NEWS
Cyber Security
Vol. 3 | Issue 2 February 2018

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

This month I have selected a few articles I believe you will find of interest and hopefully beneficial in some way.

As you can see below, there is an article about an Ohio man who was charged with putting spyware on computers. This is not the first time something like this has happened, but most people are unaware it is possible and could be unknowingly broadcasting content across the Internet that they would rather not.

The first article on the next page is about Phishing and how Harris County fell victim to a Phishing/Social Engineering campaign that almost cost them $900,000. The next article on that page brings to light some of the vulnerabilities to IoT (Internet of Things) devices and how they can be dangerous to YOU. I follow that with a disturbing article about Strava. You might have heard about this in the news. While the article talks about the danger to military bases, I want everyone to think about how these types of devices could be a danger to you as well as work related things.

On the next page I posted an article about Ford Motor Company trying to patent driverless police cars. I figured that would be of interest to most DPS employees. The second article on the third page is about Uber's implementing of two-factor authentication and how a flaw could compromise users. The final security article is about Firefox. If you are a Firefox user you should insure your browser is up to date to protect you from a dangerous security flaw.

I hope you find these articles of interest. Feel free to email me and let me know if you enjoy the content and/or what you might like me to discuss in future newsletters.

Kirk

Ohio Man Charged With Putting Spyware On Thousands of Computers

A 28-year-old man who allegedly hacked into thousands of computers to watch and listen to users has been indicted in Ohio. Federal prosecutors say Phillip Durachinsky created malware that enabled him to remotely access and turn on the cameras and microphones of computers.

Durcachinsky was indicted in the U.S. District Court for the Northern District of Ohio. Prosecutors say he has been hacking into computers for over 13 years. A source close to the case, who spoke on background, says Durachinsky was working from the basement of his parents' house.

To read more click **HERE**.

Cyber News!!

Harris County tightens cybersecurity after almost losing $900K in phishing attack

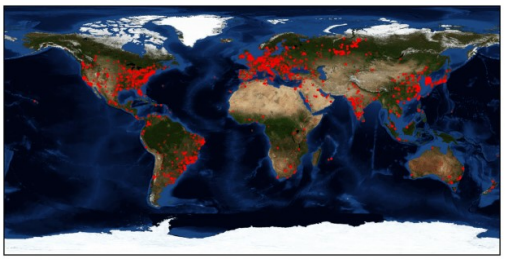
On Sept. 21, not three weeks after Houston was ravaged by Hurricane Harvey, the Harris County auditor's office received an email from someone named Fiona Chambers who presented herself as an accountant with D&W Contractors, Inc.

The contractor was repairing a Harvey-damaged parking lot, cleaning up debris and building a road from the country, and wanted to be paid. Chambers asked if the county could deposit $888,000 into the contractor's new bank account.

To read more click **HERE**.

New HNS botnet has already compromised more than 20,000 IoT devices

A new botnet called Hide 'N Seek (HNS botnet) appeared in the threat landscape, the malware is rapidly spreading infecting unsecured IoT devices, mainly IP cameras.



The HNS botnet was first spotted on January 10th by malware researchers from Bitdefender, then it disappeared for a few days, and it has risen over the weekend.

The number of infected systems grew up from 12 at the time of the discovery up to over 20,000 bots, at the time of writing.

To read more click **HERE**.

