Texas Department of Public Safety
Cyber Security

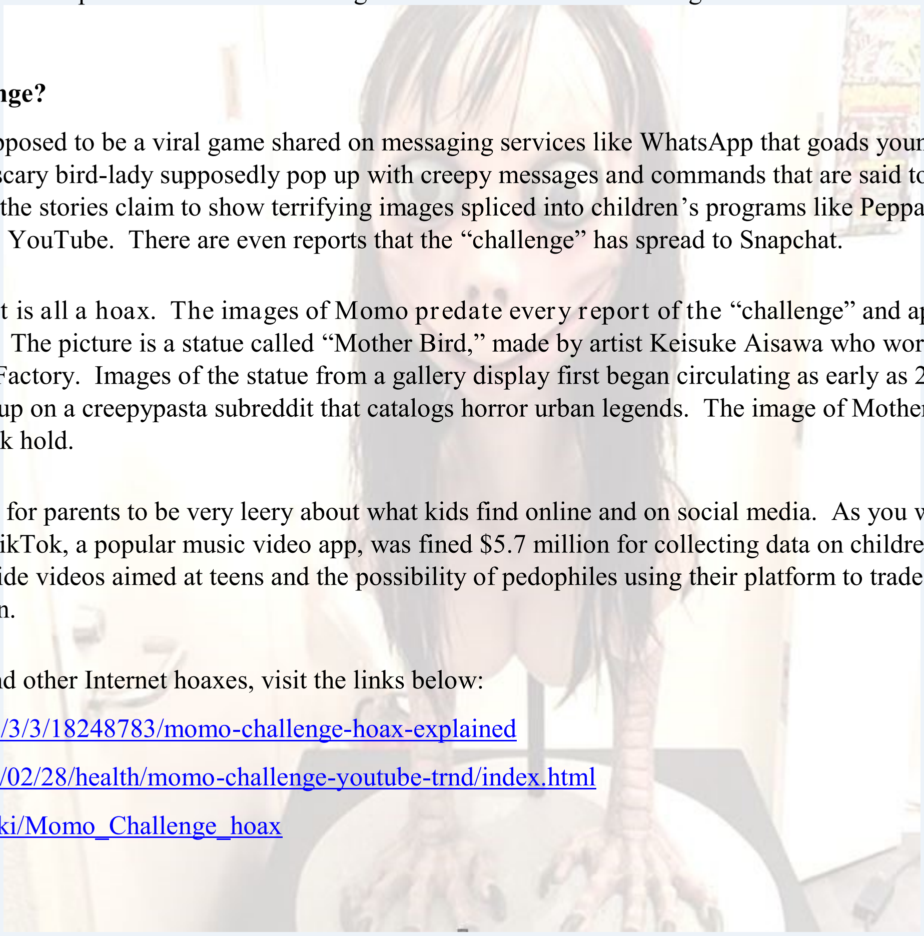
NEWS Cyber Security

Vol. 4 | Issue 3
March 2019

Page 2 | Page 3 | Page 4 | Page 5 | Page 6 | Reader Articles | Challenge | Closing

Welcome to the TXDPS Cyber Newsletter.

To begin the newsletter I want to spend a few minutes talking about a new Internet "challenge" I heard about recently. It is called the **Momo Challenge**.



What is the Momo challenge?

The Momo challenge is supposed to be a viral game shared on messaging services like WhatsApp that goads young children into violence or even suicide. Images of a scary bird-lady supposedly pop up with creepy messages and commands that are said to escalate to extreme violence and horror. Some of the stories claim to show terrifying images spliced into children's programs like Peppa Pig or video games like Fortnite in videos posted to YouTube. There are even reports that the "challenge" has spread to Snapchat.

The GOOD News is that it is all a hoax. The images of Momo predate every report of the "challenge" and appears to have nothing to do with the viral sensation. The picture is a statue called "Mother Bird," made by artist Keisuke Aisawa who works with the Japanese special effects company Link Factory. Images of the statue from a gallery display first began circulating as early as 2016. The challenge appears to have been cooked up on a creepypasta subreddit that catalogs horror urban legends. The image of Mother Bird was uploaded in July 2018 and the myth took hold.

