Cyber Security NEWS
Vol. 4 | Issue 11
November 2019

TXDPS Cyber Newsletter

DPS 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.

As everyone is well aware, we are in the holiday season. Halloween just passed, Thanksgiving, Christmas and New Years are coming up. Everyone will be spending time with friends and family and doing lots of shopping. This is a joyous time of year where people celebrate what is good in their life and show respect and love for their fellow man. However, it also brings out the darker side of humanity. It is the favorite time of year for scammers, phishers and others trying to steal your money.

Unscrupulous people prey on the kindheartedness of people during this time of year. You need to be wary of people trying to pick your pocket in the mall, but also wary of online scams. Fake charities will try to scam you out of your money. Phishing sites that look a LOT like the legitimate site will try to steal your money and/or identity. Extra vigilance will help keep you and your loved ones safe.

Listed below are some basic things you should do with all of your computers to keep yourself and your loved ones safe online year round, not just during the holiday season.

- Keep your Operating System up to date. Do the security updates and reboot your computers.
- Update programs and apps so any patches to the program are secured. This is just as important as keeping the security updates to your Operating System up to date.
- Have an anti-virus program and keep it up to date. (other free AV for Windows for Mac)
- Never use your work email as a username for personal sites.
- Use complex passwords, pass phrases, or a good password manager.
- Never use your work password for any other site.
- Try to avoid using passwords or pass phrases on more than one device or site.
- Enable Two Factor Authentication (2FA/MFA) on any website you visit if they have the capability. Enabling this will help prevent unauthorized access and someone buying stuff as you.
- Use a Virtual Private Network (VPN) if you are attaching to a free WiFi. Also a good idea if you are using WiFi on a private network. Using one will help prevent what is known as a Man-in-the-Middle attack.

These tips are valid for ALL computers. This means desktops, laptops, tablets, AND phones. All of these, and more, are computers. If it can store data then it should be thought of as a computer. Most people do not understand this and think their phones and tablets are safe and do not need anti-virus software and do not need to have security updates installed. If you do not have an anti-virus program on these devices, I strongly encourage you to install one. If you have a Mac or Android device and do not have an up to date anti-virus program, you are playing Russian Roulette.

I provided hyperlinks to resources related to the best practices listed above. If you have additional questions or need to ask personal advice, please feel free to email me.

We hope everyone has a happy and safe holiday season!

Siri / Android

Researchers hack Siri, Alexa, and Google Home by shining lasers at them

(by **Dan Goodin | 11/4/2019, 12:00 PM**)

MEMS mics respond to light as if it were sound. No one knows precisely why.

Siri, Alexa, and Google Assistant are vulnerable to attacks that use lasers to inject inaudible—and sometimes invisible—commands into the devices and surreptitiously cause them to unlock doors, visit websites, and locate, unlock, and start vehicles, researchers report in a research paper published on Monday. Dubbed Light Commands, the attack works against Facebook Portal and a variety of phones.

Shining a low-powered laser into these voice-activated systems allows attackers to inject commands of their choice from as far away as 360 feet (110m). Because voice-controlled systems often don't require users to authenticate themselves, the attack can frequently be carried out without the need of a password or PIN. Even when the systems require authentication for certain actions, it may be feasible to brute force the PIN, since many devices don't limit the number of guesses a user can make. Among other things, light-based commands can be sent from one building to another and penetrate glass when a vulnerable device is kept near a closed window.

The attack exploits a vulnerability in microphones that use micro-electro-mechanical systems, or MEMS. The microscopic MEMS components of these microphones unintentionally respond to light as if it were sound. While the researchers tested only Siri, Alexa, Google Assistant , Facebook Portal, and a small number of tablets and phones, the researchers believe all devices that use MEMS microphones are susceptible to Light Commands attacks.

Click **HERE** to read the article.

