Monthly Newsletter

March 2016 **Viruses and Anti-Virus Programs**

In This Issue

Website Links

Cyber Security Page

What is a virus?

Computer Crime Research Center

Virus Information

Sophos

Virus Total

F-Secure

Symantec

Anti-Virus Software

Sophos

AVG

Security Essentials

Contact Us

Cyber Security

kirk.burns@dps.texas.gov

Introduction

This month's DPS Cyber Security Newsletter focuses on Computer Viruses and Anti-Virus programs. There are a few questions I want to focus this month's training on. They are:

1) What exactly is a computer virus?
2) How can you get more information about them?
3) How can I protect my computer against viruses?
4) Is the free anti-virus software as good as the pay versions?

Computer Viruses

What exactly is a computer virus? A good definition is "a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data."

Simply put, it is a program that has been designed to do something malicious on a computer system. Often it is done behind the scenes without the user being aware there is something malicious occurring. All computers are vulnerable. It doesn't matter if you have a PC, Mac, Android or Linux computer; all are susceptible to catching a virus. Cell phones, tablets and even your smart TVs are vulnerable also.

Viruses can be programmed to do all kinds of things. The most common are deleting files, corrupting data, erasing everything on your hard drive, emailing itself out to other people, etc. Basically it is capable of doing anything that it is possible to program it to do.

It is difficult for the average person to identify a virus because viruses are rarely standalone programs or files. They are most often attached to a file and tailgate into a computer through email, instant messages, compromised USB drives or CD/DVDs. Viruses are often disguised as funny images, greeting cards, audio or video files, or any type of file that might be sent through email.

To find out more about viruses, click on the links on the left under Website Links.

Anti-Virus Software

The best way to protect any computer from a virus is to keep the Operating System (OS) up to date, have an anti-virus program installed that is up to date, and be wary of email attachments, Internet activity, and anything you connect to your computer.

Other than vigilance, having good anti-virus software is probably the most

important thing you can do to protect your computer. There are several to choose from. Some are free, others are by subscription; and it is debatable which is better. Companies such as Symantec, McAfee and Kaspersky try to convince you that you need to purchase their software to protect your computer. While these are good programs, there are others that are just as good and free for personal use. AVG is a program that can be run on Windows, MAC or Android devices. Microsoft Security Essentials is a free program from Microsoft. Another program, which is what DPS uses, is Sophos. **Sophos** is free for personal use and will work on MAC or PC. The Cyber Security division strongly recommends this for your personal computers. You can find a link to it on the left side of the newsletter under Anti-Virus Software.

Remember, even with being cautions and doing everything right, it is still possible to get a virus. The only way to ever keep a computer completely safe is to turn it off and lock it in a vault. While that would work, it is definitely impractical. So always be cautious of what you do with your computer.

For more information

For more information and tutorials about this month's topics, please visit the Cyber Security website on dpsnet. And always remember to Do Good Cyber.

Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has been working in the IT field for over 16 years. Kirk has a BS in Criminal Justice, a BS in Computer Science, and a MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University, holds a current CISSP certification and is a member of the Texas Army National Guard.

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He will be happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.

Monthly Newsletter

September 2016 **Social Engineering**

In This Issue

Other Interesting Links

- Best Defenses
- Life Hacker
- YouTube
- Social-Engineer

Contact Us

Cyber Security

kirk.burns@dps.texas.gov

Introduction

Social Engineering is a non-technical psychological manipulation of a person (or people) designed to gather confidential information by breaking normal security procedures. ~~It is used to gather information about the person~~ and/or ~~where they work, for things like identity theft, fraud, compromising of computer systems, etc.~~ The gathered information is commonly used for identity theft, fraud, and to compromise computer systems.

A good Social Engineer can also be thought of as a good "con man" or interrogator. Social Engineers will research their victim(s) and decide what tactic will likely work best to get the information they desire. ~~The traditional techniques used are to appeal to the person's vanity or greed. However, the one that often works best is appealing to the victim's natural desire to be helpful.~~ Traditional techniques appeal to individual vanity or greed;However, the most successful attacks exploit our helpful human nature. This is especially effective when targeting people in service related positions.

Social Engineering Techniques

In a March 2000 article of the Washington Post, the well-known hacker Kevin Mitnick said "in more than half of his successful network exploits he gained information about the network, sometimes including access to the network, through social engineering." The weakest link in any security system is the human element.

All social engineering techniques are based on attributes of the human decision-making process known as **cognitive biases**. The term cognitive bias refers to a systematic pattern of deviation from the norm or rationality in judgment, whereby inferences about other people and situations may be drawn in an illogical fashion. Individuals create their own "subjective social reality" from their perception of the input. In simpler terms, an attacker will devise a scheme that seems legitimate but in reality is designed to cause the victim to deviate from what they would normally do and what they know is the right procedure.

The most common type of social engineering happens over the phone. However, that is not the only type. Individuals posing as exterminators, fire marshals, technicians and

Commented [A2]: "And/Or" isn't technically a thing.

Commented [A3]: Pikachu used Social Engineering.." It was Super Effective" lolz

Commented [A4]: I would recommend revising. This like may be helpful as well. (News Writing Guide) http://thenewsmanual.net/Manuals%20Volume%201/volume1_08.htm

Commented [A1]: Necessary ?

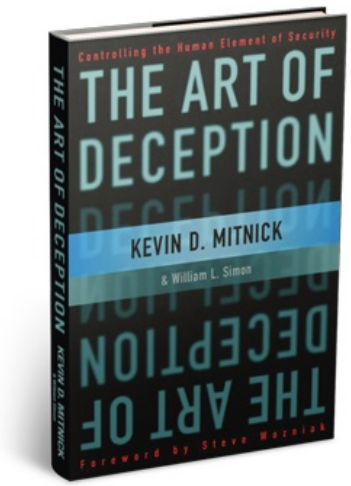
Commented [A5]: We can try using Bold or Italics if it needs to stand out.

Commented [A6]: [Phone; however,] is the best use of "however"

janitors, delivery people, etc., are also forms of social engineering. –Attackers will pose as these people because they are either overlooked or considered experts who should be left alone to do whatever it is they do. Exterminators, fire marshals, janitors, etc., are often let into areas without verifying their credentials, and often are left unsupervised while in those areas. And it isn't uncommon for a "technician" to be left unsupervised for hours at a time around computers. Thus, providing them the perfect opportunity to steal company secrets.

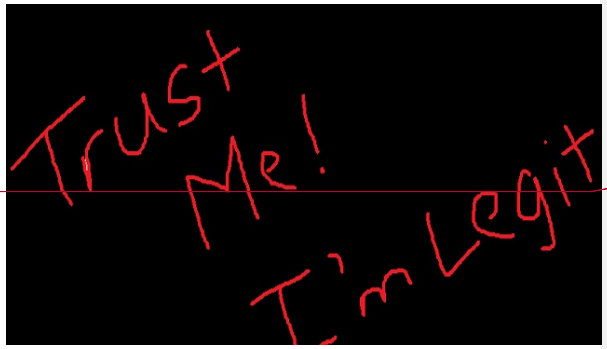
How is it done?

One example of social engineering is an individual who walks into a building and posts an official-looking announcement on the company bulletin board saying the number for the help desk has changed. Employees see this and call the "new number". The person who answers asks for the callers ID and login password to "verify" the person. Since the employee is calling what they think is an official number for the company help desk, the employee provides the information even though they know the help desk should not be asking for their login password. This provides the attacker with valid information they can then use to contact the real helpdesk and have complete access to whatever the employee has access to.



Another example is a woman calls a credit card company. In the background there is a baby crying. She says that she is needing to get some information because her husband is out of town and they are trying to buy a house. If she can't provide the information immediately the deal will fall through. She has some basic information but seems flustered and can't remember everything. The whole time the person on the phone can hear a baby crying. The woman apologizes about the baby explaining that it has been like this since early this morning. The person on the other end of the phone can sympothize and wants to help the poor woman, so shortcuts are taken and procedures bypassed to help her out. Account information is provided to the woman as well as passwords changed and new contact information provided. Thus locking the legitimate user out of the account and giving the caller complete access.

Another example is an attacker will contact a target on a social media site (Facebook, LinkedIn, Twitter, Tumblr, Pinterest, etc.) and start a conversation. Slowly and gradually the attacker gains the trust of the victim and then uses what they have learned to get access to sensitive information like the victims passwords or bank account information.