All your base are belong to us: Exercise app maps military sites, reveals where spies jog

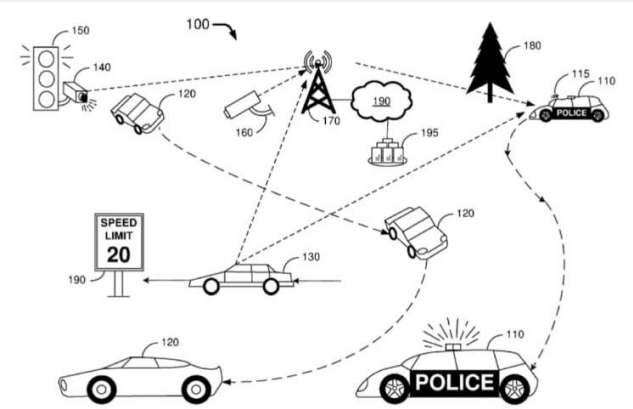
In November, exercise-tracking app Strava published a "Heatmap" of user activity which it cheerily boasted comprised a billion activities, three trillion lat-long points, 13 trillion rasterized pixels and 10 TB of input data.

It took a while, but late last week someone wondered "how many Strava users are members of the military or national security groups, and are uploaded their activity?" The answer is "plenty - and they've revealed where they work, where they live, when they were sent to a new outpost and where to ambush them when they least expect it."

To read more click **HERE**.

More Cyber News!!

Ford wants to patent a driverless police car that ambushes lawbreakers using artificial intelligence



Imagine a police car that issues tickets without even pulling you over.

What is the same car could use artificial intelligence to find good hiding spots to catch traffic violators and identify drivers by scanning license plates, tapping into surveillance cameras and wirelessly accessing government records?

What if a police officer tapping on your car window asking for your license and registration became a relic of transportation's past?

To read more click **HERE**.

Uber security flaw compromised two-factor authentication

Two-factor authentication only works if it's strictly enforced in software, and it sounds like Uber *might* have fallen short of that goal for a while. In a chat with ZDNet, security researcher Karan Saini has revealed a flaw in Uber's two-factor verification that reportedly rendered it useless. Saini has been keeping the exact details of the exploit under wraps to prevent abuse, but it revolved around a vulnerability in how Uber authenticates users when they sign in. The net effect was clear: an intruder might have only needed your username and password to sign in, giving them the chance to swipe personal info or misuses services.

{original article has been deleted}

I am hiding in code!!!

Firefox 58.0.1: Mozilla releases fix for critical HTML hijack flaw

Mozilla has fixed a critical flaw in Firefox that could allow a remote attacker to execute arbitrary code on a targeted device.

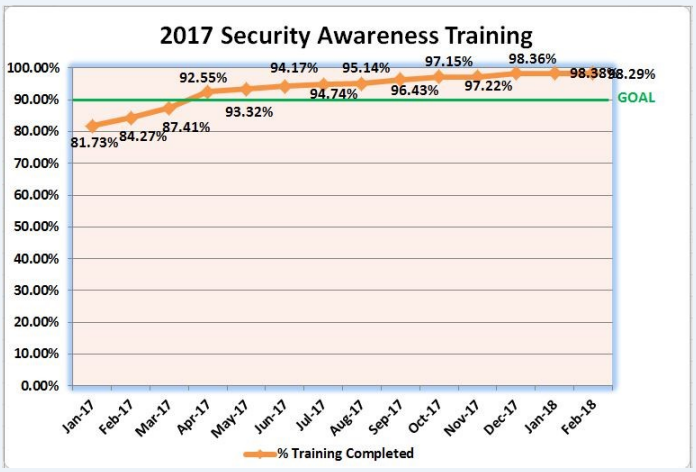
An attacker could exploit the vulnerability by persuading a user to access a link or file that then submits malicious input to the affected software, according to a security advisory from Cisco.

A successful exploit could allow the attacker to execute arbitrary code with the privileges of the user. If the user has elevated privileges, the attacker could compromise the system completely.

To read more click **HERE**.