Hackers Can Use NFC To Plant Malware On Your Android Smartphone

(by **Kavita Lyer | November 4, 2019**)

Smartphones running Android 8.0 (Oreo) or above are impacted by a bug, tracked as CVE-2019-2114, that allows hackers to plant malware on nearby devices via NFC beaming discreetly.

However, Google recently released a patch to address this vulnerability.

For those unaware, NFC (Near Field Communication) beaming works via an internal Android OS service known as Android Beam. Android Beam allows data to be transferred between two devices via NFC radio waves and also allows the rapid short-range exchange of web bookmarks, contact info, directions, YouTube videos, and other data.

Normally, when apps (APK files) are transferred via NFC beaming, they are stored on disk and a notification is displayed on the screen. The prompt asks the device owner for permission to allow the NFC service to install an app from an unknown source.

In January this year, security researcher Y. Shafranovich discovered that APK files sent via NFC beaming on Android 8 (Oreo) or later versions would not display any security notification to the users Instead, the notification would allow the user to install the app from unknown source with just one tap, without asking for any explicit security permissions.

Usually, Google displays a security warning when you install apps from unknown sources, as any app installed from outside the official Play Store is considered untrusted and unverified. However, certain services like Google Chrome and Dropbox Android app receive the same level of trust as the official Play Store app, and can be downloaded without being blocked..

Click **HERE** to read the article.

Russian Hacker / Facebook

RUSSIAN HACKER, NA'AMA ISSACHAR ASK HIGH COURT TO BLOCK U.S. EXTRADITION

(by **Yonah Jeremy Bob** | **November 3, 2019 21:40**)

A Russian hacker and an Israeli woman in an Russian prison for cannabis possession on Sunday both requested the High Court of Justice block the hacker's extradition to the US.

The family of Na'ama Issachar, who is serving a seven-and-a-half-year sentence in Russia for possession, filed their petition at the end of last week, while the hacker, Alexei Burkov, filed a petition on Sunday.

These moves allowed Acting Justice Minister Amir Ohana's signing the extradition order to send Burkov to the US for perpetrating cyber fraud. There were also prior rulings by the Jerusalem District Court and the Supreme Court to extradite him.

Generally, the petitioners oppose any extradition, but given the current state of legal play, they are pushing for extradition to Russia rather than the US, as part of a package deal for Russia to return Issachar to Israel.

Israelis generally view Issachar as having violated the law, but sense that the violation was itself was minor and the seemingly heavy Russian jail sentence was a political move to try to press Israel into returning Burkov to Moscow.

In a bizarre legal twist unique to the extradition process, though the Supreme Court already ordered Burdov's extradition, he has a second opportunity to object after the justice minister signs the extradition order by addressing his petition to the same body, but in its capacity as the High Court of Justice.

Click **HERE** to read more.

Facebook says 100 software developers may have improperly accessed user data

(by **Salvador Rodriguez** | **11/5/2019 @ 4:15 PM CST**)

KEY POINTS

- Facebook discloses that as many as 100 software developers may have improperly accessed user data, including the names and profile pictures of people in specific groups on the social network.
- Facebook says that at least 11 developer partners accessed this type of data in the last 60 days.

Facebook on Tuesday disclosed that as many as 100 software developers may have improperly accessed user data, including the names and profile pictures of people in specific groups on the social network.

The company recently discovered that some apps retained access to this type of user data despite making changes to its service in April 2018 to prevent this, Facebook said in a blog post. The company said it has removed this access and reached out to 100 developer partners who may have accessed the information. Facebook said that at least 11 developer partners accessed this type of data in the last 60 days.

"Although we've seen no evidence of abuse, we will ask them to delete any member data they may have retained and we will conduct audits to confirm that it has been deleted," the company said in the blog post.

The company did not say how many users were affected.

Click **HERE** to read more.