There are LOTS of reasons for parents to be very leery about what kids find online and on social media. As you will see in the More News section of the newsletter, TikTok, a popular music video app, was fined $5.7 million for collecting data on children under 13. And YouTube is always dealing with suicide videos aimed at teens and the possibility of pedophiles using their platform to trade information and draw attention to clips of children.

To learn more about this and other Internet hoaxes, visit the links below:

https://www.vox.com/2019/3/3/18248783/momo-challenge-hoax-explained

https://www.cnn.com/2019/02/28/health/momo-challenge-youtube-trnd/index.html

https://en.wikipedia.org/wiki/Momo_Challenge_hoax

https://hoax-slayer.com/

https://www.snopes.com/

Since we are still in Tax Season, I wanted to remind everyone about the tax scams I mentioned in last month's newsletter. If you haven't done so, I would encourage you to visit the websites below to make yourself familiar with the most current tax scams.

IRS website Tax Scams / Consumer Alerts

IRS website IRS Urges Public to Stay Alert for Scam Phone Calls

TurboTax website Beware of IRS Phone Scams

YouTube video published Jul 24, 2018 Two IRS scammers arrested in Arizona

Federal Trade Commission IRS Imposter Scams

Good luck and hopefully you will not have to give extra money to the IRS this year.

Ring / Visitor Check-In

Nest competitor Ring reportedly gave employees full access to customers' live camera feeds

(by **Abner Li | Jan 10, 2019 @ 11:05 am PT**)

Last year, Amazon made waves in the smart home space by acquiring Ring for over $1 billion. Known for home security doorbells, a new report today claims that the company has a lax stance towards privacy that allowed more employees than seemingly necessary to access customers' live camera feeds.

According to *The Intercept*, Ring's engineers and executives have "highly privileged access" to live camera feeds from customers' devices. This includes both doorbells facing the outside world, as well as cameras inside a person's home. A team tasked with annotating video to aid in object recognition captured "people kissing, firing guns, and stealing." [Update: According to Ring, annotation is only conducted on "publicly shared Ring videos."]

U.S. employees specifically had access to a video portal intended for technical support that reportedly allowed "unfiltered, round-the-clock live feeds from some customer cameras." What's surprising is how this support tool was apparently not restricted to only employees that dealt with customers.

Update: In a statement, Ring explicitly argues that "employees do not have access to livestreams from Ring products."

The Intercept notes that only a Ring customer's email address was required to access any live feed.

> Although the source said they never personally witnessed any egregious abuses, they told The Intercept "I can say for an absolute fact if I knew a reporter or competitor's email address, I could view all their cameras." The source also recounted instances of Ring engineers "teasing each other about who they brought home" after romantic dates.

According to the report's sources, employees had a blasé attitude to this potential privacy violation, but noted that they "never personally witnessed any egregious abuses."

Click **HERE** to read the article.

Flawed visitor check-in systems let anyone steal guest logs and sneak into buildings

(by **Zack Whittaker**)

Security researchers at IBM have found, reported and disclosed 19 vulnerabilities in five popular visitor management systems, which they say can be used to steal data about visitors—or even sneak into sensitive and off-limit areas of office buildings.

You've probably seen one of these visitor check-in systems—they're often found in lobbies or reception areas of office buildings to check staff and visitors onto the work floor. Visitors check in with their name and who they're meeting using the touch-screen display or tablet, and a name badge is either printed or issued.

But the IBM researchers say flaws in these systems provided "a false sense of security."

The researchers examined five of the most popular systems: Lobby Track Desktop, built by Jolly Technologies, had seven vulnerabilities; eVisitorPass, recently rebranded as Threshold Security, had five vulnerabilities; EasyLobby Solo, built by HID Global, had four vulnerabilities; Envoys flagship Passport system had two vulnerabilities; and The Receptionist, an iPad app, had one vulnerability.

