Vol. 4 | Issue 8

Cyber Security NEWS

August 2019

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.

Before you read the articles I selected for this month's newsletter, I want to take a few minutes to talk about the Equifax leak and the settlement. If you are unaware of this, Equifax had a data breach in 2017 that exposed roughly 147 million American's Personally Identifiable Information (PII), credit card data, driver's license information, and Social Security information online. Because of this, the company has agreed to a settlement with the US Federal Trade Commission to pay at least $650 million with up to $425 million being reserved for individuals. You can find out if you are eligible for a claim by going to the Equifax website and putting in some information. The website is https://www.equifaxbreachsettlement.com/. To file a claim go to https://www.equifaxbreachsettlement.com/file-a-claim. As part of the check to determine if you are eligible for the claim you will have to put in the last six (6) of your Social Security Number. This is a point of contention for people. A company who just lost the information on 147 million Americans wants you to put in most of your Social Security Number to check to see if you are eligible for part of the settlement. I'll let you think about that for a bit.

If you are eligible for the settlement, apparently you get the option of picking from receiving either $125 or 10 years of free credit monitoring. If you decide to take the cash it will be paid through either a check or a pre-paid card. And if you were one of the unlucky people who suffered from identity theft from this breach, you might be eligible for a reimbursement of $25 per hour for each hour you spent dealing with recovering from the identity theft.

Now that you have a synopsis of the issue, lets talk about what we are seeing on the cybersecurity side. Scammers and other criminals are trying to capitalize on this and steal money you are authorized. Anyone who may have had their information stolen is at risk for these scams, and it is possible malicious people might reach out to those not affected to convince them to buy protection products or services. To protect yourself:

- Make sure you are only using legitimate websites for checking and filing. It is very easy to setup fake websites so don't fall victim to a false site. Make sure you are typing in the link correctly or clicking the hyperlink from a legitimate source.
- You do not have to pay anything to file a claim, look into your data, receive credit monitoring services or participate in the settlement so do not pay for anything.
- Never give your information to someone who contacts you and offers to find out if you have been affected.
- NEVER give your Social Security Number to someone who contacts you.
- Do NOT believe anyone who calls you and tells you that your Social Security Number has been compromised and is being suspended or deactivated. That is a new scam happening and is definitely not true.

If you have questions you should be able to find the answers, or at least the contact information for a legitimate representative, in the links I provided above.

SSN / Facebook

Social Security scams could rise following Capital One breach

(by **Brittany De Lea** published **August 02, 2019**)

The Capital One data breach is stoking fears about a new wave of Social Security scams, which have been on a precipitous rise in 2019.

As first reported by The Wall Street Journal, thieves could exploit the event to go after vulnerable victims.

Social Security scams have overtaken IRS imposter scams this year, becoming one of the most prevalent thievery attempts.

According to Capital One, about 140,000 Social Security numbers belonging to its credit card customers could have been compromised.

However, scammers do not need your Social Security information in order to carry out their schemes.

According to the Federal Trade Commission (FTC), the most common Social Security scams involve imposters telling consumers their Social Security number were suspended because of suspicious activity, after which victims are asked to convirm their numbers.

People have filed more than 76,000 complaints regarding Social Security imposter scams over the past 12 months, with losses reported at $19 million, according to the FTC.

The FTC cautioned that the Social Security Administration (SSA) will not contact you out of the blue, and urges concerned individuals to reach out to the real SSA with questions.

Click **HERE** to read the article.

Facebook hit with new questions over Cambridge Analytica

(by **HARPER NEIDIG - 08/04/19 08:00 AM EDT**)

Facebook is facing new questions over its handling of the Cambridge Analytica debacle even after a record settlement with the FTC ended a year-long investigation by regulators into the matter.

Facebook has maintained that it first became aware of Cambridge Analytica's illegal harvesting of user data in December of 2015, when The Guardian first reported it.

But internal emails from Facebook employees, first described in a lawsuit from the attorney general for Washington, D.C. in March, show that Cambridge Analytica had been flagged within the company as early as September 2015 over suspicions that it had been "scraping" Facebook data in violation of the platform's policies.

Those warnings were further detailed last week, in a filing from the Securities and Exchange Commission (SEC) as part of the agency's $100 million settlement with Facebook over charges that it misled investors about the material risk of the scandal.