There are multiple examples that can be provided but the best way to truly understand is to watch it happening. This YouTube address will show you an example of how it is done

Commented [A7]: Ect in middle of sentence is followed by comma

Commented [A8]: Although allowed, I would recommend against beginning with a conjunction

Commented [A9]: As a personal tactic, I prefer to excite the reader with active voice or challenge in an informative section.

Commented [A10]: Bold?

Commented [A11]: I find this example very complex to read. I would recommend reconstructing flow.

Commented [A12]: Is multiple examples necessary? If so I would use simplify or shorten the example if possible.

Commented [A13]: Same^

(**https://www.youtube.com/watch?v=bjYhmX_OUQQ**). I suggest copying the link down and watching it at home since YouTube is blocked for most people on the TLE network.

Commented [A14]: It seems one detailed example of S.E is necessary and this think would be sufficient to express the idea. This would provide the resource, and substancially shorten the Article

How to protect against Social Engineering

Commented [A15]: Very good on this section!!!
I believe it may be the most important part of the article. If so, I would consider adjusting the flow of the newsletter to ensure the audience arrives.

There is no singular foolproof way to protect against Social Engineering. However, there are somethings that can help.

1) Education. The more you know the safer you are. **Social-Engineer.org** provides a number of information resources on social engineering attacks. The two most effective attacks used are posing as an internal employee or posing as someone hired to perform an audit or take a survey.

2) Be aware of the information you're releasing. This applies to social media as well as in person or over the phone. Social media is often the first thing looked at when researching for a social engineering attack.
3) Determine which of your assets are most valuable to criminals. Knowing what you have access to will help you be on guard for attempts to get it from you.
4) Awareness training. Security awareness training is always a good thing. ☺
5) Keep your software up to date. Your work computers are managed and kept up to date. But are your personal computers up to date? Unpatched and out of date programs and anti-virus software makes you vulnerable. Also be wary of anyone asking you about what version of software you are running or if you have the ability to update your software.
6) Security is everyone's business. We are all in the security business no matter what division you are in. Keeping our data, our employees and the citizens of Texas safe are part of our mission statement.
7) When asked for information, consider whether the person you're talking to deserves the information they're asking about. If you aren't sure, verify they are authorized to have the information before giving it to them. In most cases, someone you are talking to does not need to know what operating system you are using, what programs you have on your computer, or even what company handles trash collecting.
8) Watch for questions that don't fit the pretext. If a person asks a question that does not fit the persona they present, it should set off alarm bells. A sudden sense of pressure or urgency is often a sign they are trying to get unauthorized information.
9) If on the phone answering questions, consider putting the caller on hold for a minute. While this might not be the best customer service thing to do, it does break up the rhythm that a social engineer has going. Putting someone on hold also gives you time to collect your thoughts and ask your supervisor if this seems legitimate or not.
10) Stick to your guns. If you get the feeling that someone is fishing for information they shouldn't have, then you are probably correct.

Upcoming Cyber Projects

Commented [A16]: Maybe start on its own page?

Commented [A17]: This is an opportunity to use a catchy sentence. "Be Secure, Stay Involved"

I want to use this part of the newsletter to notify you of upcoming Cyber related projects.

- Online mandatory yearly cyber/CJIS awareness training. The training is in place and will soon be pushed out.

- All employees listed in HR as working in an IT field have received the training information.
- If you haven't received it already, all other employees should be seeing an email later today with instructions on how to take the training. You will have two (2) months to complete the training.

The online cyber/CJIS awareness training is a yearly requirement. Sometime after the beginning of the new year all accounts will be reset and you will be notified on when you have to have the training completed.

For More Information

For information, tutorials and contact information about this month's topics, you can click the links on the side of the newsletter. For other Cyber Security news, please visit the Cyber Security website. Remember that security is a shared responsibility and,

"**Do Good Cyber**".

Commented [A18]: Love the Flavor!

Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has a BS in Criminal Justice, a BS in Computer Science, and an MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University with over 16 years of IT experience. Kirk serves as a member of the Texas Army National Guard and holds a current CISSP certification.

Commented [A19]: I like it when you smile ☺

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He is happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.

Cyber Security Newsletter

December 2016 | Cyber Security Articles

In This Issue

Other Interesting Links

- Slashdot
- Security Week
- Security Now

Contact Us

Cyber Security Site

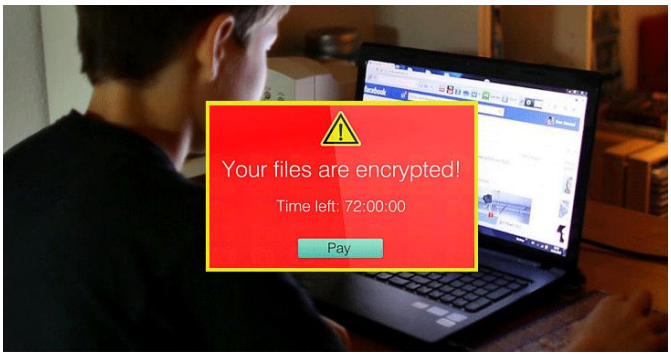
Security Awareness Email

Introduction

Last month's newsletter was a different format from previous newsletters. Several people gave positive responses to that format, so I decided to do the same thing this month. Below you will see several articles that I feel most people will find interesting. Hopefully everyone will find the articles informative and interesting.

Malicious images on Facebook lead to Locky Ransomware

CSO, 21 Nov 2016: Researchers have discovered an attack that uses Facebook Messenger to spread Locky, a family of malware that has quickly become a favorite among criminals. The Ransomware is delivered via a downloader, which is able to bypass whitelisting on Facebook by pretending to be an image file. The attack was discovered on Sunday by malware researcher Bart Blaze, and confirmed later in the day by Peter Kruse, another researcher that specializes in internet-based crime and malware. The attack leverages a downloader called Nemucod, which is delivered via Facebook Messenger as a .svg file. The usage of SVG (Scalable Vector Graphics) files, is important. SVG is XML-based, meaning a criminal can embed any type of content they want – such as JavaScript. In this case, JavaScript is exactly what the attackers embedded. If accessed, the malicious image will direct the victim to a website that appears to be YouTube in design only, as it's hosted on a completely different URL.



To read more click **HERE**.

Five Dollar Raspberry Pi-Based Hacking Device Can Break into Any Computer in Seconds

Softpedia, 17 Nov 2016: Passwords, iris scanning, and fingerprint protection, are all here to help protect a computer from unauthorized access, but all of these have been rendered useless by a device that costs only $5 to build. Samy Kamkar has shown in a video [**https://youtu.be/Aatp5gCskvk**] that it takes only a $5 Raspberry Pi Zero computer and free software to bypass protection on a computer using backdoor that's installed through USB. The hacking device is called PoisonTap and can emulate an Internet over USB connection that tricks the computer into believing that it's connected via the Ethernet.

To read more click **HERE**.

iOS Flaw Allows Anyone to Bypass iPhone Passcode and access photos and Messages

Softpedia, 16 Nov 2016: A new security flaw discovered in iOS allows pretty much anyone with access to your phone to bypass the passcode protection (it doesn't even matter if you configured Touch ID or not) and look at your photos or read the existing messages. Discovered by EverythingApplePro and iDeviceHelps, this glitch uses Siri to break into the device, and all it takes is a few simple steps. What's more important to know is that the same flaw exists on iOS 8 and newer, including 10.2 beta 3, but Apple is very likely to patch it in the next beta now that it has gone public

To read more click **HERE**.

Ransomware Piggybacking on Free Software Downloads

Graham Cluley, 15 Nov 2016: A ransomware sample is piggybacking off of free software downloaded from the internet to encrypt the files of unsuspecting users. A researcher by the name of slipstream/RoL discovered the ransomware, which goes by the name "Karma." Other ransomware samples have masqueraded as Pokémon Go apps or IT security software solutions in the past. They've done so to disguise themselves so that they trick users into thinking they're benign programs. Karma is no different, which is why it's donned the mask of a Windows optimization program known as Windows-TuneUp. All that remains is for the ransomware to catch users off-guard. It does this by bundling its fake Windows-TuneUp program with other downloadable software available on the web.

To read more click **HERE**.

Shazam for Mac Keeps the Microphone on Even After Users Manually Turn It Off

Softpedia, 16 Nov 2016: Shazam has become quite a popular app for those who want to find the name of a song in a second, but it turns out that Mac users are getting some extra features that they didn't necessarily ask for. Mac security expert Patrick Wardle has discovered that Shazam keeps the microphone enabled even after the user manually turns it off, which is undoubtedly worrying for users aiming for uncompromised privacy. The company, however, claims that the simple fact that the microphone stays on is a feature and not a bug, pointing out that the app needs to do that because, otherwise, it would take longer to load and users could miss a song they want to scan.

