Vol. 3 | Issue 11

# Cyber Security NEWS

November 2018



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

Like always, I have picked articles for the newsletter based on what I feel is most appropriate for the average reader. I have included several articles most of you might find good to know about for your personal life as well as here at the agency. But before we get to the articles, our Cyber Technical Writer Ean Meacham and our Ops team asked me to include a couple of short information write ups for the newsletter. Ean's article about the CPAC is first and the next 2 pages are about Email Encryption. Feel free to email me if you have questions about the articles or anything else in the newsletter.

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

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

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

1. Policy identified
2. Cyber researches, develops drafts
3. Draft submitted to CPAC
4. Cyber compiles inputs, edits, or updates draft. Returned to CPAC for final review.
5. Policy draft approved by Cyber leadership
6. Policy draft sent to EPMO for routing and approval by DPS executive leadership.
7. Upon executive approval. EPMO updates General Manual.
8. CPAC distributes to divisional players for consideration and input. This step is your opportunity to be heard. The CPAC members are your way to have a say in how these policies are formed, as they may affect your current operations. If you would like to know who your member is and contact them, the members are listed below:

| | | |
|---|---|---|
| Chair | Aaron Blackstone | Aaron.Blackstone@dps.texas.gov |
| Secretary | Ean Meacham | Ean.Brown-Meacham@dps.texas.gov |
| Cyber Security | Miguel Scott | Miguel.Scott@dps.texas.gov |
| IT | Michael Lucero | Michael.Lucero@dps.texas.gov |
| LES | Mike Lesko | Mike.Lesko@dps.texas.gov |
| OGC | Cari Bernstein | Cari.Bernstein@dps.texas.gov |
| THP | Chris Nordloh | Chris.Nordloh@dps.texas.gov |
| ICT | Eric Baker | Eric.Baker@dps.texas.gov |
| Administration | Jessica Ballew | Jessica.Ballew@dps.texas.gov |
| TDEM | Jeff Newbold | Jeff.Newbold@dps.texas.gov |
| DL | Jeff Thiel | Jeff.Thiel@dps.texas.gov |
| CAO | Catherine Melvin | Catherine.Melvin@dps.texas.gov |
| RSD | Diana Burns | Diana.Burns@dps.texas.gov |
| TRD | Corey Lain | Corey.Lain@dps.texas.gov |
| OIG | Brian Lillie | Brian.Lillie@dps.texas.gov |

Security is an enterprise responsibility equally shared by all persons and Divisions. As such, Cyber values your input and welcomes your participation in security policy development. So reach out to your CPAC member.

# Email Encryption

Our Operations team asked me to include the following tutorial on how to Encrypt E-mails. The next two pages will give you information to encrypt emails. If you have any questions you can contact me or Grp_Cyber_Security@dps.texas.gov. Some will be happy to reply and answer your questions.

## Feature Highlight - Email Encryption

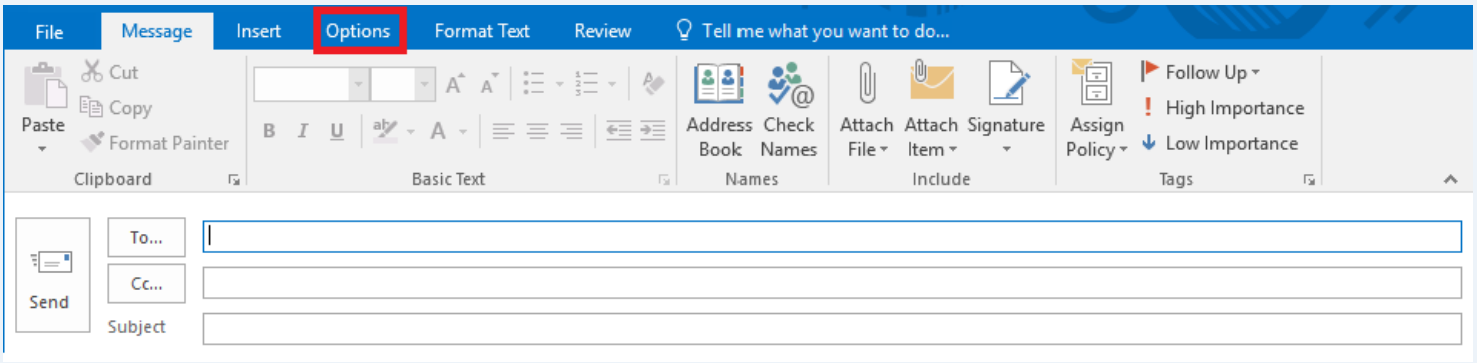
What is it? Email encryption involves encrypting, or disguising, the content of email messages in order to protect sensitive information from being read by anyone other than intended recipients. This is especially important when sending messages that contain sensitive, confidential and certain regulated information to recipients outside of the agency.