Texas / Trump

Texas Updates Data Breach Notification Requirements

(by **Gregory Bautista** and **William Douglas Sanders** | **November 1, 2019)**

Effective January 1, 2020, the Texas legislature will impose new notification requirements on businesses that maintain personal information of customers. House Bill 4390 amends the Texas Identity Theft Enforcement and Protection Act by requiring that Texas residents be notified of a data security breach **within sixty (60) days** of the determination that a breach has occurred. A "breach of system security" is defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data." This Amendment marks a substantial departure from section 521.053(b) of the former law, which only required that businesses notify impacted individuals "as quickly as possible" - in effect allowing businesses greater flexibility in reporting a given data security incident.

Additionally, if a breach impacts more than **250 Texas residents**, the business responsible for maintaining the sensitive personal information must provide notice of the incident to the Texas Attorney General within the same 60-day time period that governs notification of Texas residents.

The notification to the Texas Attorney General must include the following information:

- A detailed description of the breach or the use of sensitive information acquired during the breach
- The number of Texas residents affected
- Measures taken to date regarding the breach
- Any measures that will be taken in the future regarding the breach
- An indication of whether law enforcement has been notified.

Click **HERE** to read more.

Fake ransomware named after Donald Trump tried to trick victims out of a buck

(by **Jeff Stone** | **NOV 5, 2019**)

Donald Trump can add ransomware to the list of things named after him, thanks to scammers who again have demonstrated how current events create opportunities to steal data.

Security researchers from Cisco's Talos threat intelligence team on Tuesday published findings explaining how hackers are using the likeness of the president, his predecessor and other political figures to dupe victims into paying up. Numerous ransomware attacks, screenlockers and remote access Trojans are named after Trump, Barack Obama, Hillary Clinton and Vladimir Putin. It's the latest evidence that digital miscreants will use any trending topics to woo potential victims.

"One of the unexpected aspects of the investigation was the presence of lures that dropped malware associated with multiple nation-state attacks in the past, showing how even advanced, sophisticated adversaries will use any means to achieve their nefarious goals," researchers wrote.

The scammers' emails mention the world leaders to catch victims' attention, or the malicious files themselves contain references to Trump or the others. One message that appeared to be from the director of global risk from Visa alerted recipients to an apparent fraud alert. Instead of including information about fraud prevention, though, the files has malicious email attachments with names like "trump.exe".

Click **HERE** to read more.

Joker's Stash / Phishing

Joker's Stash, once a forum for credit data, grows as breaches yield more stolen data

(by **Jeff Stone** | **OCT 24, 2019**)

If it's possible to describe a cybercriminal marketplace as "reputable" while maintaining a straight face, then Joker's Stash fits the description as well as any other.

The site has emerged in recent years as a destination for scammers who buy and sell credit card information stolen after data breaches from victims including the Hy-Vee supermarket chain, Sonic Drive-In and others. Now, the site has expanded to include an array of personal information on high-value targets, including members of the Trump administration, as part of an evolution toward making illicit transactions more user friendly, according to research published Thursday by threat intelligence firm Recorded Future.

It's also available without the use of Tor, the well-known anonymity software that unlocks websites not accessible with mainstream web browsers.

Researchers who explored Joker's Stash following reports that information stolen from Hy-Vee had been made available also found a new section dedicated entirely to Social Security numbers, which personal details available for $5 per record and searchable by name, birth data, or victim location. The expansion came amid a new marketing campaign, with Joker's Stash operators advertising the site on Twitter, Reddit, and other carding forums. (Those advertisements don't appear to have generated much attention, as the Joker's Stash Twitter page has a mere eight followers and few, if any, interactions.)

Click **HERE** to read more.

