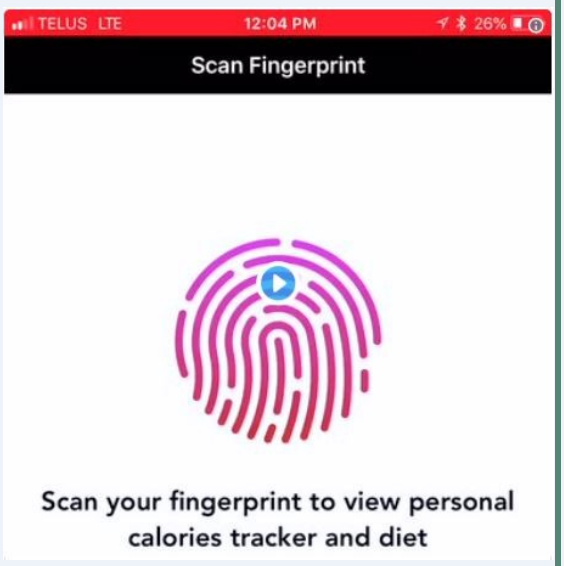
Click **HERE** to read the article.

Touch ID / Russian

App Store scammers are using Touch ID tricks to steal money

(by **Saqib Shah, @eightiethmnt** 12.04.18 in **Security**)

Reddit users are exposing shady iOS fitness apps that use the Touch ID feature on iPhones and iPads to scam people out of cash. Both "Fitness Balance app" and "Calories Tracker app" were active on the App Store until recently, though Apple appears to have now removed them.



Like their genuine counterparts, they promised to calculate your BMI, track daily calorie intake, or remind you to drink more water. But they also used a cunning, but downright fraudulent, trick tied to the iOS Touch ID sensor. While asking to secure your personalized diet data by scanning your fingerprint, the apps would display a pop -up showing a payment of $119.99. With just seconds to act, the scam could easily see users inadvertently handing over money from their connected credit or debit cards.

It seems people reported the apps to Apple, which likely led to their removal, though Apple itself hasn't released an official statement on the takedowns. According to *WeLiveSecurity*, the "Fitness Balance app" has an average rating of 4.3 stars, and received at least 18 mostly positive reviews, which may well have been faked.

Click **HERE** to read more.

Russian Hackers Allegedly Attacked Germany and the U.S. on the Same Day

(by **Max de Haldevang**, Quartz, December 3, 2018)

Russian hackers seem to have been busy on Nov. 14.

Separate reports have tied the country's hackers to attacks on officials in both the U.S. and Germany on the same day. It's unclear if the events were linked.

First, U.S. cybersecurity companies repoted that the group known as Cozy Bear - allegedly an arm of Russia's foreign intelligence service, best known for being the first Russian hacking team to infiltrate the Democratic National Committee - seemed to have come back to life. The group was the likely source of new hacking attempts on U.S. government agencies, think tanks, and businesses, the companies said. The emails purported to contain files from senior State Department official Heather Nauert, but they actually held malicious software.

Click **HERE** to read .

Chrome / Facebook

Cyber-espionage group uses Chrome extension to infect victims

(by **Catalin Cimpanu** for **Zero Day** | December 5, 2018 - -15:00 GMT (07:00 PST)**)**

Suspected North Korean APT uses Google Chrome extension to infect victims in the academic sector.

In what appears to be a first on the cyber-espionage scene, a nation-state-backed hacking group has used a Google Chrome extension to infect victims and steal passwords and cookies from their browsers.

This is the first time an APT (Advanced Persistent Threat - - an industry term for nation-state hacking groups) has been seen (ab)using a Chrome extension, albeit it's not the first time one has used a browser extension, as the Russian-linked Turla APT previously used a Firefox add-on in 2015.

Click **HERE** to read more.

Nearly 250 Pages of Devastating Internal Facebook Documents Posted Online By UK Parliament

(by **Jason Koebler** and **Joseph Cox** | Dec 5 2018, 3:23pm)

The documents include emails between Mark Zuckerberg and Sheryl Sandberg about the company's business model and how it leverages your data to make money.

Facebook really didn't want this to happen. On Wednesday, a British politician who has been highly critical of the social media giant publicly dumped a huge cache of sensitive internal Facebook documents for anyone to download and read.