The General Manual, Chapter 26 section 26.120.00 DATA CLASSIFICATION policy (Information Resource Policy) defines sensitive, confidential and regulated data and provides examples (Chapter 26 Annexes) of each. If you have any questions concerning data classification, please contact the Cyber Risk and Vulnerability Management Team at GRP_Cyber_Risk@dps.texas.gov.

Fortunately, the feature to encrypt an email message is built into your version of Microsoft Outlook. With just a few steps, the content of your email is encrypted which gives you confidence that the intended recipient is the only person who will be able to read it. The intended recipient does not receive a traditional email within their mailbox. Instead, they receive a link to securely log into a portal where they can safely read and reply to the message. This feature is not to be overlooked as it provides an additional layer of security that prevents information from getting into the wrong hands.

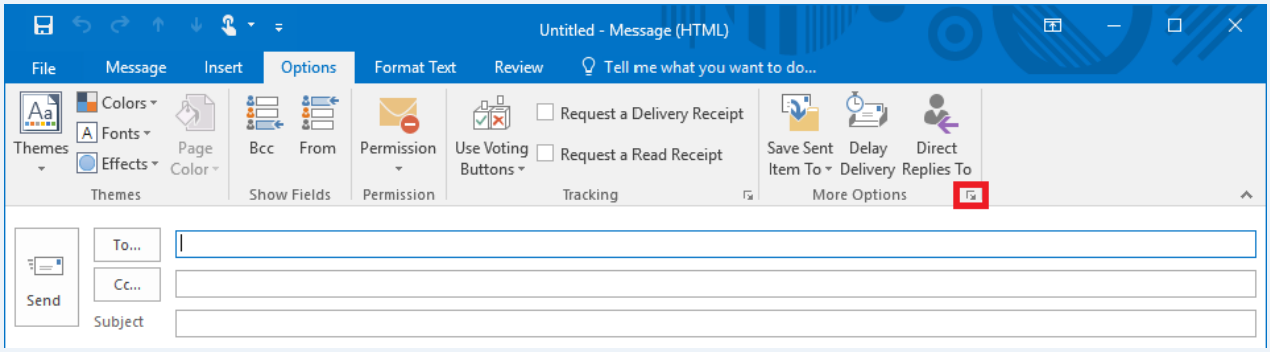
The steps provided below are for Microsoft Outlook 2016. Steps for Outlook versions 2010 and 2013 are similar but will not reflect the screenshots exactly. We will provide links to instructions for versions 2010 and 2013 at a later time.

**Step 1:** Begin by starting a new email and click the "Options" tab



# Email Encryption

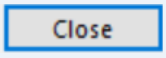
**Step 2:** Within the More Options section, click the icon in the right-hand corner




**Step 3:** Once the Properties window appears, click the "Sensitivity" drop-down menu


**Step 4:** Select "Confidential" from the menu list


**Step 5:** Click "Close". The email is now set for encryption and will be encrypted once the message is sent




If you encounter any difficulty with encrypting emails using this process, please contact the Service Desk at 512-424-5432.

For more information on this and other topics, DPS employees can visit our SharePoint site by going to https://dpsnet.tle.dps and clicking on our Cyber Security link.

# Facebook/TX Votes

## Senators tell Facebook to fix the bugs in its political ad system

**(by PCmag)**


Facebook's attempts to stop foreign governments from buying political ads on its platform appear to have major loopholes – and two Democratic senators are not happy.

On Friday, Sens. Amy Klobuchar and Mark Warner called on Facebook to fix the problem, which can reportedly let anyone buy political ads under almost any name you like, including ISIS or Vice President Mike Pence.

"It is increasingly clear that major gaps exist in Facebook's efforts, potentially allowing adversaries to exploit your platform with continued disinformation efforts," the senators wrote in a letter to Facebook CEO Mark Zuckerberg about the problems.