Months before the Guardian first revealed that Cambridge Analytica had obtained data on tens of millions of Facebook users without their knowledge, Facebook employees had requested an investigation of the right-wing political consulting firm over suspicions it had misused data.

Before declaring bankruptcy last year as a result of the debacle, Cambridge Analytica had deep ties with the Republican party and in 2016 worked for the Trump campaign, assembling voter profiles based on data from a range of sources, including social media sites.

After the Guardian story ran, the employees again raised concerns about Cambridge Analytica, describing it as a "sketch (to say the least) data modeling company that has penetrated our market deeply," according to the SEC complaint.

Click **HERE** to read the article.

Louisiana / Malware

Louisiana governor declares state emergency after local ransomware outbreak

(by **Catalin Cimpanu** for **Zero Day** | **July 25, 2019**)


State of Louisiana

EXECUTIVE DEPARTMENT

PROCLAMATION NUMBER 115 JBE 2019

STATE OF EMERGENCY – CYBERSECURITY INCIDENT

WHEREAS, the Louisiana Homeland Security

Louisiana Governor John Bel Edwards has activated a state-wide state of emergency in response to a wave of ransomware infections that have hit multiple school districts.

The ransomware infections took place this week and have impacted the school districts of three North Louisiana parishes - - Sabine, Morehouse, and Ouachita.

IT networks are down at all three school districts, and files have been encrypted and are inaccessible, local media outlets are reporting.

This is the second time that a state governor has activated a state emergency due to ransomware or any form of cyber-attack. The first time was in Colorado in February 2018, when the Colorado Department of Transportation was forced to shut down operations because of an infection with the SamSam ransomware. However, that state emergency activated additional state resources to help with traffic, road management, and transportation, and not with deploying cyber-security experts to help victims, like in Louisiana's case.

By signing the Emergency Declaration, the Louisiana governor is making available state resources to impacted schools.

This includes assistance from cybersecurity experts from the Louisiana National Guard, Louisiana State Police, the Office of Technology Services, the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), and others.

Click **HERE** to read more.

Cybersecurity: Malware lingers in SMBs for an average of 800 days before discovery

(by **Alison DeNisco Rayome** on **July 11, 2019**)

Small and medium-sized businesses lack the IT staff needed to run comprehensive security detection and response, according to Infocyte.

Despite the adoption of advanced cybersecurity tools, SMBs remain particularly vulnerable to long-lasting breaches compared to enterprise companies, due to a lack of IT staff needed to detect and respond to threats, according to Infocyte's Mid-market Threat and Incident Response Report, released Thursday.

INfocyte measured threats over the 90-day span from April to June 2019, reviewing more than 550,000 forensic inspections on systems across hundreds of customer networks in the mid-enterprise business sector. Unsurprisingly, SMBs are more vulnerable to various types of threats, the report found: 22% of SMBs said their networks have encountered a ransomeware attack that bypassed preventative security controls, while fileless malware attacks are also on the rise.

Average attack dwell time - the time between an attack penetrating a network's defenses and being discovered - ranged from 43 to 895 days for SMBs, the report found. The average dwell time for confirmed, persistent malware was 798 days. Dwell time for riskware - including unwanted applications, web trackers, and adware - averaged 869 days.

Dewll time for attacks including ransomware was much lower, averaging 43 days between the infection and the initial Trojan (often Trickbot or Emotet) and remediation, due to how the ransomeware informs its victims, the report noted.

Some 72% of inspected SMB networks found riskware and unwanted applications in their environment that took longer than 90 days to remove, Infocyte found. While riskware is generally a lower risk than other attacks, networks that fail to control riskware also tend to be less ready to respond to high-priority threats once they are uncovered, according to the report.

Click **HERE** to read more.

Apple / Cisco

Apple's AirDrop and password sharing features can leak iPhone numbers

(by **DAN GOODIN - 8/1/2019, 6:11 AM)**

Partial hashes broadcast in Bluetooth can be converted to phone numbers, researchers say.

Apple makes it easy for people to locate lost iPhones, share Wi-Fi passwords, and use AirDrop to send files to other nearby devices. A recently published report demonstrates how snoops can capitalize on these features to scoop up a wealth of potentially sensitive data that in some cases includes phone numbers.

Simply having Bluetooth turned on broadcasts a host of device details, including its name, whether it's in use, if Wi-Fi is turned on, the OS version it's running, and imformation about the battery. More concerning; using AirDrop or Wi-Ri password sharing broadcasts a partial cryptographic hash that can easily be converted into an iPhone's complete phone number. The information—which in the case of a Mac also includes a static MAC address that can be used as a unique identifier—is sent in Bluetooth Low Energy packets.