To read more click **HERE**.

DPS Cyber Security Assists Local High School Students in Preparing for National Youth Cyber Defense Competition

Earlier this fall, several DPS Cyber Security analysts teamed up with the Liberal Arts and Science Academy (LASA) here in Austin to work with students as part of the Cyber Patriot program. Cyber Patriot is a National Youth Cyber Education Program established in 2009 that strives to inspire students toward careers in cyber security or other science, technology, engineering, and mathematics (STEM) disciplines.

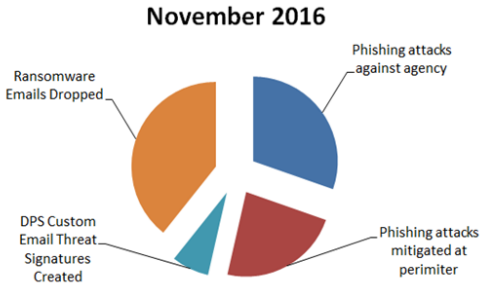
DPS Cyber Security analysts visit the LASA campus three times a week during their lunch hour to work with the high school students (mostly sophomores and juniors). The students are formed into two teams of six and are currently learning about advanced system hardening techniques and networking. Each Cyber Patriot team across the country trains to compete in the National Youth Cyber Defense Competition, which began its early rounds in November. In each round, teams are tasked with finding cyber security vulnerabilities and hardening a system while also keeping other computer functions and services (such as email) working over a six hour period. Teams can progress to the state level and even the National Finals that take place in Baltimore, MD in the spring, where they can earn national recognition and scholarship money.

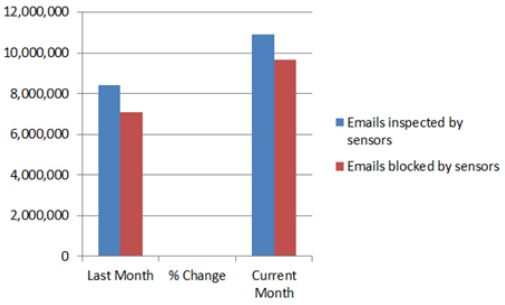
The LASA Cyber Patriot team recently competed in the first qualifying round of the competition. One team placed 175th and the other team placed 446th out of 2,000 teams nationwide. That means one of the teams placed in the top 10% in the country! The second qualifying round will be held in mid-December and offer a chance for the teams to move on to the State round in January. DPS Cyber Security is proud to be a part of introducing these students to an exciting and vital career!

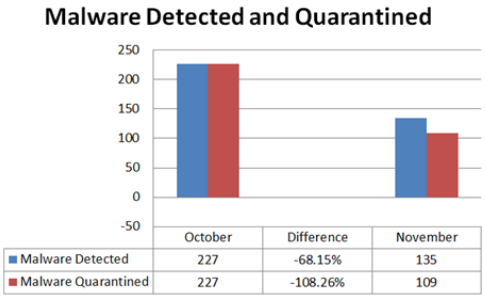
Cyber Security at work

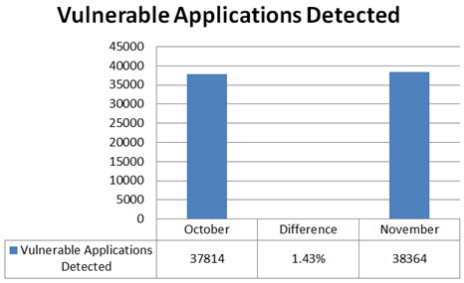
Are you curious about what kind of things Cyber Security is dealing with and protecting the agency from?

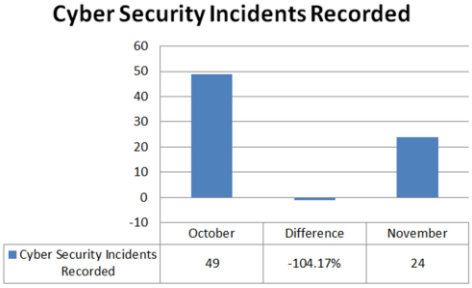
Here is some graphical information on some of the more important things we are able to release regarding what was handled within the last month.





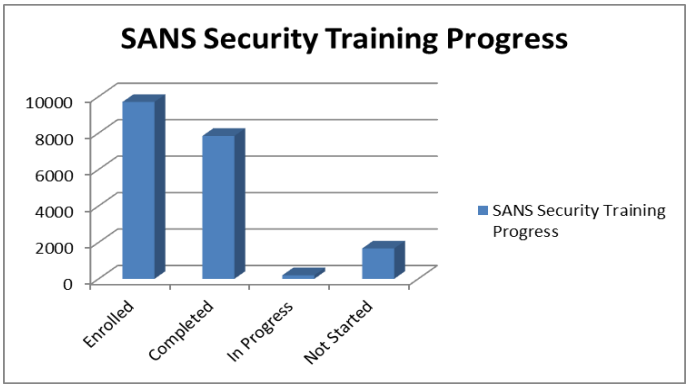






Important Information

SANS Securing the Human Online Training: As a reminder, this is yearly training that everyone who has access to the DPS network must take. If you have not taken the training in the last couple of months, you need to email **GRP_Security_Awareness_Training@dps.texas.gov** and someone will be happy to assist. Those that have already completed the training can expect to see a reminder they need to take the training again in about a year.



Cyber Security Awareness Training Officer: For those who don't know, I am also a pilot in the Texas Army National Guard. I am currently scheduled to be deployed to the Middle East after the first of the year. Others on the Cyber Security team will be taking over my duties while I am gone. January's newsletter, and all other newsletters until I get back, will be written and sent out by someone else on the team. I am confident that you will find those newsletters just as informative as mine have been.

For More Information

For information, tutorials and contact information about this month's topics, you can click the links on the side of the newsletter. For other Cyber Security news, please visit the Cyber Security website. Remember that security is a shared responsibility and,

"**Do Good Cyber.**"

Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has a BS in Criminal Justice, a BS in Computer Science, and an MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University with over 16 years of IT experience. Kirk serves as a member of the Texas Army National Guard and holds a current CISSP certification.

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He is happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.

NEWS
Cyber Security
Vol. 2 | Issue 1 January 2017

In This Issue

Interesting Links

Slashdot

Security Week

Security Now

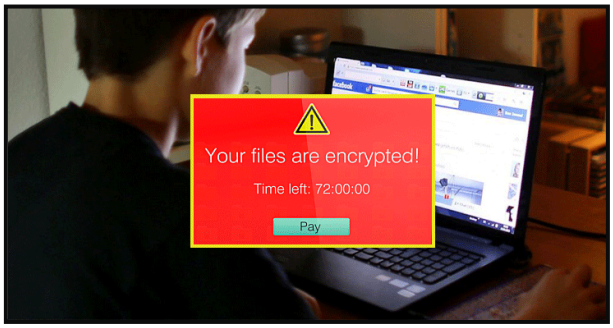
Contact Us

Cyber Security Site

Security Awareness Email

Malicious Facebook Images Lead to Locky Ransomware

CSO, 21 Nov 2016: Researchers have discovered an attack that uses Facebook Messenger to spread Locky, a family of malware that has quickly become a favorite among criminals. The Ransomware is delivered via a downloader, which is able to bypass whitelisting on Facebook by pretending to be an image file. The attack was discovered on Sunday by malware researcher Bart Blaze, and confirmed later in the day by Peter Kruse, another researcher that specializes in internet-based crime and malware. The attack leverages a downloader called Nemucod, which is delivered via Facebook Messenger as a .svg file. The usage of SVG (Scalable Vector Graphics) files, is important. SVG is XML-based, meaning a criminal can embed any type of content they want – such as JavaScript. In this case, JavaScript is exactly what the attackers embedded. If accessed, the malicious image will direct the victim to a website that appears to be YouTube in design only, as it's hosted on a completely different URL.



To read more click **HERE**.

DPS Cyber Security Assists Local Students

Earlier this fall, several DPS Cyber Security analysts teamed up with the Liberal Arts and Science Academy (LASA) here in Austin to work with students as part of the Cyber Patriot program. Cyber Patriot is a National Youth Cyber Education Program established in 2009 that strives to inspire students toward careers in cyber security or other science, technology, engineering, and mathematics (STEM) disciplines.