In April, Zuckerberg said Facebook would verify the buyers of political and issue-based ads on the platform. To get verified, you need to supply residential mailing address and a picture of a US passport or driver's license, along with the last 4 digits of your Social Security number.

In addition, Facebook began requiring political ads to list who sponsored the advertisement. The problem is that authorized political ad buyers can place almost whatever text they want in the "paid for by" field for the ad, according to *The New York Times*. This allowed one anonymous buyer to run attack ads against a Democratic congressional candidate in Virginia on Facebook using the name "A freedom loving American Citizen exercising my natural law rights…"

Click **HERE** to read the article.

---

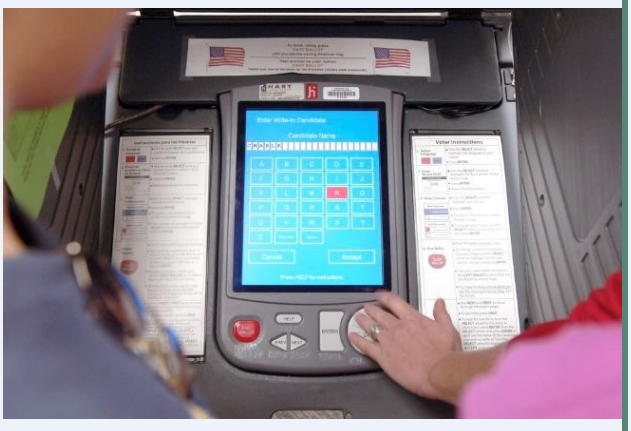
## Software bugs could compromise midterm votes in Texas

**(by Laura Hautala, OCTOBER 31, 2018 3:43 PM PDT)**

**It doesn't take a hacker to mess with voting machines. Sometimes the problem comes from within.**

A software flaw can be just as damaging to the voting process as a hacker.

That much is clear in Texas, where some early voters have claimed that machines are changing their votes in the midterm election. Keith Ingram, the Texas Director of Elections, said in an advisory that the problem is happening because voters are jumping the gun. The issue crops up if a voter selects the "straight party ticket" option, and then keeps pressing buttons before the page finishes loading on the screen, he said.



"As a reminder, voters should always carefully check their review screen before casting their ballots," Ingram said.

The complaints show that even though much of the public debate about voting machines has focused on whether they could be hacked, crummy software has the potential to undermine US elections as well. It's a problem for two reasons. First, it's nearly impossible to quickly patch bugs in voting machines when they appear this close to an election, experts said. And second, sometimes elections officials don't fix issues that they've known about for years. In the case of the machines used in Texas, voters have complained about the machines "flipping" their votes since 2008.

Click **HERE** to read the article.

# Google/MS Office

## Google Security Blog

**(Posted by Jonathan Skelker, Product Manager, October 31, 2018)**

It's Halloween and the last day of Cybersecurity Awareness Month, so we're celebrating these occasions with security improvements across your account journey: before you sign in, as soon as you've entered your account, when you share information with other apps and sites, and the rare event in which your account is compromised.

We're constantly protecting your information from attackers' tricks, and with these new protections and tools, we hope you can spend your Halloween worrying about zombies, witches, and your candy loot – not the security of your account.

**Protecting you before you even sign in**

Everyone does their best to keep their username and password safe, but sometimes bad actors may still get them through phishing or other tricks. Even when this happens, we will still protect you with safeguards that kick-in before you are signed into your account.

When your username and password are entered on Google's sign-in page, we'll run a risk assessment and only allow the sign-in if nothing looks suspicious. We're always working to improve this analysis, and we'll now require that JavaScript is enabled on Google sign-in page, without which we can't run this assessment.

Chances are, JavaScript is already enabled in your browser; it helps power lots of the websites people use everyday. But, because it may save bandwidth or help pages load more quickly, a tiny minority of our users (0.1%) choose to keep it off. This might make sense if you are reading static content, but we recommend that you keep Javascript on while signing into your Google Account so we can better protect you. You can read more about JavaScript here.

Click **HERE** to read more.

## Abusing Microsoft Office Online Video

**(by Avihai Ben_Yossef, October 25, 2018)**

Cymulate's research team has discovered a way to abuse the Online Video feature of Microsoft Word to execute malicious code (Read the press release here).