According to IBM, the vulnerabilities could only be exploited by someone physically at check-in. The bugs ranged from allowing someone to download visitor logs, such as names, driver license and Social Security data and phone numbers; or, in some cases, the buggy software could be exploited to escape "kiosk" mode, allowing access to the underlying operating system, which the researchers say could be used to pivot to other applications on the network, if connected.

Click **HERE** to read the article.

Cyber Command / 20-yr-old

U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms

(by **Ellen Nakashima | February 27, 2019**)

The U.S. military blocked Internet access to an infamous Russian entity seeking to sow discord among Americans during the 2018 midterms, several U.S. officials said, a warning that the Kremlin's operations against the United States are not cost-free.

The strike on the Internet Research Agency in St. Petersburg, a company underwritten by an oligarch close to President Vladimir Putin, was part of the first offensive cyber-campaign against Russia designed to thwart attempts to interfere with a U.S. election, the officials said.

"They basically took the IRA offline," according to one individual familiar with the matter who, like others, spoke on the condition of anonymity to discuss classified information. "They shut them down."

The operations marked the first muscle-flexing by U.S. Cyber Command, with intelligence from the National Security Agency, under new authorities it was granted by President Trump and Congress last year to bolster offensive capabilities. The president approved of the general operation to prevent Russian interference in the midterms, officials said.

Whether the impact of the St. Petersburg action will be long-lasting remains to be seen. Russia's tactics are evolving, and some analysts were skeptical that the strike would deter the Russian troll factory or Putin, who, according to U.S. intelligence officials, ordered an "influence" campaign in 2016 to undermine faith in U.S. democracy. U.S. officials have also assessed that the Internet Research Agency works on behalf of the Kremlin.

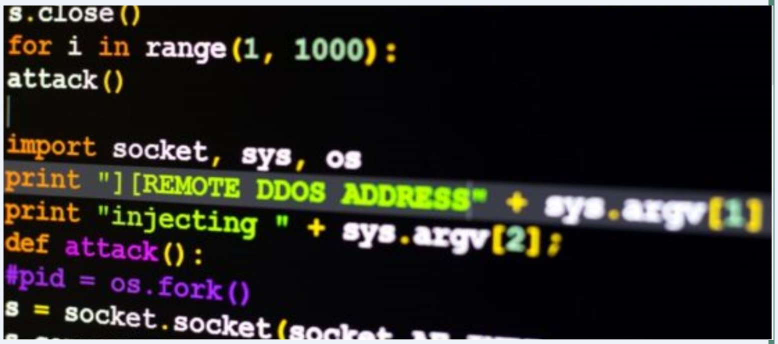
Click **HERE** to read more.

20-year-old pleads guilty to DDoS-for-hire scheme that netted $550,000

(by **Jeff Stone | Feb 27, 2019**)

A 20-year-old Illinois man pleaded guilty to charges related to a scheme to launch millions of distributed denial-of-service attacks against U.S. school districts and other targets, the U.S. Department of Justice announced Wednesday.

Sergiy Usatyuk and a co-conspirator gained more than $550,000 by charging subscribers for access to booter and stresser services, which typically enable attackers, using only a web browser, to launch a DDoS attack capable of knocking target sites offline. Usatyuk was involved with booter and stresser services including ExoStresser, QuezStresser, BetaBooter Databooter, Instabooter, Polystress and Zstress.



```
s.close()
for i in range(1, 1000):
attack()

import socket, sys, os
print "][REMOTE DDOS ADDRESS" + sys.argv[1]
print "injecting " + sys.argv[2];
def attack():
#pid = os.fork()
s = socket.socket(socket
```

The Exostresser services alone facilitated 1,367,610 DDoS attacks which caused victims to suffer 109,186 hours of downtime, the DOJ said Wednesday.

In one case in 2017, a Betabooter user launched a number of DDoS attackers against a Pittsburgh, Pennsylvania, school district that also affected 17 other organizations, including the county government, prosecutors said.

Usatyuk was active from around August 2015 to November 2017.

"DDoS-for-hire services pose a malicious threat to the citizens of our district, as well as districts across the country, by impeding critical access to the internet and jeopardizing safety and security in the process," said U.S. Attorney Robert Higdon Jr. in the Justice Department's announcement. "The operation and use of these services to disrupt the operations of our businesses and other institutions cannot be tolerated."