The information disclosed may not be a big deal in many settings, such as work places where everyone knows everyone anyway. The exposure may be creepier in public places, such as a subway, a bar, or a department store, where anyone with some low-cost hardware and a little know-how can collect the details of all Apple devices that have BLE turned on. The data could also be a boon to companies that track customers as they move through retail outlets.

Click **HERE** to read more.

Cisco pays $8.6 million for selling surveillance system it knew was vulnerable

(by **DAN GOODIN - 8/1/2019, 2:42 PM**)

Whistleblower said Cisco waited more than 4 years to fix serious flaw.

Cisco is paying $8.6 million to settle claims that it sold a video-surveillance product the company knew made federal and state agencies vulnerable to serious hacking attacks. This is believed to be the first time a company has made a payout under a federal whistleblower lawsuit alleging failure to have adequate security protections.

The settlement stems from a Video Surveillance Manager package Cisco sold, starting more than a decade ago, to a raft of government agencies. These agencies include the Department of Homeland Security, the Secret Service, the Department of Defense Biometrics Taskforce, the Federal Emergency Management Agency, NASA, the Army, the Navy, the Air Force, and the Marine Corps. Known as VSM, the surveillance package was also used by government agencies in at least 15 states, including New York and California.

A 2011 lawsuit unsealed on Wednesday alleged that Cisco knowingly sold VSM to customers even after learning of a critical vulnerability. This vulnerability allowed hackers to spy on video footage in real time, turn cameras on or off, delete footage, and tamper with locks and other physical security systems connected on the same network. The lawsuit was filed under the False Claims Act in the US District Court for the Western District of New York. The act allows individuals with inside knowledge to bring suits on behalf of the government when they believe a contractor is committing fraud.

The individual suing Cisco is James Glenn, who was working for a Cisco partner in 2008 when he discovered the vulnerability and privately reported it. In 2010—about a year after being laid off in a cost-cutting measure—Glenn found that the vulnerability still hadn't been fixed. He filed the complaint a year later. Cisco didn't fix the vulnerability until July 2013, more than four years after Glenn made the private report.

Click **HERE** to read more.

North Carolina / CAN Bus

North Carolina county lost $1.7 million in email scam

(by **Benjamin Freed** on **July 31, 2019**)

Cabarrus County, North Carolina, was the victim last December of an email scheme that diverted $2.5 million meant for the construction of a new high school, county officials said this week. Though the county has recovered $776,518, more than $1.7 million remains unaccounted for.

While no suspects have been named, the incident made Cabarrus County the latest public-sector victim of business email compromise, which is one of the most common lucrative forms of online crime. Such scams, which occur when scammers target a specific individual or organization while impersonating another party that the victim is conducting transactions with, snagged nearly $1.3 billion last year, according to the FBI's 2018 Internet Crime Report.

Cabarrus County was ensnared last November when online scammers posed as Branch and Associates, a firm based in Roanoke, Virginia, hired as the general contractor for a new high school. The scammers emailed Cabarrus County Schools with a request to alter details on the electronic funds transfer account the county had set up to pay its contractor, according to a county government report. Unaware of the ruse, county officials followed their standard processes for such a request, including an updated EFT form and bank documentation. The scammers returned the signed forms as requested on Dec. 4, and the county wired a $2.5 million payment a few weeks later to an account at Bank of America.

Click **HERE** to read more.

Investigating CAN Bus Network Integrity in Avionics Systems

(by **Patrick Kiley** on **July 30, 2019**)

Introduction

Modern aircraft systems are becoming increasingly reliant on networked communications systems to display information to the pilot as well as control various systems aboard aircraft. Small aircraft typically maintain the direct mechanical linkage between the flight controls and the flight surface. However, electronic controls for flaps, trim, engine controls, and autopilot systems are becoming more common. This is similar to how most modern automobiles no longer have a physical connection between the throttle and the actuator that causes the engine to accelerate.

Before digital systems become common within aircraft instrumentation, the gauges and flight instruments would rely on mechanical and simple electrical controls that were directly connected to the source of the data they were displaying to the pilot. For example, the altitude and airspeed indicators would be connected to devices that measure the speed of airflow through a tube as well as the pressure outside the aircraft. In addition, the attitude and directional indicators would be powered by a vacuum source that drove a mechanical gyroscope. The flight surfaces would be directly connected to the pilot's control stick or yoke—on larger aircraft, this connection would be via a hydraulic interface. Some flight surfaces, such as flaps and trim tabs, would have simple electrical connections that would directly turn motors on and off.