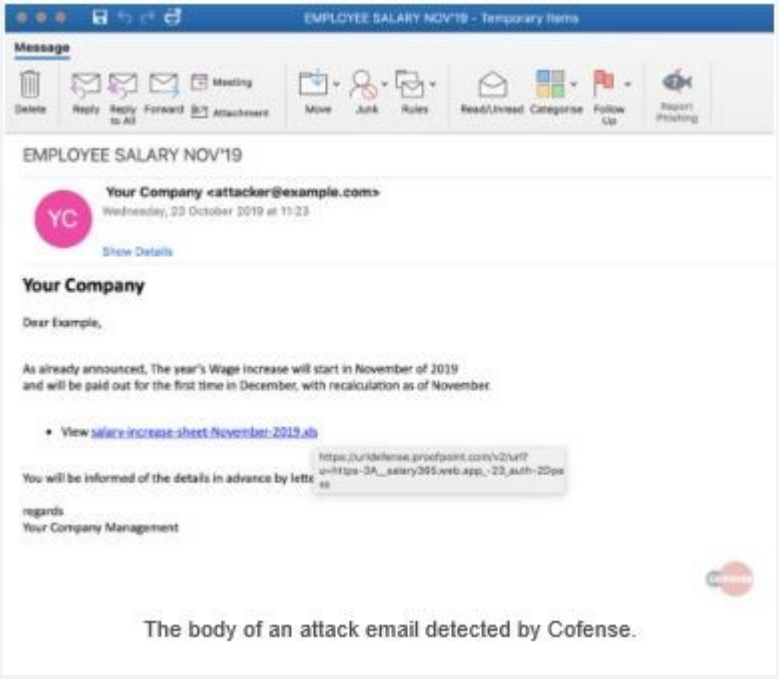
Fraudsters Use Salary Increase Scam to Steal Employees' Credentials

(by **David Bisson** | **NOV 1, 2019**)

Digital fraudsters have launched a new phishing campaign that uses a salary increase scam to trick employees into handing over their credentials.

Spotted by Cofense Phishing Defense Center, the campaign used spoofing techniques to trick recipients into thinking that the attack emails came from their HR department. Those emails claimed that the recipient's wages would increase as part of a larger organization-wide effort to raise salaries in November 2019 and begin paying out these increases the following month. In support of this ruse, the emails came with an embedded link to what it claimed was a spreadsheet detailing employees' raises.

Ultimately, the salary increase scam campaign transported the user to a phishing landing page hosting a fake Office 365 login portal. The URL for this page appended the user's email address and leveraged this information to auto-populate the form's "email" text field. The campaign then prompted the user to enter their password.



The body of an attack email detected by Cofense.

Click **HERE** to read more.

More News

32,000+ WiFi Routers Potentially Exposed to New Gafgyt Variant

https://www.darkreading.com/iot/32000+-wifi-routers-potentially-exposed-to-new-gafgyt-variant/d/d-id/1336238

Cyber-attack hits Utah wind and solar energy provider

https://www.zdnet.com/article/cyber-attack-hits-utah-wind-and-solar-energy-provider/

China-backed hackers stole text messages and phone records in push for intelligence, report says

https://www.cnbc.com/2019/11/01/chinese-hackers-stole-text-messages-phone-records-in-intelligence-push.html

New Google Android Threat: Malicious App Installed By 40 Million Play Store Users

https://www.forbes.com/sites/kateoflahertyuk/2019/10/30/new-google-android-threat-malicious-app-installed-by-40-million-play-store-users/#5ae2e04f511e

Subpoena Phishing Emails Serve Nasty Predator Thief Infection

https://www.bleepingcomputer.com/news/security/subpoena-phishing-emails-serve-nasty-predator-thief-infection/

Shadow Brokers data dump tipped researchers off to a mysterious APT dubbed DarkUniverse

https://www.cyberscoop.com/darkuniverse-kaspersky-apt-shadow-brokers/

Leaked documents show Facebook leveraged user data to fight rivals and help friends

https://www.nbcnews.com/news/all/leaked-documents-show-facebook-leveraged-user-data-fight-rivals-help-n1076986

Microsoft Defender ATP Gets Advanced Hunting Capabilities, More

https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-atp-gets-advanced-hunting-capabilities-more/

