Vol. 4 | Issue 6

Cyber Security NEWS

June 2019

Welcome to the TXDPS Cyber Newsletter

Hello everyone and welcome to this month's cybersecurity newsletter. This month you will find several articles which I believe everyone will find of value. But before you start reading the articles I wish to share with you a story a reader told me after reading about Vishing in the last newsletter. She has asked me to keep her name anonymous but she gave me permission to share the story. Here is what she sent me:

"Thanks, Kirk.

Great info as always. I wanted to share a personal experience with "Vishing". My husband was the victim. It went exactly as you described, but they convinced him a company he purchased something from was now defunct and in a civil restitution, they were ordered to refund money. He checked and the company was indeed out of business. He was suspicious so he kept refusing the 'refund'. Long story short, they finally wore him down enough over calling daily for a month and he gave them online access to his bank account so they could "direct deposit the refund". Fortunately I was standing right there when they stole $2400 and were moving to the next account and I called the bank which froze everything. He eventually filed with the Secret Service and got his money back. The bank said it wasn't stolen because he gave them access. However, he also had the account number the money was transferred to, which the Secret Service was very pleased to learn.

Three things –

I don't know why he didn't block the number when they kept calling because….

If you hear something often enough, it becomes true.

You can enter a phone number into Google, and if it's a fraudulent number or one associated with fraud, Google knows!"

I appreciate her willingness to share her experience. If any other readers have cyber experiences they feel others could benefit from, please share them. I will keep your name anonymous if you wish but I would like to hear reader's personal experiences that I can share with others to help protect them. To the reader who shared this, thank you very much for being willing to share this with everyone.

Another thing I wish to talk about before you start reading this month's articles is the use of public WiFi and how VPNs can help protect you from the dangers of open WiFi. Have you ever used an open WiFi connection in an airport, hotel, coffee shop etc? If so, did you stop to think about how safe it was to use? Public WiFi connections are convenient when you want to get online, but are VERY insecure and open you up to multiple dangers. One danger is someone can setup a "rogue" access point and intercept all Internet traffic. The person who setup the rogue device now can monitor everything you do online. This includes usernames and passwords to bank accounts, emails, Instant Messenger messages, etc. If you need to use a public WiFi, I strongly suggest you consider using a VPN to help protect your communications. While a VPN will not guarantee your online safety, it greatly decreases the chances someone will intercept what you are doing and steal your identity, money, etc. Click the VPN hyperlink to find out more about what a VPN is and how it works. To find what PCMag says are the best free VPNs of 2019, click HERE: To find what Techradar says are the best VPNs, click HERE. Or you can email me and I'll tell you what I use.

CyberPAC

Our Cybersecurity Technical Writer asked me to include a write-up from him about the DPS CyberPAC. Below is what he wants everyone to know.

Ever wanted to have a voice in the creation or shaping of Cyber Security policies? Well now you can!

The Cyber-PAC (CPAC) was established in 2017 with authority from the Chief Information Security Officer (CISO) as an inter-divisional relationship to better develop Department policies. The ultimate goal is to provide DPS divisions a means to actively participate, provide input, and address any concerns that policies would impact current business process and goals.

Security policies are typically created or updated as a result of assessment/audit findings, state or federal laws, development of new technologies, and changes in threat landscapes. This is how policy creation works and how you can be heard:

- Policy identified
- Cyber researches, develops drafts
- Draft submitted to CPAC
- Cyber compiles inputs, edits, or updates draft. Returned to CPAC for final review.
- Policy draft approved by Cyber leadership
- Policy draft sent to EPMO for routing and approval by DPS executive leadership.
- Upon executive approval, EPMO updates General Manual.