Modern aircraft use a network of electronics to translate signals from the various sensors and place this data onto a network to be interpreted by the appropriate instruments and displayed to the pilot. Together, the physical network, called a "vehicle bux," and a common communications method called Controller Area Networks (CAN) create the "CAN bus," which serves as the central nervous system of a vehicle using this method. In avionics, these systems provide the foundation of control systems and sensor systems and collect data such as altitude, airspeed, and engine parameters such as fuel level and oil pressure, then display them to the pilot.

After performing a thorough investigation on two commercially available avionics systems, Rapid7 demonstrated that it was possible for a malicious individual to send false data to these systems, givne some level of physical access to a small aircraft's wiring.

Click **HERE** to read more.

More News

Robinhood admits to storing some passwords in cleartext

https://www.zdnet.com/article/robinhood-admits-to-storing-some-passwords-in-cleartext/

The hot microphone in lawmakers' pockets

https://gcn.com/articles/2019/07/12/microphone-phone-vulnerability.aspx?admgarea=TC_SecCybersSec

El Paso shooting: 8chan offline after Internet company Cloudflare pulls support for 'cesspool of hate' online forum

https://www.foxnews.com/tech/el-paso-8chan-offline

THE THREAT OF ONLINE SKIMMING TO PAYMENT SECURITY

https://www.pcisecuritystandards.org/pdfs/PCISSC_Magecart_Bulletin_RHISAC_FINAL.pdf

I Always Feel Like Somebody's ~~Watching~~ Listening to Me

https://medium.com/tenable-techblog/i-always-feel-like-somebodys-w%CC%B6a%CC%B6t%CC%B6c%CC%B6h%CC%B6i%CC%B6n%CC%B6g%CC%B6-listening-to-me-938cc14aa13c

Can You Spell 2FA? A Luno Phish Example

https://isc.sans.edu/forums/diary/Can+You+Spell+2FA+A+Luno+Phish+Example/25186/

A 33-year-old woman who used to work for Amazon is the suspect in the massive Capital One hack—meet Paige Thompson

https://news.yahoo.com/33-old-woman-used-amazon-185438807.html

Google Researchers Find Remotely Exploitable Vulnerabilities in iOS

https://www.securityweek.com/google-researchers-find-remotely-exploitable-vulnerabilities-ios

Capital One data breach: what you can do following banking hack

https://www.cnet.com/news/back-to-school-deals-keep-heating-up-get-the-brand-new-macbook-air-for-900/?i10c.ua=3

U.S. Warns of 5G Wireless Network Security Risks

https://www.securityweek.com/us-warns-5g-wireless-network-security-risks?utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch

Defense contractors aren't securing sensitive information, watchdog finds

https://fcw.com/articles/2019/07/26/dod-ig-contractor-data-security.aspx?admgarea=TC_Security&utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch

More News

How IoT Opens the Door for Insider Attacks Against Industrial Infrastructure

https://www.securityweek.com/how-iot-opens-door-insider-attacks-against-industrial-infrastructure

Faceapp Poses Potential National Security And Privacy Risks, Experts Say

https://inhomelandsecurity.com/faceapp-poses-potential-national-security-and-privacy-risks-experts-say/?utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch

Marcus 'MalwareTech' Hutchins gets no prison time, one year supervised release

https://www.zdnet.com/article/marcus-malwaretech-hutchins-gets-no-prison-time-one-year-supervised-release/

Exclusive: Hack Breaks Your Visa Card's Contactless Limit For Big Frauds

https://www.forbes.com/sites/thomasbrewster/2019/07/29/exclusive-hackers-can-break-your-credit-cards-30-contactless-limit/#4adb917941e1

Critical flaw in Android can lead to device compromise just by playing video

https://cyware.com/news/critical-flaw-in-android-can-lead-to-device-compromise-just-by-playing-video-29d0d64b

MILLIONS 'GAMBLING WITH PERSONAL DATA' BY ACCESSING FAKE WIFO HOTSPOTS, POLL SUGGESTS

https://www.independent.co.uk/life-style/gadgets-and-tech/fake-wifi-hotspots-malware-security-data-warning-a9025441.html