The documents include details on the distribution of Facebook's various apps; how the company worked very closely with some app developers to grant them access to user data, and how the company specifically incentivizes sharing on the platform in order to feed that data back to advertisers. They also include information about how the company tried to hide and downplay the amount of data that it collected from the Android version of the Facebook app.

The documents also include emails between top company executives, including COO Sheryl Sandberg and CEO Mark Zuckerburg.

"Facebook knew that the changes to its policies on the Android mobile phone system, which enabled the Facebook app to collect a record of calls and texts sent by the user would be controversial," a summary of the documents written by Damian Collins, Conversative MP and Chairman of the Digital Culture, Media and Science Committee who published the documents, reads. "To mitigate any bad PR, Facebook planned to make it as hard of possible for users to know that this was one of the underlying features of the upgrade of their app."

The news signals an escalation in the fallout around Facebook's Cambridge Analytica and data sharing scandals, which have irked European politicians in particular.

Collins tweeted a link to the documents, which are hosted on Parliament's official website.

Click **HERE** to read more.

Printers / ATMs

Hacker hijacks 50,000 printers urging them to subscribe to PewDiePie's YouTube channel

(by **E Hacking News** on Wednesday, December 05, 2018)

A hacker took the whole sole responsibility of hijacking over 50,000 printers worldwide to print a message to subscribe to PewDiePie's YouTube channel, which is the most-subscribed channel on YouTube.

Youtuber Felix Kjelberg owns the top channel for years now, but his position has been threatened by a channel T-Series, which is owned by a music production company in India. The growth rate of a subscriber of the music channel has been explosive in 2018, it has over 72 million subscribers while PewDiePie has 150,000 fans. Many analytics think that T-Series' subscriber would soon overthrow PewDiePie from its position, but Kjellbeg's fans are putting up a fight.

The Twitter handle, TheHackerGiraffe, tweeted about the attack in a Reddit AMA that reads, 'I hacked 50,000 printers worldwide out of potential 800,000 for PewDiePie and security awareness.'

Click **HERE** to read more.

Hackers using a new method for stealing money from ATM

(by **E Hacking News** on Tuesday, December 04, 2018)

Hackers create a new method of stealing money from ATMs. As a result, they remain elusive to law enforcement.

According to Kaspersky Lab, the method was named KoffeyMaker. Hackers opened the chosen ATM and connected their laptop with the official KDIAG program to it via a USB cable. This program is used to test the performance of the dispenser issuing money.

After first step, the attackers left the laptop inside the ATM, closed it and left. The interesting thing is that the ATM dispenser perceived the laptop as one of its own parts.

Further, the hackers remotely run the modified version of the program KDIAG on their computer, after which the ATM gave all the money to criminals. And after some time they took their laptop from ATM.

It should be noted that cyber security professionals in recent years have more and more questions about ATMs. Experts of Positive Technologies recently revealed the vulnerability in 26 models of ATMs produced by Diebold Nixdorf, NCR and GRGBanking. Due to this fact the attackers in 15 minutes can steal not only personal data of customers, but also money. (http://www.ehackingnews.com/2018/11/many-atms-can-be-compromised-within-30.html)

According to Prosecutor General's Office of Russia, this year a sevenfold increase in the number of frauds using electronic means of payment was recorded. The results are not encouraging. Last year, only 1,883 such crimes were registered, but in the first half of this year, the number of offenses already reached 1,233.

Click **HERE** to read more.

More News

This phishing scam group build a list of 50,000 execs to target

https://www.zdnet.com/article/this-phishing-scam-group-built-a-list-of-50000-execs-to-target/

Quora Gets Hacked - 100 Million Users Data Stolen

https://thehackernews.com/2018/12/quora-hack.html

Pied Piper phishing scheme infests victims with FlawedAmmyy, RMS RATs

https://www.scmagazine.com/home/security-news/pied-piper-phishing-scheme-infests-victims-with-flawedammyy-rms-rats/

Free Airport Wi-Fi: A Tempting Cyber-Trap!