CPAC distributes to divisional members for consideration and input. This step is your opportunity to be heard. The CPAC is your way to have a say in how these policies are formed, as they may affect your current operations. If you would like to know who your member is and contact them, the members are listed below:

Chair	Aaron Blackstone	Aaron.Blackstone@dps.texas.gov
Secretary	Ean Meacham	Ean.Brown-Meacham@dps.texas.gov
Cyber Security	Jeremy Wilson	Jeremy.Wilson@dps.texas.gov
IT	Michael Lucero	Michael.Lucero@dps.texas.gov
IT	Bryan Lane	Bryan.Lane@dps.texas.gov
IT	Ron Zikha	Ron.Zikha@dps.texas.gov
LES	Mike Lesko	Mike.Lesko@dps.texas.gov
OGC	Cari Bernstein	Cari.Bernstein@dps.texas.gov
THP	Chris Nordloh	Chris.Nordloh@dps.texas.gov
ICT	Eric Baker	Eric.Baker@dps.texas.gov
Administration	Jessica Ballew	Jessica.Ballew@dps.texas.gov
TDEM	Jeff Newbold	Jeff.Newbold@dps.texas.gov
DL	Jeffrey Thiel	Jeffrey.Thiel@dps.texas.gov
CAO	Jennifer Wu	Jennifer.Wu@dps.texas.gov
RSD	Diana Burns	Diana.Burns@dps.texas.gov
TRD	Corey Lain	Corey.Lain@dps.texas.gov
OIG	Brian Lillie	Brian.Lillie@dps.texas.gov
CID	Reena Bawa	Reena.Bawa@dps.texas.gov
Finance	Maureen Coulehan	Maureen.Coulehan@dps.texas.gov

In other exciting news, Cyber Security has published its own chapter in the General Manual, Chapter 25 Cyber Security Policy! Here you'll be able to find policies related to Cyber Security for daily operations.

Google / Windows 10

Massive Google Outage Turned Smart Homes Into Zombies

(by **Kelly Weill** on **June 3, 2019**)

Your smart home is only as smart as the network that runs it.

On Sunday, some Google users found themselves locked out of YouTube and Gmail as the tech giant experienced major outages across the U.S. But while the service disruption only affected most users' browsing history, others saw their homes malfunction. Next, a Google -owned smart home company, was also affected by the outage. For Nest users, that meant losing access to smart thermostats, smart baby monitors, and smart front doors.

They might seem like a plot device in a heavy-handed sci-fi movie, but smart home glitches are an inevitability as more people invite digital helpers into their homes.

"Can't use my Nest lock to let guests into my house," a commenter on the tech forum Hacker News wrote on Sunday. "I'm pretty sure their infrastructure is hosted in Google Cloud."

The commenter, StanfordKid, had been trying to use Nest to unlock his door for guests while he was away. In theory, the software is safer than leaving the keys under a doormat. Unless Google is down—then the smart home device loses its brain.

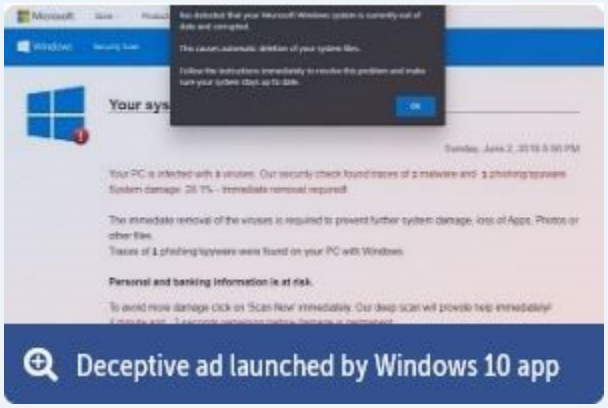
StanfordKid wasn't the only Nest user locked out of his devices on Sunday. Nest also makes smart smoke detectors, smart camera systems, and smart thermostats, some of which were reported useless during the four-hour outage. (Nest did not immediately respond to a request for comment.)

Click **HERE** to read the article.

Windows 10 Apps Serving Malicious Ads Warning of Virus Infections

(by **Bogdan Popa** on **Jun 3, 2019 08:11 GMT**)

Ads bundled into Windows 10 apps available for users from the Microsoft Store point users to deceptive campaigns eventually trying to deploy malware on their devices.



Most of the fraudulent ads warn of malware infections and prompt users to perform scans with fake security solutions that could eventually compromise their devices.

Some of these ads load websites that resemble the design of Microsoft's support pages in an attempt to convince users to "scan" their devices.