Attackers could use this for malicious purposes such as phishing, as the document will show the embedded online video with a link to YouTube, while disguising a hidden html/javascript code that will be running in the background and could potentially lead to further code execution scenarios.

This attack is carried out by embedding a video inside a Word document, editing the XML file named document.xml, replacing the video link with a crafted payload created by the attacker which opens Internet Explorer Download Manager with the embedded code execution file.

Click **HERE** to read more and see how this is done.

# History/Email Attacks

## New techniques expose your browsing history to attackers

**(by Help Net Security, November 2, 2018)**

Security researchers at UC San Diego and Stanford have discovered four new ways to expose Internet users' browsing histories. These techniques could be used by hackers to learn which websites users have visited as they surf the web.

```
class AttackPainter {
  static get inputProperties () {
    // Use the CSS font-family property as a communication channel from the main
    // script.
    return ['font-family'];
  }

  paint (ctx, geom, properties) {
    // Retrieve the key corresponding to the target URL.
    var targetKey = properties.get('font-family').toString();

    // Abuse registerPaint to perform a 1-bit swap operation in persistent state.
    try {
      // If the painter has *not* been previously executed for the given key,
      // this will set the bit for that key.
      registerPaint(targetKey, AttackPainter);
    } catch (e) {
      // Otherwise, a painter-already-registered exception will be thrown, telling is
      // the bit has already been set to 1.
      try {
        // Set another bit in persistent state marking the fact that the painter was
        // executed more than once for the given key. This will be observable from the
        // main script.
        registerPaint(targetKey + '_visited', AttackPainter);
      } catch (e2) {}
    }
  }
}

registerPaint('attack', AttackPainter);
```

The techniques fall into the category of "history sniffing" attacks, a concept dating back to the early 2000s. But the attacks demonstrated by the researchers at the 2018 USENIX Workshop on Offensive Technologies (WOOT) in Baltimore can profile or 'fingerprint' a user's online activity in a matter of seconds, and work across recent versions of major web browsers.

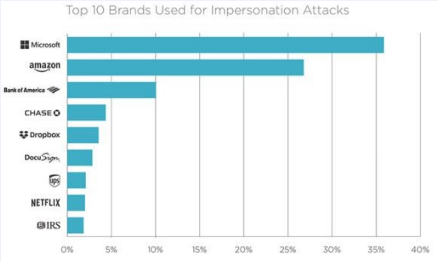
All of the attacks the researchers developed in their WOOT 2018 paper worked on Google Chrome. Two of the attacks also worked on a range of other browsers, from Mozilla Firefox to Microsoft Edge, as well various security-focused research browsers. The only browser which proved immune to all of the attacks is the Tor Browser, which doesn't keep a record of browsing history in the first place.

"My hope is that the severity of some of our published attacks will push browser vendors to revisit how they handle history data, and I'm happy to see folks from Mozilla, Google, and the broader World Wide Web Consortium (W3C) community already engage in this," said Deian Stefan, an assistant professor in computer science at the Jacobs School of Engineering at UC San Diego and the paper's senior author.

Click **HERE** to read more.

## Most impersonated brands in email attacks? Microsoft and Amazon

**(by Help Net Security, November 2, 2018)**




Nearly two-thirds of all advanced email attacks used emails impersonating Microsoft or Amazon, according to new research by Agari.

Microsoft was impersonated in 36 percent of all (brand) display name impersonation attacks in the third quarter. Amazon was the second most commonly impersonated company used in 27 percent of these attacks. Amazon and Microsoft run the largest public cloud computing platforms, which are widely used by companies undergoing digital transformation projects.

The pattern was different for high-value targets, such a C-suite executives - Microsoft was impersonated in 71 percent of these attacks. Dropbox is a distant second at seven percent, followed by UPS at si percent.

These attacks often take the form of service updates, security alerts and password resets. The ubiquity of Microsoft Office in corporate environments and the rapid adoption of cloud-based Office 365 makes Microsoft an attractive impersonation target, while file-sharing services such as Dropbox are frequently imitated to distribute malware because users are more likely to trust its installation.

According to the FBI, business email compromise (BEC) has become a $12 billion scam. Advanced email attacks, such as BEC, leverage identity deception techniques, including domain name spoofing, look-alike domains and display name deception to take advantage of end-user trust. Legacy email security solutions, such as secure email gateways (SEGs), are unable to detect advanced email attacks because they do not include malicious URLs or malware attachments - the attacks Agari identified in tis Q4 2018 report evaded detection by other email security solutions.