http://www.ehackingnews.com/2018/12/free-trap-did-youthink-airport-wi-fi.html

Hackers targeted Dell customer information in attempted attack

https://www.engadget.com/2018/11/29/dell-hack-attempt/

Little FYI: Wi-Fi calling services on AT&T, T-Mobile US, Verizon are insecure, say boffins

https://www.theregister.co.uk/2018/11/30/wifi_calling_services_insecure/

Here are another 45,000 reasons to patch Windows systems against old NSA exploits

https://www.theregister.co.uk/2018/11/30/akamai_routerwreckers_active/

Alleged crypto-crook CEO cuffed by FBI after $4m investment in his bank bafflingly vanishes

https://www.theregister.co.uk/2018/11/29/arisebank_funds_arrest/

Viral Facebook Hoax Messages Prompts Warning From Officials

https://philadelphia.cbslocal.com/2018/11/28/viral-facebook-message-hoax-prompts-warnings-from-officials/

OneDrive is broken: Microsoft's cloudy storage drops from the sky for EU users

https://www.theregister.co.uk/2018/11/29/microsoft_onedrive_down/

</Closing Comments>

User Suggested:

This month's suggested articles come from Stephen "Doc" Petty and Deborah Wright. Thank you very much for sending me the articles. Hopefully our readers will find these articles as interesting as I did.

Here are the articles:

How to fit all of Shakespeare in one tweet (and why not to do it!)

https://nakedsecurity.sophos.com/2018/11/12/how-to-fit-all-of-shakespeare-in-one-tweet-and-why-not-to-do-it/?utm_source=Naked+Security+-+Sophos+List&utm_campaign=75cf373b96-Naked+Security+daily+news+email&utm_medium=email&utm_term=0_31623bb782-75cf373b96-455012257

Ransomware Suspects Indicted

https://www.fbi.gov/news/stories/iranian-ransomware-suspects-indicted-112818?utm_medium=email&utm_source=fbi-top-stories

9 Ideas for Cyber Security Awareness Month

https://thecybermaniacs.com/2018/08/20/9-ideas-cyber-security-awareness-month/

If you find articles you think would be of interest to me and our readers, please email them to me. I will share them with the readers but will not post your name if you ask me not to.

Thank you for taking the time out of your busy schedule to read the articles in this month's newsletter. I hope you found all of them to be interesting and useful. Remember, you can only defend yourself against threats when you are knowledgeable about the threats. I realize cybersecurity is not the most liked topic by most people, but it is important to understand the dangers you and your family face when being online and how your actions and the actions of others can affect the Agency. Knowing about cyber dangers are all part of Cybersecurity Awareness Continuation Training. Everyone in the Agency has to take Cybersecurity Awareness training every two years, but the learning does not end when the online training is over. My hope is this newsletter provides a little more up-to-date information about Cybersecurity as well as making it a little more enjoyable than watching generic training videos online. Feedback on how to improve the newsletter is always appreciated, so feel free to email me with suggestions. If possible, I will implement them in future editions.

As I mentioned above, everyone has to take the online training every two years. I send out notifications monthly to people when it is time for their retraining. If you know you are coming up on your two year mark, please be on the lookout for the email. If you are unsure, feel free to email me and I will let you know when you are due retraining.

In closing, hope you enjoyed the newsletter and good luck with the Cyber Challenge on the next page. And as always, **Do Good Cyber!**

Kirk

Cyber Challenge

Last Month's Challenge

Last month's challenge had a few more people complete than the previous month, but not as many as I had hoped for. There were a total of 5 challenges to find and figure out. **Jaelyn Edwards** completed the 2 hardest challenges and emailed me on 17 Nov. **Erich Neumann** completed 3 of challenges and emailed me on 14 Nov. Three other people were able to find and complete all 5 challenges. Those people were:

Deborah Wright @ 1604 on 14 Nov	**Tracy Kingsley @ 1118 on 15 Nov**	**Rene Hess @ 1755 on 20 Nov**

Congratulations to everyone who was able to complete any of the challenges.

For this month's challenge you will need to use a couple of the things I have talked about in previous newsletters to come up with the answer. For your first clue, I am giving you a QR Code. You will need it to help determine the answer to the question I'm asking. Once you get the answer, email me so I can recognize you in next month's newsletter. If you get stumped…..email me and I'll help point you in the right direction.

GOOD LUCK with the challenge.
Kirk