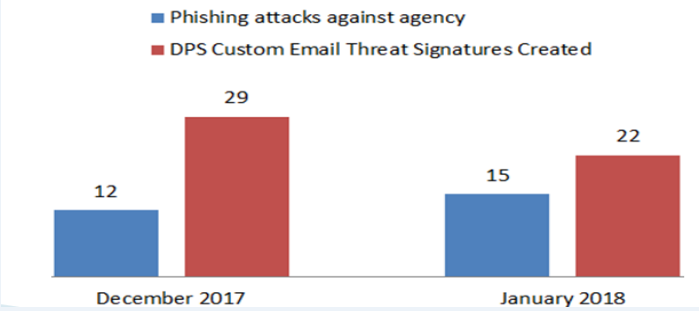
<Cyber Stats - Dec and Jan/>

Below is the graph on how the agency is doing overall with the online cybersecurity training. We have dropped to 98.29% complete from last month's 98.36% because of new hires who have not started the training yet. Overall the agency is doing well with the training but there are still people who are well behind their training requirement. For those of you who have not accomplished the training, please do so immediately so that we do not have to contact supervisors.

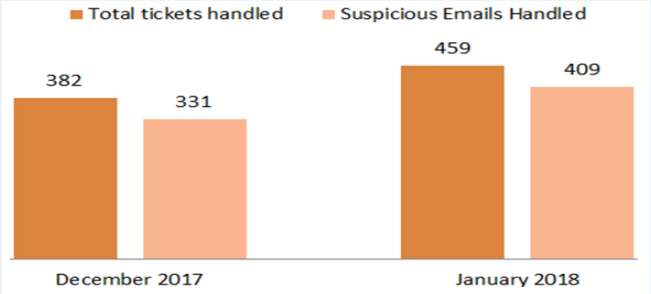


Other Statistics

There were 12 phishing attacks against DPS for the month of December and 15 for last month. While impossible to prevent all phishing attacks, we have increased the Threat Signatures by 29 in December and 22 more last month to help try to protect the Agency as well as all employees.



Another statistic I would like to tell everyone about are the number of suspicious emails sent to DPS. In December the agency received 331 suspicious emails and 409 in January. Because email numbers will vary significantly from month to month, the increase should not be alarming. Staying vigilant and reporting all suspicious emails as quickly as possible is the best way you can help us protect the agency.



Cyber Challenge

01000011 01111001 01100010 01100101 01110010 00100000 01000011 01101000 01100001 01101100 01101100 01100101 01101110 01100111 01100101

For those who tried to answer last month's challenge but were unable to, here is the answer:

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked"
— Richard Clarke

For those who were unable to figure out the code, here is how you can decode the message. I combined encodings that my predecessor, Jennifer, introduced in previous months. All the encoding can quickly be decoded through various websites. The code you saw in the newsletter was Binary. Once you converted it to text it gave you Hexadecimal. Once you convert that you got Base64. Finally, once you convert that you see the above message. Hopefully you were able to figure out the code and enjoyed the challenge. If you weren't able to finish, I encourage you to follow the steps above to complete the challenge.

For this month's challenge, I want to talk about Steganography. Steganography is a word derived from the Greek words steganos, or "covered," and graphie, or "writing." It can be thought of as the art of hiding something within something else while keeping it in plain sight. There are many ways to do this. The Greeks and Romans use to shave the heads of trusted slaves then tattoo messages on their scalps and let the hair grow back. The slave would then be used as a messenger with little fear of the message being found by enemies if the slave was stopped and searched. Obviously this method could only be used a couple of times before the scalp had no open space for messages.

In today's world Steganography has been used by governments, criminal organizations, and individuals. The messages are most often hidden in pictures, but that is **NOT** the only way to hide messages in plain sight. While not well known, Steganography is being used by terrorist and criminals. One of the most noted cases was an al-Qaeda operative who was detained in Germany in 2011 and found to be carrying plans for an attack stegged into pornographic movies. You can read more about the incident at this **CNN article**. There was a more recent report of ISIS relying heavily on Steganography for Operational Security. You can read more **HERE**. There is also evidence that drug cartels might be using Steganography to communicate.

For this month's challenge, I have hidden a form of Steganography in the newsletter. I will give you a hint: It is NOT one of the pictures. Have fun looking for the message.