"Your PC is infected with 3 viruses. Our security check found traces of 2 malware and 1 phishing/spyware. System damage: 29.1% - immediate removal required. 4 minutes and 2 seconds remaining before damage is permanent" one such deceptive website caught in a screenshot published by BornCity reads.

"Your Microsoft Windows system is currently out of date and corrupted. This causes automatic deletion of your system files. Follow the instructions immediately to resolve this problem and make sure your system stays up to date," a message shown on the page reads.

Just close the windows

Needless to say, there's no malware infection on these devices, but inexperienced users can easily be tricked into downloading the fake security apps. In most of the cases, closing the browser window warning of malware infections is enough to simply keep the device protected, albeit it's pretty clear that Microsoft itself needs to block the ads too.

Click **HERE** to read the article.

West Africa / Snapchat

West Aftica's Scattered Canary gang shows how cybercriminals supersize email scams

(by **Sean Lyngaas** on **JUN 5, 2019**)

Sometimes the most effective scam techniques are also the most mundane.

Business email compromise attacks don't involve advanced malware, and aren't carried out by headline-grabbing nation-state hackers. BEC scams simply rely on personalized emails to dupe victims into transferring funds to someone who appears to be a co-worker, friend, or family member.

But this fraud technique is taking a toll, depriving Americans of a vast sum of money each year. In 2018, the FBI's cybercrime center received over 20,000 BEC complaints that accounted for estimated losses of $1.2 billion. Understanding the scale of the problem requires understanding how perpetrators scale their operations.

The decade-long evolution of one Western African cybercriminal gang is a case in point. Email security firm Agari on Wednesday published research documenting the so-called Scattered Canary group's rise from a lone individual to dozens of operatives specializing in various aspects of fraud. The group also has grown from peddling romance scams to targeting big corporations with email schemes.

After honing their skills, in March 2017, two of Scattered Canery's original members turned to phishing for enterprise credentials by spoofing Adobe, DocuSign, and OneDrive applications, according to the research. From then until November 2018, the group almost exclusively targeted businesses in the U.S. and Canada, netting over 3,000 account credentials through phishing.

Click **HERE** to read more.

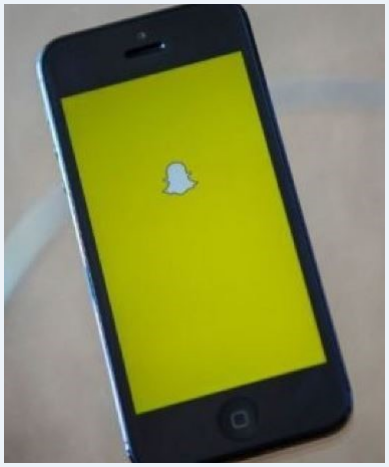
Snapchat employees abused data access, spied on users: report

(by **Chris Perez**)

Snapchat employees have been using internal tools - which offer them privileged access to user data - to spy on people's pages, a report says.

Two workers who are no longer with the app's parent company, Snap, spoke to Motherboard about the alleged abuse of poser - which included breaches of location info and other sensitive data.

In some cases, employees allegedly accessed old photos and videos that users had saved, according to the Motherboard sources.



Two other ex-workers and a current employee described how Snapchat's data access tools allowed them to peel back the curtain on people's pages. They said one of the tools is called SnapLion and was originally used to gather info at the request of law enforcement or a court subpoena.

According to Motherboard's sources, there are at least two departments in Snap that use SnapLion. They include the "Spam and Abuse" team, which deals with bullying and harassment, and the "Customer Ops" crew, which deals with user issues.

Until now, nobody had ever revealed the tool's existence. Internal emails reportedly confirmed its usage.

One former Snapchat worker told Motherboard that SnapLion ultimately gave employees "the keys to the kingdom." The app currently has more than 185 million users. It's unclear if the company has reached out to any of the accounts affected.

Requests for comment were not immediately returned Thursday.