Hackers who tried extorting Uber, Lynda plead guilty

https://www.cyberscoop.com/uber-hackers-plead-guilty-lynda/

Banking Apps Blacklisted Samsung Galaxy S10 After Fingerprint Vulnerability Was Exposed

https://www.ibtimes.com/banking-apps-blacklisted-samsung-galaxy-s10-after-fingerprint-vulnerability-was-2851509

TrendMicro Employee Sold Customer Info to Tech Support Scammers

https://www.bleepingcomputer.com/news/security/trendmicro-employee-sold-customer-info-to-tech-support-scammers/

Japanese hotel chain sorry that hackers may have watched guests through bedside robots

https://www.theregister.co.uk/2019/10/22/japanese_hotel_chain_sorry_that_bedside_robots_may_have_watched_guests/

More News

Tech Support Scammers Are Abusing a New Firefox Browser Lock Bug

https://www.bleepingcomputer.com/news/security/tech-support-scammers-are-abusing-a-new-firefox-browser-lock-bug/

Avast, Avira Products Vulnerable to DLL Hijacking

https://www.securityweek.com/avast-avira-products-vulnerable-dll-hijacking

Georgia suffered a massive cyberattack. Let's take a look at similar incidents from recent history

https://cyware.com/news/georgia-suffered-a-massive-cyberattack-lets-take-a-look-at-similar-incidents-from-recent-history-ba70846c

Office 365 to Prevent Malicious Docs From Infecting Windows

https://www.bleepingcomputer.com/news/microsoft/office-365-to-prevent-malicious-docs-from-infecting-windows/

First Cyber Attack 'Mass Exploiting' BlueKeep RDP Flaw Spotted in the Wild

https://thehackernews.com/2019/11/bluekeep-rdp-vulnerability.html

Eye Clinic Breach Reveals Data of 20,000 Patients

https://threatpost.com/eye-clinic-breach-reveals-data-of-20000-patients/149878/

Google Analytics Emerges as a Phishing Tool

https://threatpost.com/google-analytics-phishing-tool/149917/

IBM: Face Recognition Tech Should be Regulated, Not Banned

https://www.securityweek.com/ibm-face-recognition-tech-should-be-regulated-not-banned

US MS-ISAC Releases the October List of End of Support Software

https://www.bleepingcomputer.com/news/software/us-ms-isac-releases-the-october-list-of-end-of-support-software/

5 Places Where Hackers Are Stealthily Stealing Your Data In 2019

https://thehackernews.com/2019/10/hacking-data-breach-protection.html

Wizard Spider Upgrades Ryuk Ransomware to Reach Deep into LANs

https://threatpost.com/wizard-spider-upgrades-ryuk-ransomware/149853/

Nemty Ransomware Now Spreads via Trik Botnet

https://www.bleepingcomputer.com/news/security/nemty-ransomware-now-spreads-via-trik-botnet/

Reader Suggested Articles

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

From Lauren Meadows:

- https://www.youtube.com/watch?v=C4Uc-cztsJo

More adventures in replying to spam

This is an extremely funny way that an English comedian dealt with a scammer.

- https://www.crowdstrike.com/blog/huge-fan-of-your-work-part-1/

Huge Fan of Your Work: How TURBINE PANDA and China's Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet

This article takes a look at how the Chinese government partnered with local hackers to commit industrial espionage and other crimes.

From Deborah Wright:

- https://www.propublica.org/article/the-ransomware-superhero-of-normal-illinois

The Ransomware Superhero of Normal, Illinois

This article talks about a real person who in his free time breaks encryption on ransomware strains.

From Erich Neumann:

- https://www.helpnetsecurity.com/2019/10/09/phishing-increase-2019/

Phishing attempts increase 400%, many malicious URLs found on trusted domains

This article talks about the rise in phishing attempts and how no website you visit is truly safe.