DPS Cyber Security analysts visit the LASA campus three times a week during their lunch hour to work with the high school students (mostly sophomores and juniors). The students are formed into two teams of six and are currently learning about advanced system hardening techniques and networking.

In each round, teams are tasked with finding cyber security vulnerabilities and hardening a system while also keeping other computer functions and services (such as email) working over a six hour period. Teams can progress to the state level and even the National Finals that take place in Baltimore, MD in the spring, where they can earn national recognition and scholarship money.

The LASA Cyber Patriot team recently competed in the first qualifying round of the competition. One team placed 175th and the other team placed 446th out of 2,000 teams nationwide. That means one of the teams placed in the top 10% in the country! The second qualifying round will be held in mid-December and offer a chance for the teams to move on to the State round in January. DPS Cyber Security is proud to be a part of introducing these students to an exciting and vital career!

Five Dollar Raspberry Pi Hacking Device

Softpedia, 17 Nov 2016: Passwords, iris scanning, and fingerprint protection, are all here to help protect a computer from unauthorized access, but all of these have been rendered useless by a device that costs only $5 to build. Samy Kamkar has shown in a video [https://youtu.be/Aatp5gCskvk] that it takes only a $5 Raspberry Pi Zero computer and free software to bypass protection on a computer using backdoor that's installed through USB. The hacking device is called PoisonTap and can emulate an Internet over USB connection that tricks the computer into believing that it's connected via the Ethernet.

To read more click **HERE**.

iOS Flaw Allows iPhone Passcode Bypass

Softpedia, 16 Nov 2016: A new security flaw discovered in iOS allows pretty much anyone with access to your phone to bypass the passcode protection (it doesn't even matter if you configured Touch ID or not) and look at your photos or read the existing messages. Discovered by EverythingApplePro and iDeviceHelps, this glitch uses Siri to break into the device, and all it takes is a few simple steps. What's more important to know is that the same flaw exists on iOS 8 and newer, including 10.2 beta 3, but Apple is very likely to patch it in the next beta now that it has gone public

To read more click **HERE**.

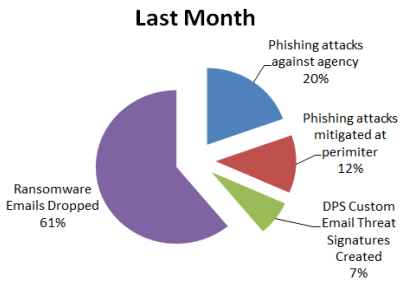
Ransomware in Free Software Downloads

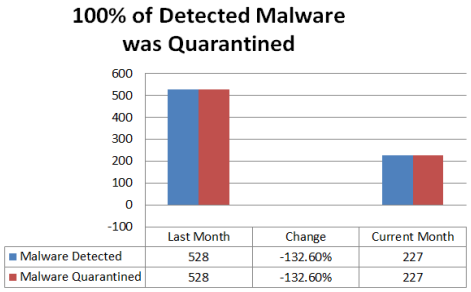
Graham Cluley, 15 Nov 2016: A ransomware sample is piggybacking off of free software downloaded from the internet to encrypt the files of unsuspecting users. A researcher by the name of slipstream/RoL discovered the ransomware, which goes by the name "Karma." Other ransomware samples have masqueraded as Pokémon Go apps or IT security software solutions in the past. They've done so to disguise themselves so that they trick users into thinking they're benign programs. Karma is no different, which is why it's donned the mask of a Windows optimization program known as Windows-TuneUp. All that remains is for the ransomware to catch users off-guard. It does this by bundling its fake Windows-TuneUp program with other downloadable software available on the web.

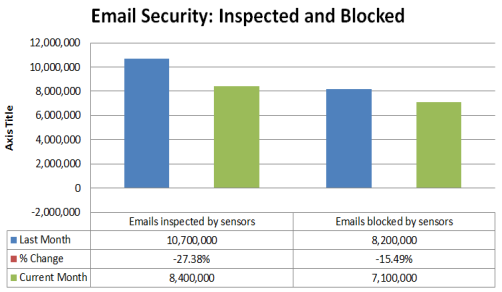
To read more click **HERE**.

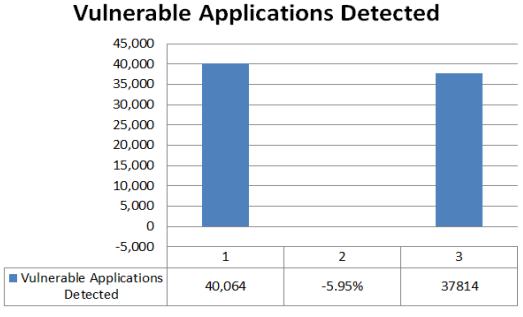
CYBER SECURITY AT WORK

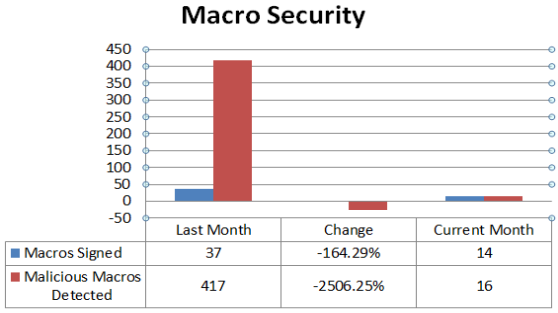
Are you curious about what kind of things Cyber Security is dealing with and protecting the agency from?
Here is some graphical information on some of the more important things we are able to release regarding what was handled within the last month.







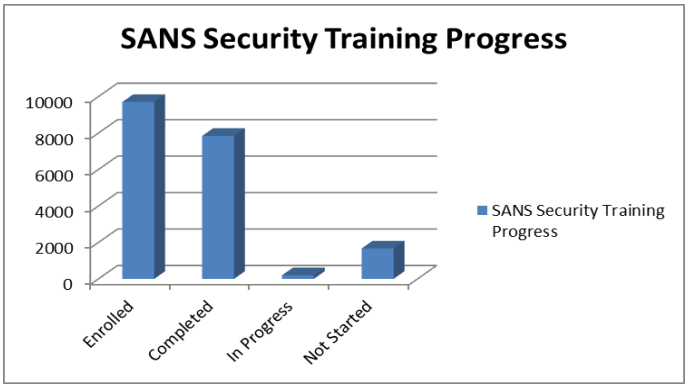




Important Information

SANS Securing the Human Online Training

As a reminder, this is yearly training that everyone who has access to the DPS network must take. If you have not taken the training in the last couple of months, email



GRP_Security_Awareness_Training@dps.texas.gov and someone will be happy to assist. Those that have already completed the training can expect to see a reminder they need to take the training again in about a year.

A Call to Duty

For those who don't know, I am also a pilot in the Texas Army National Guard. I am currently scheduled to be deployed to the Middle East after the first of the year. Others on the Cyber Security team will be taking over my duties while I am gone. January's newsletter, and all other newsletters until I get back, will be written and sent out by someone else on the team. I am confident that you will find those newsletters just as informative as mine have been

---

For More Information

For information, tutorials and contact information about this month's topics, you can click the links on the side of the newsletter. For other Cyber Security news, please visit the Cyber Security website. Remember that security is a shared responsibility and,

"**Do Good Cyber.**"

.

Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has a BS in Criminal Justice, a BS in Computer Science, and an MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University with over 16 years of IT experience. Kirk serves as a member of the Texas Army National Guard and holds a current CISSP certification.

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He is happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.