Click **HERE** to read more.

# MacBooks/Radisson

## Apple releases security updates, says new MacBooks will disconnect microphone when lid is closed

**(by Zeljka Zorz, Managing Editor, October 31, 2018)**


Apple unveiled new Macs and iPads on Tuesday and has pushed out security updates for macOS (Mojave, High Sierra, Sierra), iOS, watchOS, tvOS, Safari, iTunes, and iCloud for Windows.

Among the various vulnerabiliites fixed in an ICMP packet-handling vulnerability in the XNU kernel that could be exploited remotely to achieve code execution on, extract data from, or crash macOS powered devices (as demonstrated in the following video): {see video in article}

Closed MacBooks disable microphone

During the Apple event that presented the new devices to the world, Apple has also revealed that all new Mac portables (MacBooks) that have the T2 security chip built in automatically disable the microphone when the lid of the device is closed.

"This disconnect is implemented in hardware alone, and therefore prevents any software, even with root or kernel privileges in macOS, and even the software on the T2 chip, from engaging the microphone when the lid is closed," Apple explained.

"The camera is not disconnected in hardware because its field of view is completely obstructed with the lid closed."

Click **HERE** to read more.

## Check this out: Radisson Hotel Group 'fesses up to 'security incident'

**(by Paul Kunert 31 Oct 2018 at 10:58)**

Radisson Hotel Group has told members of its loyalty scheme that their personal details were exposed in a data breach.

The hotel chain and conferen e centre fave said it "identified" the security foul-up on 1 October, weeks after it happened on 11 September, but only emailed holders of the Radisson Rewards cards that are affected yesterday.

The mail sent ty the group stated:

**This data security incident did not compromise any credit card or password information. Our ongoing investigation has determined that the information accessed was restricted to member name, address (including country of residence), email address, and in some cases, company name, phone number, Radisson Rewards member number and any frequent flier numbers on file.**

The IT security breach affected a "small percentage" of the Radisson Rewards members, the email stated, but didn't provide any specifics about numbers.

The hotel chain said that when it identified the "issue" it immediately revoked access to the unauthorized person or persons.

"All impacted members accounts have been secured, and flagged to monitor or any potential unauthorized behavior. While the ongoing risk to your Radisson Rewards account is low, please monitor your account for any suspicious activity."

It added that loyalty card holders should also be cautious about potential phishing scams as miscreants may attempt to build on the information already gathered.

"Radisson Rewards takes this incident very seriously and is conducting an ongoing extensive investigation into the incident to help prevent data privacy incidents from happening again in the future."

Click **HERE** to read more.

# More News

**HHS IG supports adding cybersecurity to FDA criteria for medical devices**

http://federalnewsnetwork.com/federal-drive/2018/10/hhs-ig-supports-adding-cybersecurity-to-fda-criteria-for-medical-devices/

**Proper Disposal of Electronic Devices**

https://www.us-cert.gov/ncas/tips/ST18-005

**Chinese Intel Agents Indicted for 5-Year IP Theft Campaign**

http://www.darkreading.com/attacks-breaches/chinese-intel-agents-indicted-for-5-year-ip-theft-campaign-/d/d-id/1333166

**BLEEDINGBIT**

http://armis.com/bleedingbit/

**This one weird trick turns your Google Home Hub into a doorstop**

https://www.theregister.co.uk/2018/10/31/google_home_api/

**Tiny Twitter thumbnail tweaked to transport different file types**

https://www.theregister.co.uk/2018/10/31/twitter_thumbnail_code/

**iOS 12.1 extends controversial processor throttling feature to the iPhone 8, 8 Plus, and X**

https://mashable.com/article/apple-ios-12-1-iphone-8-8plus-x-battery-management/#YeiADFsoriqL

**Why 5G (and even 6G) could put your business at risk for a cyberattack**

https://www.techrepublic.com/article/why-5g-and-even-6g-could-put-your-business-at-risk-for-a-cyberattack/

**Google mandates two years of security updates for popular phones in new Android contract**

https://www.theverge.com/2018/10/24/18019356/android-security-update-mandate-google-contract

**U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections**

https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

# </Closing Comments>

## User Suggested:

The following articles are from Deborah Wright in CJIS. Thank you Deborah for sending me the articles. I would like to encourage other readers to suggest articles of interest to be included in the newsletter.