New Android Ransomware Found Using SMS Spam for Propagation

https://cyware.com/news/new-android-ransomware-found-using-sms-spam-for-propagation-f0bb4922

Congress Passes Two Small Business Administration Cybersecurity Threat Bills

https://www.proofpoint.com/us/corporate-blog/post/congress-passes-two-small-business-administration-cybersecurity-threat-bills

Attackers are deleting files on Iomega NAS devices and demanding ransom

https://cyware.com/news/attackers-are-deleting-files-on-iomega-nas-devices-and-demanding-ransom-1e6bbbaa

Georgia State Patrol agency infected with ransomware

https://www.scmagazine.com/home/security-news/ransomware/georgia-state-patrol-agency-infected-with-ransomware/

Amazon Is Coaching Cops on How to Obtain Surveillance Footage Without a Warrant

https://www.vice.com/en_us/article/43kga3/amazon-is-coaching-cops-on-how-to-obtain-surveillance-footage-without-a-warrant

Cyber Challenge

Last Month's Challenge

Last month's challenge was to answer ten questions. I decided to keep the puzzle simple last month to try to get more people to attempt the challenge. I got a few more than normal but not as many as I had hoped. I know the newsletter is getting readership far outside of DPS. For those people, you can feel free to email me with your responses to the challenges. It is not limited to only DPS employees. And if you have trouble solving the challenges, email me and I'll gladly provide hints and help you work through the challenges. The intent is to educate people and not to just stump them. The more aware everyone is about cybersecurity the better protected we all are. That goes for at home AND at work. So feel free to share the newsletter and encourage people to try the challenges.

I try to vary the complexity of the challenges to give everyone a chance to participate and learn. If you would rather not have your name listed as having solved the challenge just let me know and I will acknowledge without giving your name. So again, if you have trouble solving the challenges don't forget that you can email me for assistance. :)

The people who completed all ten of last month's challenge questions are listed below:

Erich Neumann @ 1113 on 11 July	Ronald Dean @ 1116 on 11 July	David Evans @ 1118 on 11 July
Barbara Rumley @ 1135 on 11 July	Antonio Shaffer @ 1144 on 11 July	Robin Lovelace @ 1148 on 11 July
Joanna Morgan @ 1219 on 11 July	Patricia Rogers @ 1319 on 11 July	Lindsey LaPrime @ 1359 on 11 July
Michelle Pugh @ 1359 on 11 July	Jaysen Gonzales @ 1541 on 11 July	Jeff Vogelpohl @ 1750 on 11 July
Raul Vallejo @ 2014 on 11 July	Cindy Gillam @ 2212 on 11 July	Travis Samuelson @ 1517 on 11 July
Cathy Glover @ 1357 on 18 July	Dariela Maldonado @ 2156 on 22 July	Scott Smith @ 0910 on 23 July

Other notable attempts:

Rebecca Gonzales got 9 out of 10 questions at 1345 on 11 July.

Aaron Campbell got 8 of the 10 questions at 1807 on 30 July.

Melanie McDermott got 5 of the 10 questions at 1027 on 12 July.

Michelle Fisher got 4 of the 10 questions at 1212 on 11 July.

Cyber Challenge

Last Month's Challenge Answers

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

1) I am known as '**the homeless hacker**' because I used coffee shops, libraries and internet cafes as my base. Most of my activities involved breaking into computer networks and then reporting on their vulnerabilities to the companies that owned them. Who am I? **Adrian Lamo**

2) I am known as "**Mafiaboy**". When I was 15-years-old I discovered how to take over networks of university computers and used their combined resources to perform a Distributed Denial of Service (DDoS) attack on Dell, eBay, CNN and Amazon. Who am I? **Michael Calce**

3) At the age of 17 I hacked into the Pentagon's computer network known as ARPANET. Seven years later I hacked a radio station contest and ensured I was the 102nd caller. I won a brand new Porche, a vacation, and $20,000. I use the alias **Dark Dante**. Who am I? **Kevin Poulsen**

4) I am best known as **Mudge**. I was the most prominent member of the hacking group L0pht and a longtime member of the hacking group the Cult of the Dead Cow. I was a pioneer in buffer overflow work and was the original author of the password cracking software L0phtCrack. Who am I? **Peiter Zatko**