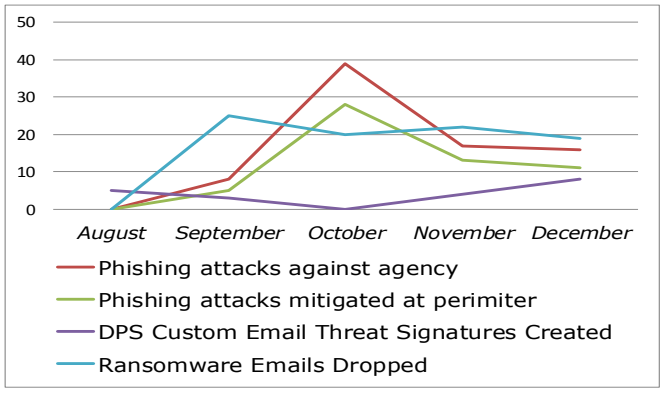
NEWS
Cyber Security
Vol. 2 | Issue 1
Jan/Feb 2017

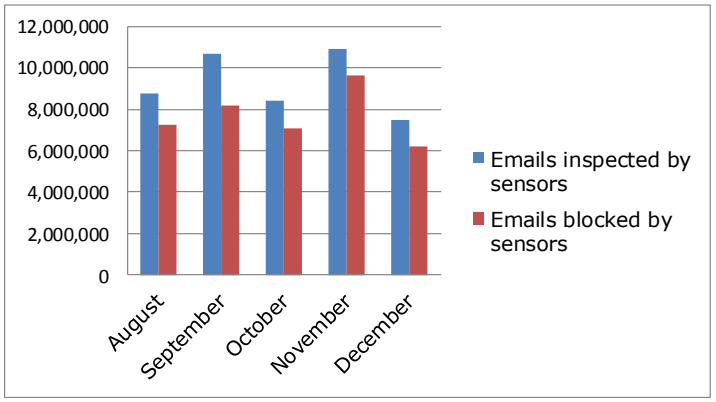
Year in Review

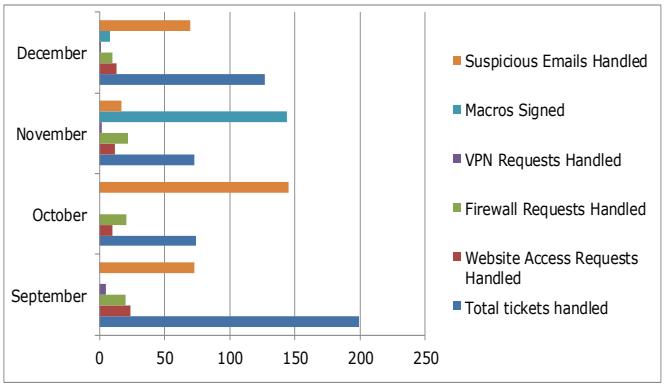
2016 was a year of many events - from the energetic Rio de Janeiro Summer Olympics; Brexit Referendum; Falcon 9 vertical landing; nail-biting Presidential election; and of all things, Russian hackers! It presented changes, and challenges to each of us, but above all else, it is important we remember the personnel, friends, and service members who worked around the clock to make Texas safer. Successfully executing the Department mission is no small feat, and I believe we all know a few persons worthy of applause.

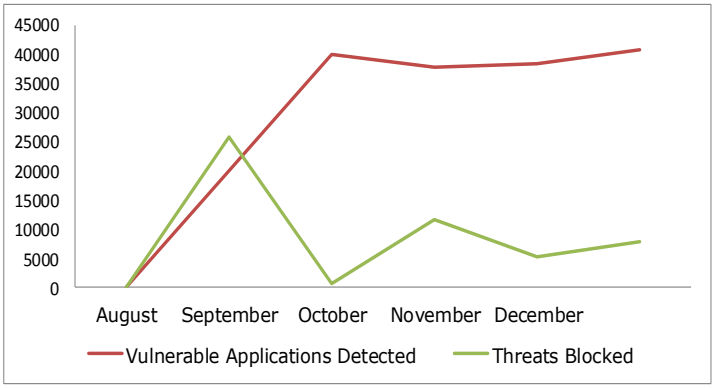
This article includes our aggregated end-of-year performance stats; highlights from 2016's most impactful data breaches; and a farewell toast to a Cyber Security staff member called to arms. Cyber Security hopes the future brings many opportunities to our readers, and you enjoy our Cyber Security Newsletter: 2016 Year in Review as much as we appreciate you reading it!

End of Year Cyber Security Stats









Breaches That Rocked 2016

Some of the most impactful breaches, hacks, and attacks worth remembering.

DNC HACK

OFFICIAL JOINT ANALYSIS REPORT

Hackers allegedly working with Russia's civilian intelligence service sent e-mails with hidden malware to more than 1,000 people working for the American government and political groups. U.S. intelligence agencies say that was the modest start of "Grizzly Steppe," their name for what they say developed into a far-reaching Russian operation to interfere with this year's presidential election. This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). The U.S. Government is referring to this malicious cyber activity as GRIZZLY STEPPE.

Note: Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities.

Review the official GRIZZLY STEPPE report: Click here.

Stolen Yahoo Data Includes Government Employee Information

Bloomberg Technology, 14 Dec 2016: More than 150,000 U.S. government and military employees are among the victims of Yahoo! Inc.'s newly disclosed data breach. It's a leak that could allow foreign intelligence services to identify employees and hack their personal and work accounts, posing a threat to national security. These employees had given their official government accounts to Yahoo in case they were ever locked out of their e-mail.

Learn more: Click here.

Hackers Hold Hollywood Healthcare Hostage

Lazarus Alliance, 19 Feb 2016: Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to hackers who seized control of the hospital's computer systems holding them a healthcare hostage. The assault on Hollywood Presbyterian occurred Feb. 5, 2016, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices.

Additional information: Click here.

Answering the Call of Duty

The New Year brings opportunities and challenges. For our very own Kirk Burns this principle is holding true. After receiving information of his call to active duty, covered in last month's newsletter, I pounced on the opportunity to interview the veteran. This article is the result of our impromptu interview and as many classic 'Kirk quotes' I could scratch down.

Late last year, the Cyber Security Training Officer received news of his forthcoming 2017 military deployment. For those who do not know, Kirk currently serves as a US Army Chief Warrant Officer 4. Destined for Afghanistan, I was stunned to learn this will be his forth Middle Eastern tour.

As we talked about his previous roles in Desert Storm and Desert Shield, I smiled at the subtle ironic similarity to most super hero comic classics (Minus the cape and tights of course). By day, the DPS Cyber Security Training Officer, but by night and some weekends, he is a US ARMY Black Hawk Pilot. Kirk has over 30+ years of aviation experience. Considering the aeronautical specialty, Kirk expects his role to be relevant to airspace management, but he is "preparing for anything".

This made absolute sense to me, but I remained curious to know if he perceived any cyber security or IT work on the horizon. 'Potentially' Kirk affirmed, "My role is pretty volatile". Many details of his deployment remain up in the air, but considering his rank, I would not be surprised if he can only provide a sanitized description.

CYBER SECURITY SHAREPOINT

Cyber Security is constantly seeking new and better ways to serve our customers. With this spirit to serve, we introduce our latest initiative: The Cyber Security SharePoint site. It streamlines information sharing by centralizing resources in one location. The site went live this month, and is routinely updated.

Check it out, and tell us what you think!

He will have already crossed the ocean by the time you read this article, but Cyber Security still asks you please keep our friend in your hearts and minds.

As our interview drifted into after work hours, and the office cubicles vacantly stand at solemn attention, I asked the Security Trainer if he had a message for his readers. "Remember your training," and with a firm, yet comforting smile, the Chief Warrant Officer replied, "**Do Good Cyber**". Thank you for your service, and safe travels Kirk!

He returns to us early 2018.

Connect with us	More Interesting Links	Visit the Website
For newsletter support contact Jennifer.Carson@dps.texas.gov	Slashdot Security Week Security Now	Check out our Website and SharePoint site for additional security information.

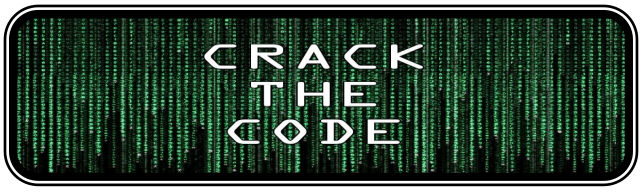
NEWS
Cyber Security
Vol. 2 | Issue 2 March 2017

Ransomware Infection Causes Loss of 8 Years of Police Department Evidence

The Police Department in Cockrell Hill, Texas admitted in a press release that they lost 8 years' worth of evidence after the department's server was infected with ransomware. The lost evidence includes all body camera video, and sections of in-car video, in-house surveillance video, photographs, and all their Microsoft Office documents.

The press release says the infection took place after an officer opened a spam message from a spoofed email address imitating a department issued email address. New-school security awareness training would highly likely have prevented this.

Read full blog article here.



Do you have what it takes to be a security professional? The newsletter Crypto Challenge engages our audience, increases security awareness, and is super fun!

"Frphevgl njnerarff vf bhe funerq erfcbafvovyvgl."

Crack the encryption; tell Jennifer your answer; and get a shout out in the next newsletter.

Hint: *"Julius Caesar did good Cyber"*

Cyber Spotlight

Calling All Cyber Champions!

Work or personal life, share with us your best and most exciting cyber stories. From how you keep your software up-to-date; learned something new about security; or even derailed a targeted social engineering attack. We love hearing from our readers, and want to give credit where credit is due!

Thank you for working hard, and remaining vigilant.