**The Cybersecurity 202: Pros to government: If your defenses fail, think pen and paper.**

https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/10/22/the-cybersecurity-202-pros-to-government-if-your-defenses-fail-think-pen-and-paper/5bcc91581b326b7c8a8d1ab3/?noredirect=on&utm_term=.7a5aa2a7ddda

**Amazon Pitches Facial Recognition to Monitor Immigrants**

https://www.bloombergquint.com/technology/amazon-pitches-facial-recognition-tools-to-monitor-immigrants#gs.sD4tzDU

**Yahoo agrees to pay $50M in damages over biggest security breach in history**

https://thehill.com/policy/technology/412800-yahoo-paying-50m-in-damages-in-biggest-security-breach-in-history

**Before You Connect a New Computer to the Internet**

https://www.us-cert.gov/ncas/tips/ST15-003

And finally, my favorite article submission. Click the link below then click on **Proper Disposal of Electronic Devices**

https://www.us-cert.gov/ncas/tips/ST18-005

---

Thank you for taking the time out of your busy schedule to read the articles in this month's newsletter. I hope you found all of them to be interesting and useful. Remember, you can only defend yourself against threats when you are knowledgeable about the threats. I realize cybersecurity is not the most liked topic by most people, but it is important to understand the dangers you and your family face when being online and how your actions and the actions of others can affect the Agency. Knowing about dangers such as the Most Impersonated Brands in Email Attacks, changes to Apple products, new Google features, large data breeches, understanding your hardware can covertly spy on you, etc. are all part of Cybersecurity Awareness Training. Everyone in the Agency has to take Cybersecurity Awareness training every two years, but the learning does not end when the online training is over. My hope is this newsletter provides a little more up-to-date information about Cybersecurity as well as making it a little more enjoyable than watching generic training videos online. Feedback on how to improve the newsletter is always appreciated, so feel free to email me with suggestions. If possible, I will implement them in future editions.

As I mentioned above, everyone has to take the online training every two years. I send out notifications monthly to people when it is time for their retraining. If you know you are coming up on your two year mark, please be on the lookout for the email. If you are unsure, feel free to email me and I will let you know when you are due retraining.

In closing, hope you enjoyed the newsletter and good luck with the Cyber Challenge on the next page. And as always, **Do Good Cyber!**

Kirk

# Cyber Challenge

## Last Month's Challenge

Apparently last month's challenge was more difficult than I thought it would be. I upped the difficulty level because so many people were solving the other challenges too quickly. There were several that solved the first and second challenge but **Deborah Wright** was the only person who solved the third challenge and notified me. There may have been others who solved the challenge, but they didn't email me with the correct solution.

For those who are curious about the answers to last month's challenges, here they are:

1) SamSam
2) The 5 cybersecurity practices every employee should follow:
    1) Realize you are an attractive target. Never think "It won't happen to me."
    2) Practice good password management.
    3) Never leave your devices unattended.
    4) Always be careful when clicking on attachments or links in email.
    5) Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, and on a network you trust.

3) For the third challenge, you have to open the newsletter in something other than Adobe Reader. This was a true Steganography challenge so it requires thinking outside the box to solve. Adobe Reader is the default program for pdf files but they can be opened with other programs also. On a Windows computer, if you **right click** on the pdf and pick **Open with** then pick **Notepad** you will see the message along with all of the stuff that makes up the pdf file. What you are looing for is all the information above the **%PDF-1.5** at the top of the file and below the **%%EOF** at the end of the file. As you can see from this challenge, it is possible to hide information inside a document and not realize it is there. In this case I hid the split message before the code to start the PDF file and after the End Of File. The message is encoded but says:

**In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters.—Jeff Jarmoc**

This quote is in reference to the Internet and how Internet of Things (IoT) devices are making it vulnerable. Now that you know how it is done, feel free to go try this out for yourself. You can find last month's newsletter at: http://www.dps.texas.gov/InformationTechnology/Cyber/Newsletters/2018/2018-10.pdf

For this month's challenge, I have hidden messages in the newsletter. As a clue, I suggest you look at previous newsletters to see if you can figure out where the messages are hidden.

GOOD LUCK with the challenges.

Kirk