Click **HERE** to read .

Phone-hacking / IBM X-Force

Phone-hacking device used by police sells on eBay for $100

(by **Kris Holt | 02.28.19 in Security)**

A phone-hacking device that law enforcement officials use to extract data from phones is popping up on eBay for as little as $100. Federal agencies in the US and elsewhere, including the FBI and Department of Homeland Security, typically spend up to $15,000 on current models of Cellebrite's Universal Forensic Extraction Device, though older versions are available on the secondary market.

It seems police forces have sold or otherwise disposed of some devices, which later made their way to the online auction house, according to Forbes. Worryingly, cybersecurity researcher Matthew Hickey bought several UFEDs from eBay and found details on what phones law enforcement officials searched (including specific device identifiers like IMEI numbers), when the devices were accessed and what kinds of data were obtained. While he did not delve further, he suspected he'd be able to obtain personal data including photos, contacts and messages.

Click **HERE** to read more.

IBM X-Force Report: Ransomware Doesn't Pay in 2018 as Cybercriminals Turn to Cryptojacking for Profit

(**February 26, 2019**)

Security today announced results from the annual 2019 IBM X-Force Threat Intelligence Index, which found that increased security measures and awareness are driving cybercriminals to alter their techniques in search of a better return on investment (ROI). As a result, the report details two major shifts, including decreased reliance on malware and a decline in ransomware, as criminals increased their use of other cybercrime techniques with the potential for greater ROI.

IBM X-Force also observed that the number of cryptojacking attacks—the illegal use of an organization's or individual's computing power without their knowledge to mine cryptocurrencies—were nearly double those of ransomware attacks in 2018. With the price of cryptocurrencies like Bitcoin hitting a high of nearly $20,000 going into 2018, lower-risk/lower-effort attacks secretly using a victim's computing power were on the rise. In fact, IBM spam researchers only tracked one ransomware campaign in 2018 from one of the world's largest malware spam distribution botnet, Necurs.

The IBM X-Force Threat Intelligence Index also found that cybercriminals were changing their stealth techniques to gain illegal profits. IBM X-Force saw an increase in the abuse of administrative tools, instead of the use of malware. More than half of cyberattacks (57 percent) leveraged common administration applications like PowerShell and PsExec to evade detection, while targeted phishing attacks accounted for nearly one third (29 percent) of attacks.

"If we look at the drop in the use of malware, the shift away from ransomware, and the rise of targeted campaigns, all these trends tell us that return-on-investment is a real motivating factor for cybercriminals. We see that efforts to disrupt adversaries and make systems harder to infiltrate are working. While 11.7 billion records were leaked or stolen over the last three years, leveraging stolen Personally Identifiable Information (PII) for profit requires more knowledge and resources, motivating attackers to explore new illicit profit models to increase their return on investment," said Wendi Whitmore, Global Lead, IBM X-Force Incident Response and Intelligence Services (IRIS). "One of the hottest commodities is computing power tied to the emergence of cryptocurrencies. This has led to corporate networks and consumer devices being secretly highjacked to mine for these digital currencies."

Click **HERE** to read more.

Chrome / 4G and 5G

Google Chrome Zero-Day Lets Hackers Harvest User Data

(by **Bogdan Popa | Feb 28, 2019**)

A zero-day vulnerability in Google Chrome allows hackers to harvest personal data using nothing else than malicious PDF documents loaded in the browser.

Discovered by EdgeSpot, the security flaw is already being exploited in the wild and an official fix would only be released by Google in late April.

The PDF documents do not appear to leak any personal information when opened in dedicated PDF readers like Adobe Reader. However, it seems the malicious code specifically targets a vulnerability in Google Chrome, as opening them in the browser triggers outbound traffic to one of two different domains called burpcolaborator.net and readnotify.com.

The exposed data includes the IP address of the device, the operating system and Google Chrome versions, as well as the path of the PDF file on the local drives.

Interestingly, the malicious PDF documents aren't detected as potentially dangerous by security products, and only some antivirus solutions trigger a warning when scanning them.