Submit your stories to Jennifer anytime!

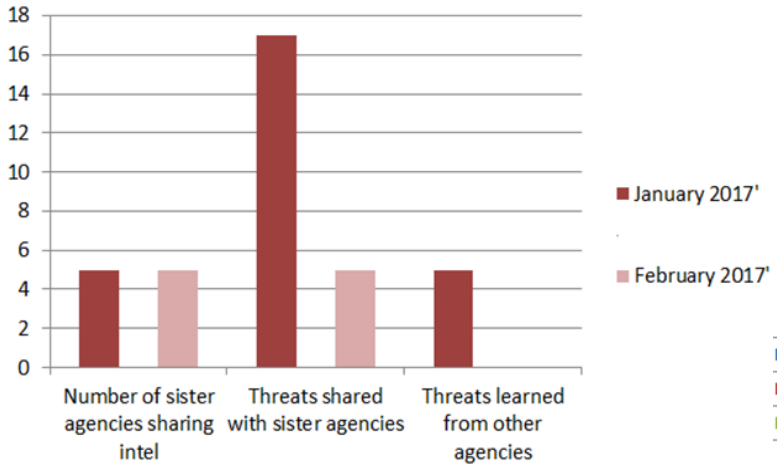
Choosing Secure Passwords

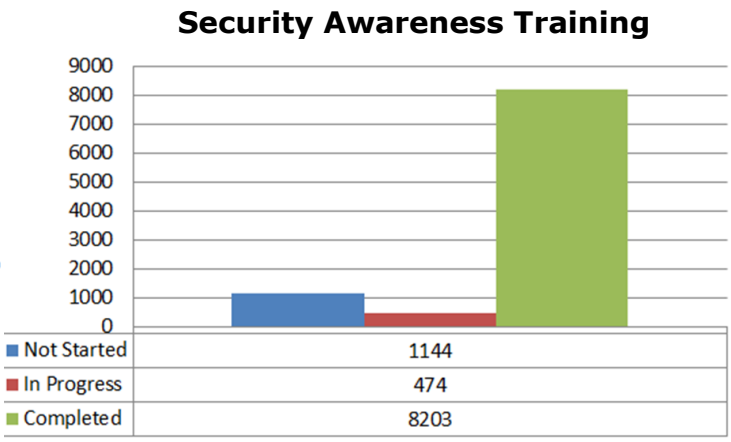
As insecure as passwords generally are, they're not going away anytime soon. Every year you have more and more passwords to deal with, and every year they get easier and easier to break. You need a strategy...

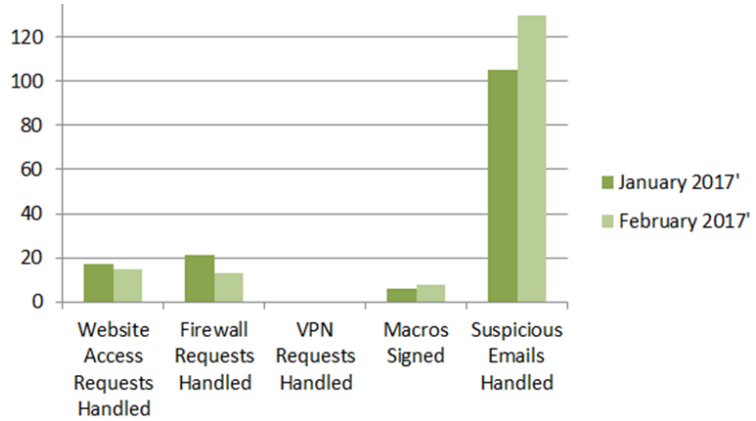
The efficiency of password cracking depends on two largely independent things: power and efficiency. **Power** is simply computing power. As computers have become faster, they're able to test more passwords per second; one program advertises eight million per second. These crackers might run for days, on many machines simultaneously. For a high-profile police case, they might run for months. **Efficiency** is the ability to guess passwords cleverly. It doesn't make sense to run through every eight-letter combination from "aaaaaaaa" to "zzzzzzzz" in order. That's 200 billion possible passwords, most of them very unlikely. Password crackers try the most common passwords first.

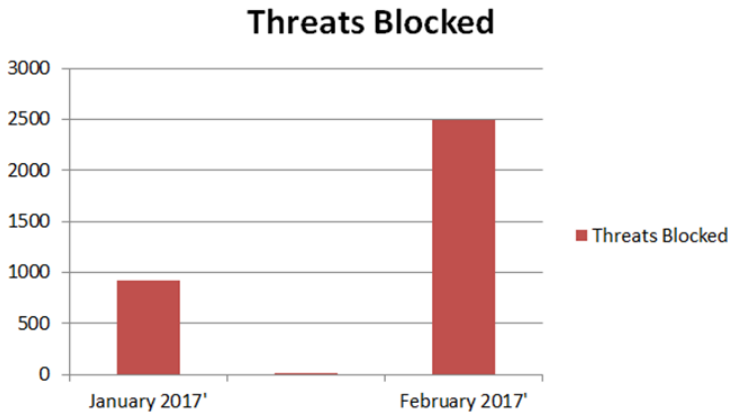
Learn to choose secure passwords by reading the full article here.

Cyber Security Stats: March 2017









W-2 Phishing Scam

The Internal Revenue Service (IRS), state tax agencies and the tax industry issued an urgent alert to all employers that the Form W-2 email phishing scam has evolved beyond the corporate world and is spreading to other sectors, including school districts, tribal organizations and nonprofits. Read the Official IRS alert here.

The IRS will never:

- call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the IRS will first mail you a bill if you owe any taxes

- threaten to immediately bring in local police or other law-enforcement groups to have you arrested for not paying

- demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe

- ask for credit or debit card numbers over the phone

Tax season is here and online scammers are in full force. Learn how to best protect your and your family from scams by reading the IRS Security Awareness For Taxpayers.

Connect with us	More Interesting Links	Visit the Website
For newsletter support contact Jennifer.Carson@dps.texas.gov	Slashdot Security Week Security Now	Check out our Website and SharePoint site for additional security information.

NEWS
Cyber Security
Vol. 2 | Issue 3 April 2017

How To Cyber: *Submit Suspicious Emails*

Receiving junk emails, a.k.a. spam, is an inevitable fact of conducting business. Sending annoying quantities of unsolicited emails is primarily a commercial practice, but it is also a popular avenue for malicious attackers. These phishing attacks are extremely successful, because differentiating between normal and malicious emails is difficult. Especially when they can originate from known and unknown sources.

In order to combat phishing attacks campaigned against the Department, Cyber Security created the following simple and safe procedure to check suspicious emails:

Step 1: Save It

In Outlook: Navigate to *File* > *Save As*, and store the file locally on your workstation.

Step 2: Attach It

Create a new email and attach the file.

Step 3: Send It

Tell us why it is suspicious and send the email to Spam@dps.texas.gov. We will do the rest!

Suspicious Email Indicators:

- Abnormal spelling or sentence structure
- Strangely named attachments or file formats
- Asking for your personal information
- Anything requiring you to login or provide your password

If an email is **suspicious** in any way, please complete this procedure. Cyber Security never misses an opportunity to neutralize potential security threats. In fact, our analysts enjoy the challenge. For more information, read our step-by-step guide, or reach out to use directly at CyberSecurity@dps.texas.gov.

Preventing phishing attacks is easy as pie...or 

Whichever you prefer.

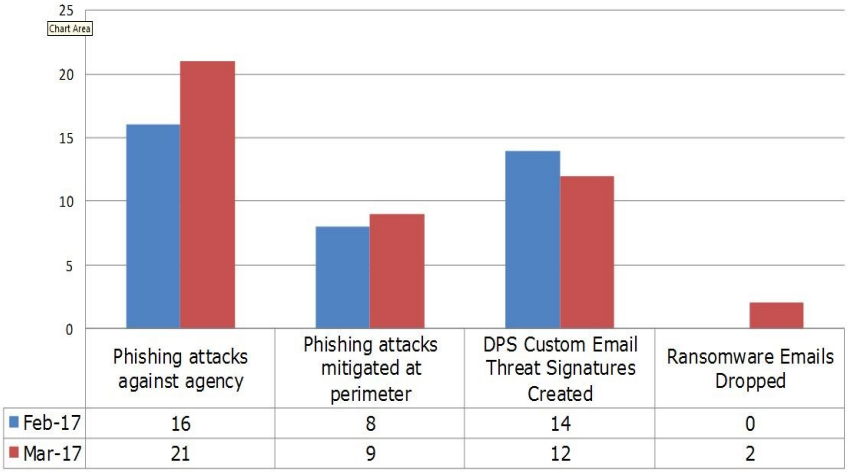
A Single Spear Phishing Click Caused the Yahoo Data Breach

A single click was all it took to launch one of the biggest data breaches ever. One mistaken click. That's all it took for a Canadian hacker aligned with rogue Russian FSB spies to gain access to Yahoo's network and potentially the email messages and private information of as many as 1.5 billion people.