5) I am a virus writer from Belgium known for a long-standing dispute with the security firm Sophos because of a comment about the gender of virus writers made by Graham Cluley, a Sophos employee. I wrote the viruses Quis, Coconut and YahaSux (also known as Sahay). I also wrote the virus Sharp (also known as "Sharpei") which is credited as being the first virus written in C#. I'm best known as **Gigabyte**. Who am I? **Kimberley Vanvaeck**

6) I am a German hacker who's death was ruled a suicide. However, peers of mine from the Chaos Computer Club and others believe I was murdered because my activities in the areas of Pay TV cracking and voice scrambling might have upset intelligence agencies and organized crime operations. I presented the first public implementation of a telephone with built-in voice encryption. I went by the pseudonym '**Tron**'. Who am I? **Boris Floricic**

7) I am an American Cyber Security Researcher and White Hat Hacker. I am a founding member of the hacker security think tank L0pht Heavy Industries and was one of the seven members who testified before the U.S. Senate committee on Governmental Affairs in 1999 about government and homeland computer security. I made the statement my group could "take down the internet within 30 minutes." I am known as **Space Rogue**. Who am I? **Cris Thomas**

8) I am a hacker known as **MinorThreat** or **mthreat**. I am also a software developer and was the first employee and lead software architect for indeed.com. In 1995 I was sentenced to 70 months in the Federal Correctional Institute in Bastrop for money laundering and banned from the Internet; thus becoming the first person to be banned from the Internet even though I was not tried and did not please guilty to any computer crimes. Who am I? **Chris Lamprecht**

9) I am a hacker known as **geohot**. I developed limera1n, a jailbreak tool, and bootrom which allowed people to unlock iPhones to be used on other wireless carriers. This was contrary to AT&T and Apple's intentions. I also reverse engineered the PlayStation 3 and was sued by Sony. I am currently working on my vehicle automation machine learning company comma.ai. Who am I? **George Hotz**

10) I am a hacker known as **Sabu**. I am the co-founder of the hacking group LulzSec and was facing a 124 year prison sentence so I became an informant for the FBI. I spent over ten months helping the FBI identify and build cases against other hackers in LulzSec and other related groups. My help enabled the arrest of 5 other hackers associated with Anonymous, LulzSec and Antisec. Who am I? **Hector Xavier Monsegur**

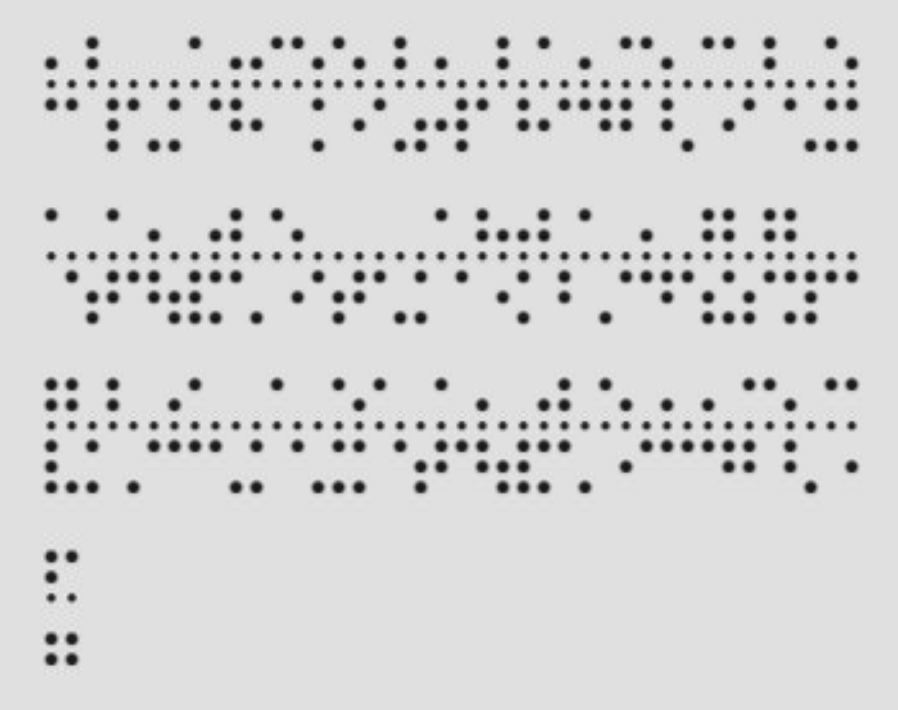
Cyber Challenge

This Month's Challenge

As you can see below, this month's challenges are a mixture of straight forward questions as well as a few puzzles to solve and is on two pages. Don't forget to do the two challenges on the next page.