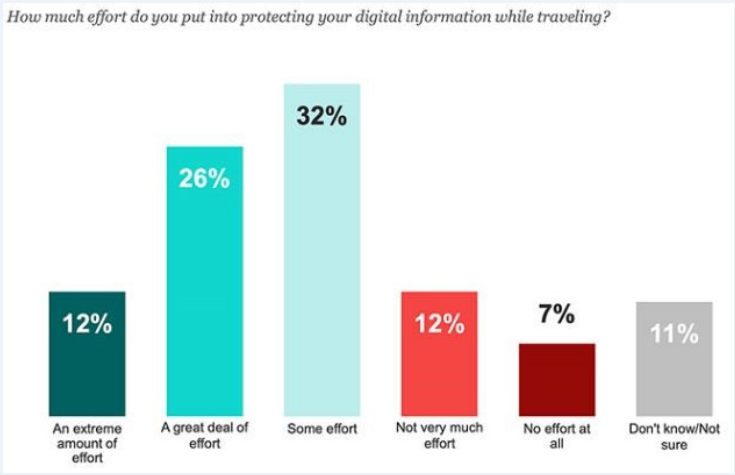
Click **HERE** to read more.

Travelers / License-plates

High-risk behaviors expose most travelers to cyber risks

(by **Help Net Security** on **May 24, 2019)**

The travel industry and its customers are increasingly the targets of cyberattacks as criminals seek to monetize highly valuable travel data, according to the new IBM Security research.



38% of respondents say they put a great deal or an extreme amount of effort into protecting their digital information when traveling

Compounding the problem, a new survey conducted by Morning Consult on behalf of IBM Security reveals that travelers are still blind to the risks they face on the road. The survey found that only 40% of respondents believed it was likely they would be targeted for cybercrime while traveling, yet 70% are engaging in high-risk behaviors while on the road.

Attacks in the travel and transportation industry are becoming more frequent, opening already unwary travelers to cybersecurity threats during their journeys.

According to the 2019 IBM X-Force Threat Intelligence Index, the transportation industry has become a priority target for cybercriminals as the second-most attacked industry - up from thenth in 2017 - attracting 13% of observed attacks. Since January 2018, 566 million records from the travel and transportation industry have been leaked or compromised in publicly reported breaches.

Click **HERE** to read more.

Maker of US border's license-plate scanning tech ransacked by hacker, blueprints and files dumped online

(by **Thomas Claburn** on **23 May 2019** at **23:45**)

Perceptics confirms intrusion and theft, stays quiet on details

Exclusive The maker of vehicle license plate readers used extensively by the US government and cities to identify and track citizens and immigrants has been hacked. Its internal files were pilfered, and are presently being offered for free on the dark web to download.

Tennessee-based Perceptics prides itself as "the sole provider of stationary LPRs [license plate readers] installed at all land border crossing lanes for POV [privately owned vehicle] traffic in the United States, Canada, and for the most critical lanes in Mexico."

In fact, Perceptics recently announced, in a pact with Unisys Federal Systems, it had landed "a key contract by US Customs and Border Protection to replace existing LPR technology, and to install Perceptics next generation License Plate Readers (LPRs) at 43 US Border Patrol check point lanes in Texas, New Mexico, Arizona, and California."

On Thursday this week, however, an individual using the pseudonym "Boris Bullet-Dodger" contacted *The Register*, alerting us to the hack, and provided a list of files exfiltrated from Perceptics' corporate network as proof. We're assuming this is the same "Boris" involved in the CityComp hack last month. Boris declined to answer our questions.

The file names and accompanying directories - numbering almost 65,000 - fit with the focus of the surveillance technology biz. They include .xlsx files named for locations and zip codes, .jpg files with names that refer to "driver" and "scene," .docx files associated with presumed government clients like ICE, and date-and0time stamped .jpgs and .mp4 files.

Click **HERE** to read more.

TeamViewer / Gatekeeper

Report Reveals TeamViewer Was Breached By Chinese Hackers In 2016

(by **Wang Wei** on **May 17, 2019**)

The German software company behind TeamViewer, one of the most popular software in the world that allows users to access and share their desktops remotely, was reportedly compromised in 2016, the German newspaper Der Spiegel revealed today.

TeamViewer is popular remote-support software that allows you to securely share your desktop or take full control of other's PC over the Internet from anywhere in the world. With millions of users making use of its service, TeamViewer has always been a target of interest for attackers.