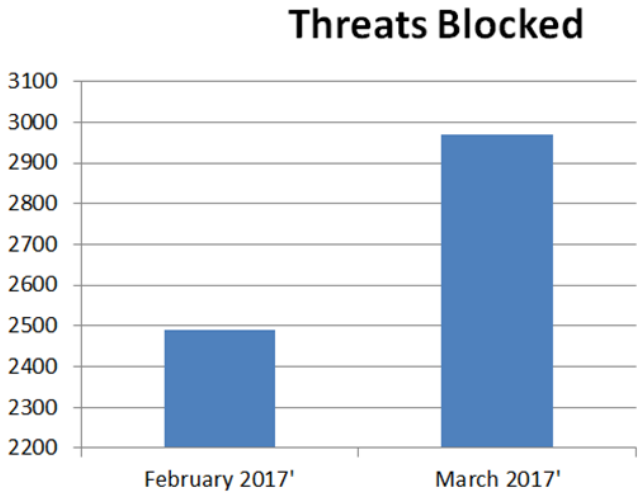
The U.S. Federal Bureau of Investigation has been investigating the intrusion for two years, but it was only in late 2016 that the full scale of the hack became apparent. The FBI indicted four people for the attack, two of whom are rogue FSB spies who work for the division that is supposed to cooperate with America's FBI on cybercrime investigations. (The FSB is the successor of the KGB).

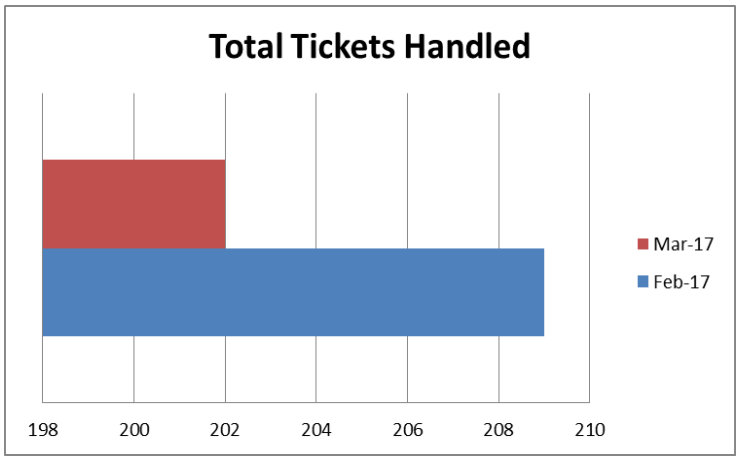
Read other relevant articles here.

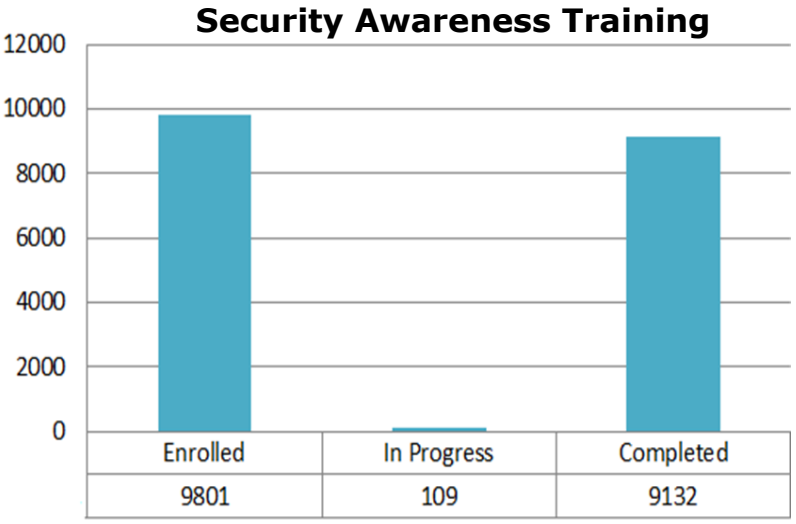
Cyber Security Stats: April 2017



	Phishing attacks against agency	Phishing attacks mitigated at perimeter	DPS Custom Email Threat Signatures Created	Ransomware Emails Dropped
Feb-17	16	8	14	0
Mar-17	21	9	12	2

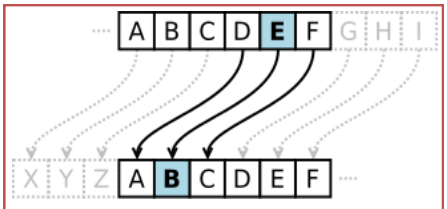






Crypto 101:
Showing the work

Sharpen your pencils, because *'Cyber-School'* is officially in session. Last month's challenge was a huge hit, and produced tons of great answers!



Note: Each letter corresponds with another letter. In essence, the cipher replaces letters by "shifting" around the alphabet! (Wiki)

For those who do not know, Crypto-Challenge 1.0 was a Caesar cipher. Named after Julius Caesar himself, this cipher is a basic encryption technique. It works by shifting letters of an alphabet against another alphabet. To keep it spicy for potential new readers, I will not provide the full solution; however, shifting the alphabet 13 rotations may be extremely helpful when decrypting last month's challenge.

Finally, kudos to all the readers and participants—especially our crypto challenge champions!

Challenge Champions: March 2017

B. Durham	*M. Allen*
D. Simpson	*R. Imhoff*
A. Baker	*D. Fout*
F. Carmichael	*M. Lherisson*
D. Palmer	*R. Flores*
S. Campbell	*J. Taylor*
D. Wright	*R. Dodson*
K. Schofield	*J. Crouse*
N. Gilbert	*A. Dooley*
S. Petty	*R. Hess*
M. Lucero	*T. Kingsley*
M. Lesko	*A. Shoop*
B. Gibson	*L. Foster*
D. Evans	*F. Davis*
C. O'Neal	*J. McClendon*
B. Means	*K. Patrick*
M. King	*M. Corona*
E. Baker	*J. Lavender*
J. Gomez	*C. Garcia*
E. Moriary	*J. Lockridge*
J. Norris	*E. Maestas*
D. Wade	*C. Herrera*
J. Kimbler	*M. Inabinet*
M. Saucedo	*D. Stefanov*
A. Burton	*E. Neumenn*
D. Conte	*W. Corona*
K. Sullivan	*R. Lytle*
V. Lawson	*G. Salinas*
B. Thomas	*B. Lewis*
A. Vazquez	*R. Snow*
T. Hampton	

Crypto Challenge 2.0

"MDEwMDExMTAgMDExMDAxMDEgMDExMTAxMTAgMDExMDAxMDEgMDExMTAwMTAgMDAxMDAwMDAgMDEwMTAwMTEgMDExMDEwMDAgMDExMDAwMDEgMDExMTAwMTAgMDExMDAxMDEgMDAxMDAwMDAgMDEwMTEwMDEgMDExMDExMTEgMDExMDExMTAxMDEgMDExMDExMTAwMTAgMDAxMDAxMDAgMDEwMTEwMDAgMDExMDAwMDEgMDExMDExMTAxMTEgMDExMDExMTAxMTEgMDExMDExMTExMTEgMDExMDExMTAwMTAgMDAxMDAxMDAg"

Hint: *"This challenge is 64 times the fun"*

Email Jennifer your answer, or if you need help. Good Luck!

Connect with us

For newsletter support contact Jennifer.Carson@dps.texas.gov

More Interesting Links

Slashdot

Security Week

Security Now

Visit the Website

Check out our Website and SharePoint site for additional security information.