A regular reader suggested the image puzzles. To keep him from receiving hate mail, I will not give his name. :) It is a very interesting code to use. As a hint, it is based off of the telegraph. Hopefully you will find the challenges fun and learn something from them.

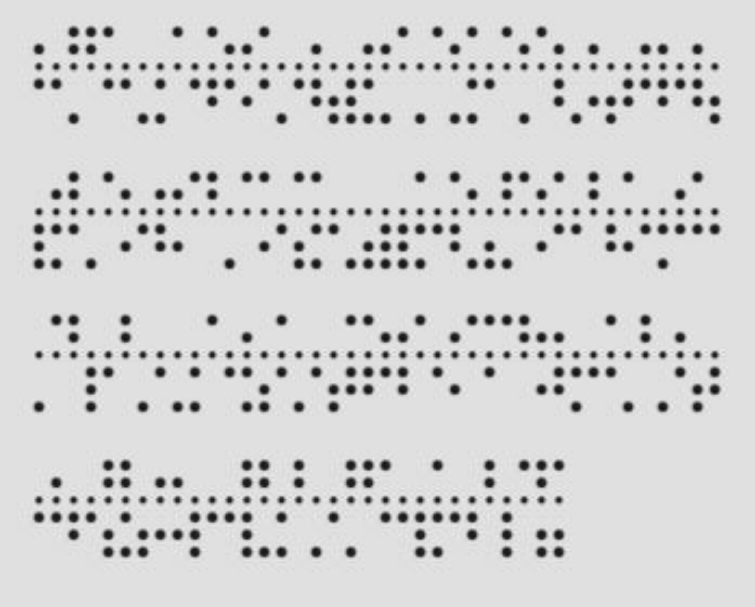
1. While not what would be considered a computer by today's standards, I was designed between 1847 and 1849 but was not built till 1991 when the London Science Museum built me. I am driven by a crank handle and contain cogs, gears and levers. I accurately calculated and printed tables of polynomials that were used for astronomy and ballistics. What am I?
2. In 1971 I made history by creating a program that is widely accepted as the first ever computer WORM. The worm bounced between computers and was not malicious. The worm displayed "I'm the creeper: catch me if you can." on affected computers. Who am I?
3. In 2002, President George W. Bush filed a bill to create this department. The department took on the responsibilities for IT infrastructure and eventually created a division specifically for cybersecurity. What is the Department?
4.



Cyber Challenge

This Month's Challenge Continued

5.



6.

Don't forget that you can always email me for hints to solve the challenges. :)

</Closing Comments>

As always, thank you for taking the time to read the newsletter. Cybersecurity is a very misunderstood subset of the Computer Science/Information Technology field. It is not uncommon to find computer professionals who are oblivious of cyber dangers or even why they are a danger. Demystifying and education about cybersecurity issues are some of the reasons I originally created this newsletter. Education is an essential part of helping users understand cybersecurity dangers and helps people better protect themselves and where they work.

Public awareness of dangers, such as those with IoT devices, can cause product change to occur. Knowledge of problems can cause enough consumer outrage that it forces manufacturers to improve safety of their products for the consumer. It puts the onus for protecting consumers on the manufacture where I believe it belongs. To quote an old adage, "knowledge is power" and with knowledge change that benefits everyone can occur.

As a final closing thought I want to talk about an article I found about Miami police body cam videos for sale on the darkweb. A terabyte of body cam videos was leaked from an unprotected, internet-facing database. To give you some context, a terabyte could hold approximately 500 hours of video. The videos were found on five different cloud service providers sites and was then sold on the DarkNet. I don't think I need to elaborate for people just how bad a thing this is, but take a minute to think about what the political and legal backlash from something like this happening to DPS would be. Researchers have found and reported on several vulnerabilities of body cameras and have been reported and discussed at conferences such as DefCon. The vulnerabilities range from making it possible to stalk officers and figure out when a raid is about to be conducted, to being able to modify the videos.

There is much more than can be discussed about this topic. To get an idea about what happened to Miami and the cyber dangers for body cams you can visit these websites:

- Miami police body cam videos up for sale on the darkweb
- 1 TB of Police Body Camera Footage Found on the DarkNet
- Hackers can infiltrate police body cameras to tamper with evidence

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.

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.