According to the publication, the cyber attack was launced by hackers with Chinese origin who used Winnti Trojan malware, activities of which have previously been found linked to the Chinese state intelligence system.

Active since at least 2010, Winnti advanced persistent threat (APT) group has previously launched a series of financial attacks against software and gaming organizations primarily in the United States, Japan, and South Korea.

Click **HERE** to read more.

Gatekeeper Bug is MacOS Mojave Allows Malware to Execute

(by **Threatpost**)

Researcher discloses vulnerability in macOS Gatekeeper security feature that allows the execution of malicious code on current version on the OS.

Researcher Filippo Cavallarin disclosed a bug in the macOS security feature Gatekeeper that allows malicious code execution on systems running the most recent version of Mojave (10.14.0).

MacOS Gatekepper is an Apple security feature that enforces code signing and verifies downloads and apps before users run them. The goal is to eliminate the possibility of malicious files being executed on systems. Gatekeeper requires the user's consent before opening a file.

"On MacOS X version <= 10.14.5 (at time of writing) it is possible to easily bypass Gatekeeper in order to execute untrusted code without any warning or user's explicit permission," wrote Cavallarin, the CEO of Segment, an Italian security firm.

While there is no patch from Apple, at this time, a workaround to mitigate the vulnerability is available.

The researcher said he notified Apple of the flaw on February 22. Since then, Apple has not issued a patch, the researcher noted. "This issue was supposed to be address, according to the vendor, on May 15th 2019 but Apple started dropping my emails. Since Apple is aware of my 90 days disclosure deadline, I make this information public," he wrote.

Click **HERE** to read more.

More News

Baltimore mayor open to paying off hackers who paralyzed city, despite once likening it to 'rewarding bank robbers'

https://www.foxnews.com/us/baltimore-mayor-open-paying-hackers

Buyer beware: Google is tracking your purchases via Gmail

https://www.foxnews.com/tech/google-tracking-purchases-gmail

Alleged LinkedIn hacker Yevgeniy Nikulin will stand trail in U.S. court, despite mental illness...

https://www.cyberscoop.com/yevginiy-nikulin-linkedin-hacker-trial-mental-illness/

DHS assessment of foreign VPN apps finds security risk real, data lacking

https://www.cyberscoop.com/dhs-mobile-vpn-apps-chris-krebs-ron-wyden/

Julian Assange charged with 17 new criminal counts under Espionage Act

https://www.cyberscoop.com/julian-assange-charged-17-new-criminal-counts-espionage-act/

Facebook scrubbed 2.2 billion fake accounts in the first quarter of 2019, a new high

https://www.cyberscoop.com/facebook-community-standards-report-may-2019/

Google: We've been storing some enterprise customer passwords in plaintext since 2015

https://www.cyberscoop.com/google-password-g-suite-plaintext/

Citing data security concerns, DHS warns industry of Chinese-made drones

https://www.cyberscoop.com/dhs-chinese-drones-warning/

Wave of SIM swapping attacks hit US cryptocurrency users

https://www.zdnet.com/article/wave-of-sim-swapping-attacks-hit-us-cryptocurrency-users/

Amazon's helping police build a surveillance network with Ring doorbells

https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells/

Walmart will stock your fridge with groceries while you're not home

https://www.cnet.com/news/walmart-will-stock-your-fridge-with-groceries-while-youre-not-home/

Facebook Set to Reveal Own Cryptocurrency in June, Report Says

https://www.coindesk.com/facebook-set-to-reveal-own-cryptocurrency-in-june-report-says

More News

2.3B Files Exposed in a Year: A New Record for Misconfigs

https://threatpost.com/files-exposed-record-misconfigs/145177/

US Secretary of State Explains Why Huawei Just Had to Be Banned

https://news.softpedia.com/news/us-secretary-of-state-explains-why-huawei-just-had-to-be-banned-526231.shtml

Researcher Exploits Microsoft's Notepad to 'Pop a Shell'

https://threatpost.com/researcher-exploits-microsofts-notepad-to-pop-a-shell/145242/