Click **HERE** to read more.

Security flaws in 4G and 5G allow snooping on phone users

(by **Jon Fingas | 02.25.19 in Security**)

Security researchers are already poking holes in 5G mere months into its existence. They've discovered three flaws in 4G and 5G that could be used to intercept phone calls and track someone's location. The first and most important, Torpedo, relies on a flaw in the paging protocol that notifies phones of incoming calls and texts. If you start and cancel several calls in a short period, you can send a paging message without alerting the device to a call. That not only lets you track the device's location, but opens the door to two other attacks.

One of these, Piercer, lets you determine the unique IMSI number attached to a user on a 4G network. An IMSI-Cracking attack can guess the IMSI number through brute force on both 4G and 5G. This makes it possible to snoop on calls and location info through devices like Stingrays even if you have a brand new 5G handset. Torpedo can also insert or block messages like Amber alerts.

The vulnerabilities potentially affect most any 4G or 5G network in the world, although the degree varies widely. All four of the largest US carriers (AT&T, Sprint, T-Mobile and Engadget parent Verizon) are susceptible to Torpedo, while one unnamed network could also fall pretty to Piercer.

Click **HERE** to read more.

More News

FTC fines TikTok $5.7 million over child privacy violations

https://www.engadget.com/2019/02/27/ftc-fines-tiktok-over-child-privacy/

Congress to Google: How'd you 'forget' about the Nest Secure's mic?

https://www.engadget.com/2019/02/27/congress-questions-nest-secure-mic/

When 2FA means sweet FA privacy: Facebook admits it slurps mobe numbers for more than just profile security

https://www.theregister.co.uk/2019/03/04/facebook_phone_numbers/

Comcast set mobile pins to "0000," helping attackers steal phone numbers

https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/

How one teenager is making millions by hacking legally

https://www.bbc.com/news/av/technology-47407609/how-one-teenager-is-making-millions-by-hacking-legally

Many computers are vulnerable to hacking through common plug-in devices

https://www.helpnetsecurity.com/2019/02/26/hacking-through-common-plug-in-devices/

Hackers Turn to Microsoft's LinkedIn to Infect Users' Devices

https://news.softpedia.com/news/hackers-turn-to-microsoft-s-linkedin-to-infect-users-devices-525099.shtml

Most IoT devices are being compromised by exploiting rudimentary vulnerabilities

https://www.helpnetsecurity.com/2019/02/26/iot-devices-exploited-rudimentary-vulnerabilities/

Ready for another fright? Spectre flaws in today's computer chips can be exploited to hide, run stealthy malware

https://www.theregister.co.uk/2019/02/27/spectre_malware_invisible/

Social media-enabled cybercrime is generating $3.25 billion a year

https://www.helpnetsecurity.com/2019/02/27/social-media-enabled-cybercrime/

PDF viewers, online validation services vulnerable to digital signature spoofing attacks

https://www.helpnetsecurity.com/2019/02/26/digital-signature-spoofing-attacks/

User Suggested Articles

As you can see below, we had several user suggested articles. I encourage you to read all of them, but I want to highlight a couple of the articles I think most readers will benefit from reading.

For those with who have a loved one in college who is interested in cybersecurity I suggest you pay special attention to the fourth article provided by Deborah Wright. For those who use Microsoft Edge as their favorite web browser, I suggest you read the last article Deborah submitted.

Ean Meacham sent me an interesting article which talks about the possible future of passwords. And finally Stacey Phetteplace sent a very interesting article about an email forensics tool expected to be available this year.

Thank you everyone who submitted recommendations, please continue to send me articles you find. As for all the other readers, feel free to email me any articles you find of interest to be included in future newsletters.