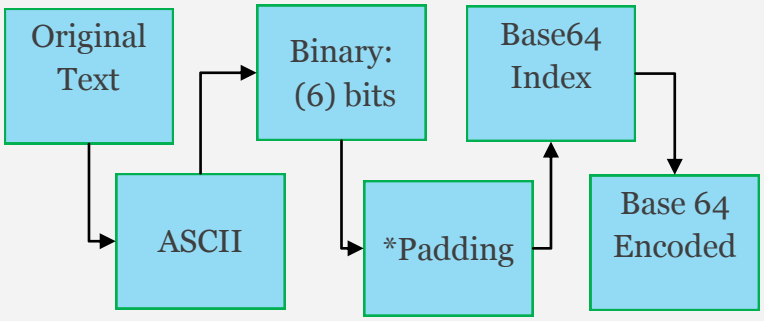
NEWS
Cyber Security
Vol. 2 | Issue 4 May 2017

Under Review
Crypto Challenge 2.0

Welcome to another Crypto Challenge review! Last month's challenge was difficult, but you rose to the occasion. Getting down to business, the challenge was obfuscated using Base64 encoding. This encoding type is very common and has many purposes. Email and web applications use it to convert binary files into text. However, this process is also maliciously used to hide malware code, and evade security measures.

Base64 Encryption: Overview

1. Convert each character to ASCII
2. Convert ASCII values to binary
3. Separate binary sequences into groups of 6 bits
4. Insert zeros when necessary—Padding
5. Reference each group to the Base64 Index,



Consider this only a primer on base64 encoding, but here is a fabulous base64 tutorial. Working it out by hand can be a long process, but honestly, it is not too difficult. Once you get the hang of it, decoding base-64 is surprisingly satisfying. For those checking their work or seeking instant gratification, you may want to use a "Text-to-Base64" encryption tool. Feel free to contact me if you ever get discouraged. I have some great tutorials and will gladly walk you through the process. Trust me, doing good Cyber isn't always easy, but it sure is fun!

Champions: April 2017

D.Wright| B.Means| R.Dodson
P.Vanney | D.Barber |W.Nichols
B.Pasmore |B.Shields | J.Norris
T.Kingsley | K.Schofield | J.Crouse
T.Hatch |D.Wade |E.Neumann
F.Krueger |S.Flores | M.Lesko
J.Carrillo |R.Maguire |J.Taylor
A.Shoop |J.Kimbler |J.Lavender
R.Hess| D.Evans |T.Siegmund
M.Millan| F.Carmichael |D.Curtin

RANSOMWARE

Most of us have heard of the WannaCry ransomware outbreak by now. Discovered around 4:00 AM EDT May 12, 2017, the WannaCry attack is still affecting various organizations around the world. Read the full United States Computer Emergency Readiness Team (US-CERT) analysis report here.

Ransomware is malicious software that encrypts critical system data and holds it for ransom – payable only in Bitcoins. This is a cruel method of criminal extortion when leveraged against vulnerable industries such as hospitals, telecommunications, and local law enforcement. Although the outbreak is most definitely newsworthy, the Department responded quickly and took actions to secure our network from WannaCry. Cyber Security wanted to take this time to highlight what really matters to us and our families: prevention. It is important we learn from this event and get serious about preventing ransomware.

Prevention

Keep software up-to-date

Maintain external backups of critical data

Do not click email links or attachments from unknown sources

WannaCry was effective because it indiscriminately 'wormed' to massive proportions by attacking any professional and private Windows workstations it touched. Here's the kicker, Microsoft had previously released a solution to protect against the exploits used by the WannaCry ransomware. The entire event could have been avoided if organizations and people had kept their software up-to-date and practiced good cyber 'hygiene'.

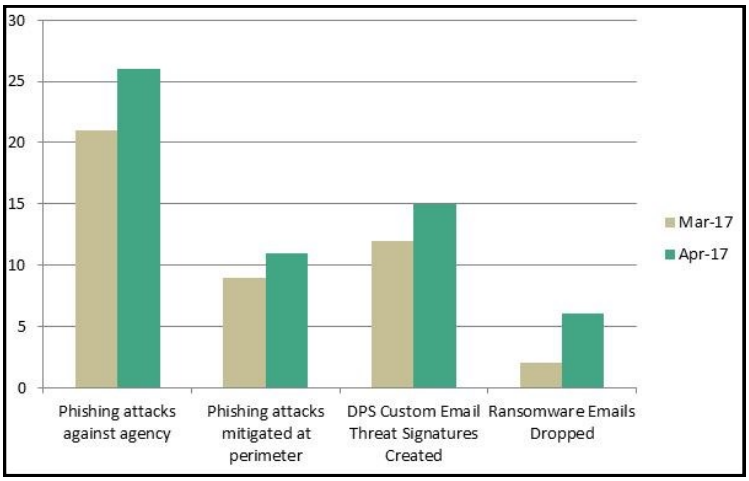
What's the moral of the story? Keep your software up-to-date. If you haven't already, here is how to update your windows systems.

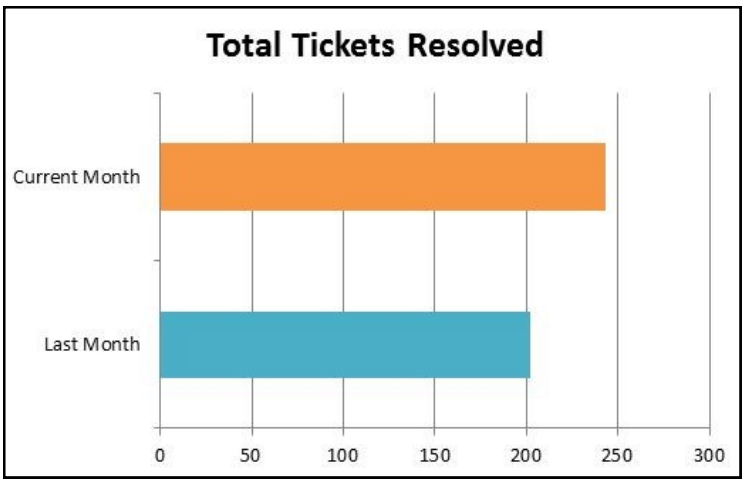
Windows Updates

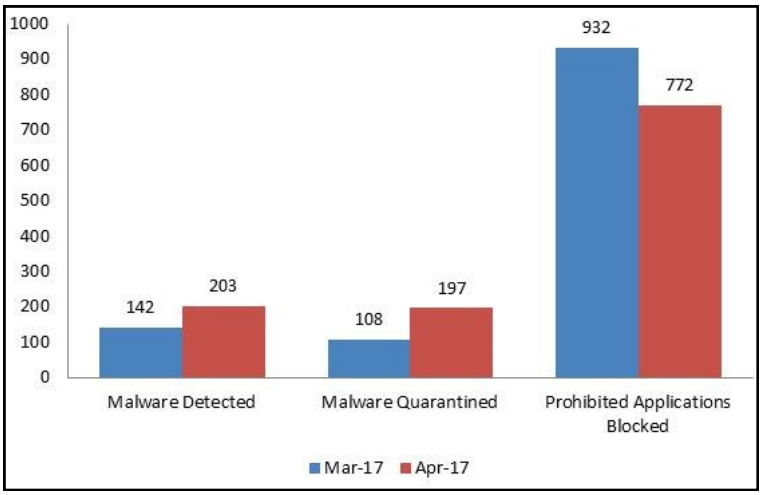
1. **Select the Start button**
2. **Go to Settings > Update & security > Windows Update**
3. **Select Check for updates.**

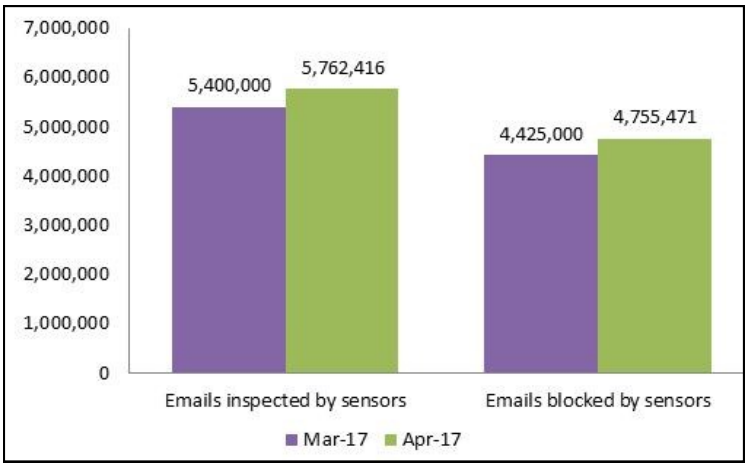
Secure.
Protect.
Inform.

<Cyber Stats />









New Cyber Twitter!

Introducing the new and super official Cyber Security Twitter account. Follow us for security news, updates, and threat intelligence. Check out our page here!

Newsletter Support

Jennifer.Carson@dps.texas.gov

Connect & Share

Website | SharePoint | Twitter