WhatsApp Hacked and Bugs in Intel Chips: What You Need to Know

https://nationalinterest.org/blog/buzz/whatsapp-hacked-and-bugs-intel-chips-what-you-need-know-60432

APPLE JUST PATCHED A MODEM BUG THAT'S BEEN IN MACS SINCE 1999

https://www.wired.com/story/apple-modem-bug-since-1999/

Microsoft warns users to patch 'wormable' Windows flaw

https://www.foxnews.com/tech/microsoft-seriously-you-need-to-patch-wormable-windows-flaw

Microsoft to Retire Microsoft Office Support for Older Android Versions

https://news.softpedia.com/news/microsoft-to-retire-microsoft-office-support-for-older-android-versions-526259.shtml

Hackers actively exploit WordPress plugin flaw to send visitors to bad sites

https://arstechnica.com/information-technology/2019/05/hackers-actively-exploit-wordpress-plugin-flaw-to-send-visitors-to-bad-sites/

TO FIGHT DEEPFAKES, RESEARCHERS BUILT A SMARTER CAMERA

https://www.wired.com/story/detect-deepfakes-camera-watermark/

Chief Executive of Communications Company Sentenced to Prison for Providing Encryption Services and Devices to Criminal Organizations

https://www.justice.gov/usao-sdca/pr/chief-executive-communications-company-sentenced-prison-providing-encryption-services

First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records

https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

Reader Suggested Articles

Below are readers suggestions for this month. They are very interesting articles so hopefully you will find them as interesting as I did.

From Erich Neumann:

Americans Overly Confident in Cyber Hygiene

- https://www.infosecurity-magazine.com/news/americans-over-confident-in-cyber/

From Deborah Wright

PATCH REMOTE DESKTOP SERVICES ON LEGACY VERSIONS OF WINDOWS

- https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-bluekeep_20190604.pdf

Romanian ATM Skimmer Gets Over 5 Years of Jail Time

- https://www.bleepingcomputer.com/news/security/romanian-atm-skimmer-gets-over-5-years-of-jail-time/

Tennessee Valley Authority Isn't Compliant with Federal Directives

- https://www.infosecurity-magazine.com/news/tva-noncompliant-with-federal-1/

Adware Hidden in Android Apps Downloaded More Than 440 Million Times

- https://www.darkreading.com/attacks-breaches/adware-hidden-in-android-apps-downloaded-more-than-440-million-times/d/d-id/1334877

From David Evans

Microsoft says mandatory password changing is "ancient and obsolete"

- https://arstechnica.com/information-technology/2019/06/microsoft-says-mandatory-password-changing-is-ancient-and-obsolete/

Cyber Challenge

Last Month's Challenge

Last month's challenge was to answer 6 questions saved as QR codes. The people who completed the challenge are listed below. For those of you who were unable to complete the challenge, remember you can always email me for assistance.

Lauren Meadows @ 0938 on 14 May	William Gentle @ 0947 14 May	David Evans @ 1004 on 14 May
Patricia Rogers @ 1008 on 14 May	Josef Lopez @ 1020 on 14 May	Jordan Hancock @ 1022 on 14 May
Erich Neumann @ 1038 on 14 May	Faye Krueger @ 1058 on 14 May	Kerry Sosa @ 1059 on 14 May
Dax Roberts @ 1104 on 14 May	Tracy Kingsley @ 1150 on 14 May	Deborah Wright @ 1214 on 14 May
Gina Bauer @ 1311 on 14 May	Mackayla Bernarn @ 1420 on 14 May	Walker Pyle @ 1425 on 14 May
Rebekah Lloyd @ 1430 on 14 May	Carla Bell @ 1436 on 14 May	Linda "Michelle" Hammonds @ 1638 on 14 May
Javier Lopez-Schulze @ 1640 on 14 May	Jared Crouse @ 0553 on 15 May	Kymberly Hernandez @ 0744 on 15 May
Aaron Campbell @ 1502 on 15 May	Jaelyn Edwards @ 1556 on 15 May	Rene Hess @ 0626 on 16 May
James Taylor @ 1047 on 17 May	Michael Mchale @ 1433 on 25 May	Evan Hernandez @ 1157 on 28 May
Cassandra Lowrie @ 1038 on 29 May	Gary Gregg @ 0942 on 30 May	Brian Hutchins @ 1258 on 30 May