Deborah Wright:

- https://fcw.com/articles/2019/02/06/jack-voltaic-lessons-learned.aspx
- https://www.dhs.gov/science-and-technology/ngfr#
- http://www.darkreading.com/attacks-breaches/devastating-cyberattack-on-email-provider-destroys-18-years-of-data/d/d-id/1333857
- https://www.cyber-fasttrack.org/
- Challenges https://go.cyber-fasttrack.org/
- https://gov.texas.gov/news/post/texas-to-partner-with-sans-institute-to-promote-cybersecurity-career-track-for-high-school-girls-and-all-college-students
- https://www.computerworld.com/article/3341394/microsoft-windows/microsoft-delays-windows-7s-update-signing-deadline-to-july.html
- https://threatpost.com/microsoft-updates-os-sha-1/142000/
- https://www.bleepingcomputer.com/news/security/microsoft-edge-secret-whitelist-allows-facebook-to-autorun-flash/

Ean Meacham

- https://www.techrepublic.com/article/infographic-the-death-of-passwords/
- https://www.loginradius.com/blog/wp-content/uploads/2018/12/The-Death-of-Passwords-V01.02.jpg

Stacey Phetteplace

- https://techbeat.justnet.org/beagle-will-sniff-out-email-fraud/

Cyber Challenge

Cyber Challenge

Last Month's Challenge

Here are the people who completed last month's challenges:

Fay Krueger @ 1028 on 11 February	James Taylor @ 1045 on 11 February	Deborah Wright @ 1332 on 11 February
Rene Hess @ 2325 on 11 February	Erich Neumann @ 1021 on 14 February	[redacted]

Here are last month's questions with answers:

1. 127 150 157 040 163 141 151 144 040 042 125 156 145 161 165 151 166 157 143 141 154 154 171 054 040 164 150 151 163 040 160 162 157 166 145 163 040 156 157 164 040 157 156 154 171 040 150 141 166 145 040 143 141 164 163 040 164 141 153 145 156 040 157 166 145 162 040 164 150 145 040 151 156 164 145 162 156 145 164 040 142 165 164 040 156 157 167 040 164 150 145 040 157 146 146 163 150 157 162 145 040 164 141 170 040 150 141 166 145 156 040 155 141 162 153 145 164 040 164 157 157 041 042 **The encoding you see is Octal. When you convert it (I suggest using a website to convert Octal to Text) you get "Who said 'Unequivocally, this proves not only have cats taken over the internet but now the offshore tax haven market too!'"** **The answer is Chris Kubecka**
2. ⎵↑⇕ ▽⇨↓⇦ ↟⇉⇕^ ▷↓◀↑⇕▶◀ ▽⇨⇨▶△↓◀◢ ⤴ ⇉⇔◀⇨△⇔⇨◀ ⇕← ^↑△⇨⇨◀▽↡⤵ **This is Wingdings 3. If you copy it to Microsoft Word you should get this: "Who said 'IoT without security = Internet of Threats'?"** **The answer is Stephane Nappo**
3. n fr fs fiafshji, rtizqfw gfspnsl ywtofs ymfy uwnrfwnqd kzshyntsx fx f itbsqtfijw tw iwtuujw tk tymjw gfspnsl ywtofsx. n fr frtsl ymj rtxy htxyqd fsi ijxywzhynaj rfqbfwj fkkjhynsl xyfyj, qthfq, ywngfq, fsi yjwwnytwnfq (xqyy) ltajwsrjsyx, fsi ymj uwnafyj fsi uzgqnh xjhytwx. bmfy fr n? **This is a Caesar cipher with an offset of 5. When you decode it you get "I am an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. I am among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors. What am I?"** **The answer is Emotet**
4. 4920616d20746865207479706520662072616e736f6d776172652074686174206869742041646616d73204d656d6f7269616c20486f73706974616c20696e2044656361746f722c20496e6469616e61206f6e203131204a616e7561727920323031382e20205768617420616d20493f **This is hexadecimal code. When you convert it (I suggest using a website to convert hexadecimal to text) you get "I am the type of ransomware that hit Adams Memorial Hospital in Decator, Indiana on 11 January 2018. What am I?" Depending on where you look you get either the "I'm Sorry" or "SamSam" ransomware. The initial message the hospital received that let them know they had an issue was a message that said "I'm Sorry". But there are later articles that call the ransomware SamSam.**
5. **This was a QR Code. When you decode it you get the message "I am a new breed of self-propagating fileless malware. What am I?" The answer is "vaporworm".**

For those of you who didn't attempt or were unable to complete last month's challenges, I encourage you to go try again and see if you get the above answers. If you need assistance, email me. You can find previous newsletters at this link: http://www.dps.texas.gov/InformationTechnology/Cyber/index.htm

This month's challenge is on the next page. Remember, if you have difficulties solving the challenges you can always email me for hints.