From An Anonymous Reader:

- https://www.usatoday.com/story/tech/2019/10/15/implanted-microchips-work-id-versus-app/3977729002/

This article was submitted by a reader who wished to remain anonymous. It is about biohacking and how it can be used for business.

Cyber Challenge

Last Month's Challenge

Congratulations to everyone who was able to solve last month's challenges. There were 4 questions and some of them were very tricky. 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.

	Completed 4 of 4 Challenges	
Faye Krueger @ 1701 on 7 Oct	Erich Neumann @ 1737 on 7 Oct	Rene Hess @ 0553 on 8 Oct
Deborah Wright @ 1559 on 8 Oct	David Evans @ 1622 on 8 Oct	Kelly Patterson @ 1409 on 10 Oct
	Completed 3 of 4 Challenges	
	James Kimani @ 1854 on 21 Oct	
	Completed 1 of 4 Challenges	
Debra Lewis @ 1650 on 7 Oct	Jacklyn Parker-Rogers @ 0917 on 8 Oct	Mercedez-Fay A Wallace-Morrison @ 1544 on 14 Oct

Here are the answers to last month's questions. I've also provided details on how you can find all the parts of question 4.

Question 1: The picture on the right is the phishing site. The biggest clue is the URL. For a commercial site you should expect the domain listed to probably be the site. This was a phishing site created on Weebly.com. The POWERED BY weebly at the bottom left of the page is another indication.

Question 2: For question 2 I got tricky. BOTH are phishing sites. Again the biggest clue is the URL. The URL on the left is: profile-chase-page.com/chasebank/77ac2899c0d67f1dd63cf69f73ec4e29 and the URL on the right is: amzinggoodcasefish.com/chasecustomer/edfd89788e46f46c34be305222b4483a/. The CORRECT URL is www.chase.com.

Question 3: The website is a phishing site. Again, you can tell by the URL. The domain is windows.net instead of windows.com. You can also tell it is also a scam when you look at the very beginning of the URL. Instead of www.windows.com you see wwwhbgoutlookofficeowa.blob.core.windows.net.

Question 4: This question was a 4 part question. I took a question and encoded it, broke it into 4 sections, then hid it around last month's newsletter. One part was in a picture on the 4th page and another in one of the black boxes on page 9. I set the font of the text to be the same as the background and made the size 1. The other 2 parts of the question were hidden in the code of the PDF newsletter. One part was at the beginning of the header and the other at the end of the footer. Once you have all of the parts you have to assemble them in the correct order then figure out the encoding being used. Once you know the encoding you can find websites that will immediately decode the message. When you do, you get this:

I am an English mathematician and writer and a Countess. I was chiefly known for my work with Charles Babbage's proposed mechanical general-purpose computer, the Analytical Engine. What is the name most people know me as and what was my actual name?

The **answer** is: Ada Lovelace, Countess of Lovelace Augusta Ada King

Cyber Challenge

This Month's Challenges

For this month's challenges I decided to go with simple questions. There is no steganography involved this month so no need to go searching around the newsletter for hidden messages.

Good luck with the challenges.

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?

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?

3. I was the first computer system to be infected by the virus in question #2. What computer system am I?

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?

5. I am an IoT botnet that launched the largest DDoS attack to date 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?

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?

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?

8. 4f43344a535342686253426849474e35596d56796332566a64584a7064486b676257396b5a5777675a47567a615764755a575167644738675a3356705a475567634739736157e705a584d675a6d397949476c755a6d3979625746306157397549484e6c59335679615852354948647064476870626942686269427663 6d6468626d6c3659585270623234754943424a49484e6f59584a6c49474567626d46745a5342336158526f4947456756564d67523239325a584a7562575675644342685a32567559336b7549434258614746304947467449456b2f

</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.

In closing I want to provide you with some great shopping tips I saw in another cyber newsletter I receive. It is some very good information for staying safe while shopping online over the holidays.

- **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.**