For those of you who don't know what a QR code is, it is a machine-readable code consisting of an array of black and white squares. It is typically used for storing URLs or other information and can be read by a camera on a smartphone that has a QR code reader program installed. However, as the challenge showed, it is possible to hide other information besides a URL. Because other than URLs can be stored in a QR code, it is possible for malware to infect your phone and have information stolen directly from it. All a malicious actor has to do is encode the malicious payload or web address into a QR code format, print the code on some adhesive paper and affix it over a legitimate one. Or it can just be emailed to you. Since the QR encoding is not human readable, the victim who scans the code wouldn't know they are scanning a malicious link until its too late.

How do you protect yourself from a malicious QR code? Caution is the best way. I suggest you do not scan random QR codes. Phishing emails can easily include a QR code and since most email scanners do not read any emailed QR code the average user will assume the code is safe to scan. Be careful about scanning codes you find on buildings or anywhere someone might have placed a malicious code. Another way to protect yourself is to download a QR scanner that will inspect the scanned code and display it to you before going to the website or activating the code.. Norton Snap is a QR code reader that is available for both iPhone and Android. After the QR code is scanned the program scans the content against a database of known malicious links prior to showing you the link. The program then lets you decide if you wish to visit the link or not. To read more about how a QR code can be weaponized, you can find more information in these links:

https://www.lifewire.com/how-to-protect-yourself-from-malicious-qr-codes-2487772

https://resources.infosecinstitute.com/security-attacks-via-malicious-qr-codes/#gref

https://www.welivesecurity.com/2018/03/28/scanning-qr-codes-ios-11s/

To read about other QR code readers similar to Norton Snap, click on this weblink:

https://www.topappslike.com/norton-snap-qr-code-reader/

Email me if you would like the answers to last month's challenges.

Cyber Challenge

This Month's Challenge

Because last month's challenge was such a success (more people completed than in any previous month), I think I'll do something similar with this month's challenge. I'll use QR codes again but I will increase the difficulty. Good luck on the challenges and let me know if you need any 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 this 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. And protecting the Agency and yourself does not end when you leave work. 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.

So in closing I want to take a couple of minutes and talk about Social Engineering. I have talked about this in previous newsletters but I think it is a good idea to periodically remind people about this non-technical but VERY effective attack. For those who don't know what Social Engineering is, it can be described as the non-technical hacking of a human. It is an attempt to gather information about a person to use that information for a malicious purpose. That purpose is generally focused on you, but not always. It is possible the attacker is trying to gather information about the Agency (or the company you work for if you are not a DPS reader) to use in a targeted attack against the organization.

Everyone deals with Social Engineering attacks every day. However, most people never realize they are being social engineered. Some people do it naturally and some learn to social engineer as a part of their job. An example is anyone who works in sales. To be successful in sales you have to be able to convince the buyer they really do want to buy this "thing" they don't need. From law enforcement an example would be any officer or investigator. To get a confession from a suspect, officers will often employ social engineering techniques similar to what a hacker would use.. As a final example, for those who have been or are currently in the military, the intelligence community does it all the time to gather information.

To learn more about what Social Engineering attacks are and how you can defend yourself, I suggest you visit YouTube and do a search for Social Engineering. I have included a few links I think give quick examples of the dangers and how you can protect yourself. If the links don't work for you, just search for the title below.

Use Instagram to Social Engineer Your Targets

Principles of Social Engineering - CompTIA Security+ SY0-501 - 1.2

Watch this hacker break into a company

How phishing scammers manipulate your amygdala and oxytocin

This is how hackers hack you using simple social engineering

What is Your Password? - Jimmy Kimmel

What's Your Password? - Jimmy Kimmel follow up

Social Media Experiment - Jack Vale Films

I hope these videos have enlightened you some and you have learned techniques to help defend yourself. Please email me if you still have questions or wish to share an example of when you were social engineered..

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 newsletter at this public facing DPS 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.

And as always,

THANK YOU FOR YOUR CYBER VIGILANCE.