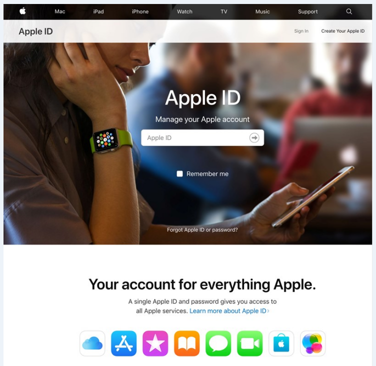
Cyber Challenge

Cyber Challenge

This Month's Challenge

This month's challenge will be a little different. It is a pick the phishing site challenge. Your challenge is to decide which of the two pictures listed per question is the Phishing Site. Email me your guesses and WHY the one you picked is the phishing site.

1)



Apple ID

Manage your Apple account

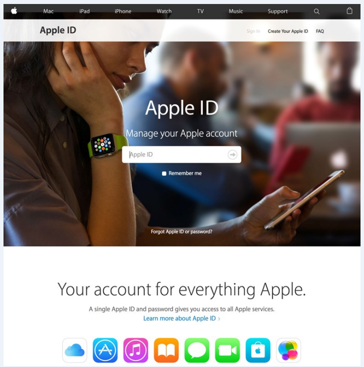
Apple ID

□ Remember me

Forgot Apple ID or password?

Your account for everything Apple.

A single Apple ID and password gives you access to all Apple services. Learn more about Apple ID ›



Apple ID

Manage your Apple account

Apple ID

■ Remember me

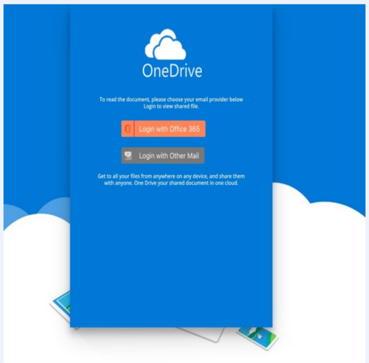
Forgot Apple ID or password?

Your account for everything Apple.

A single Apple ID and password gives you access to all Apple services.

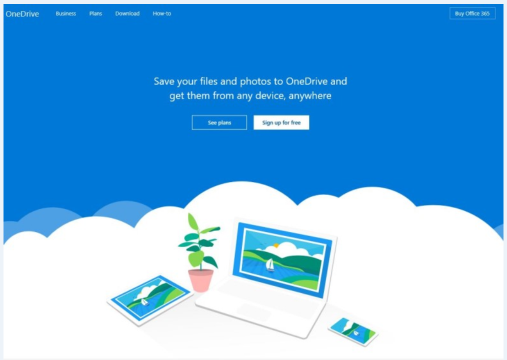
Learn more about Apple ID ›

2)



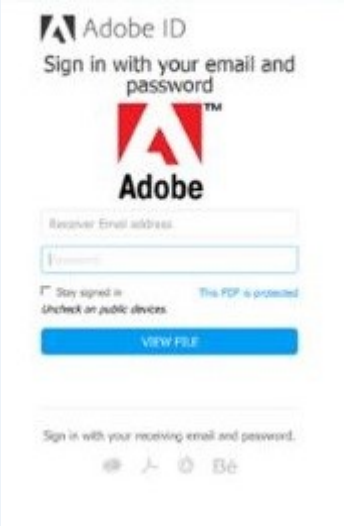
To read the document, please choose your email provider below Login to view shared file.

Get to all your files from anywhere on any device, and share them with anyone. One Drive your shared document in one cloud.



Save your files and photos to OneDrive and get them from any device, anywhere

3)



Sign in with your email and password

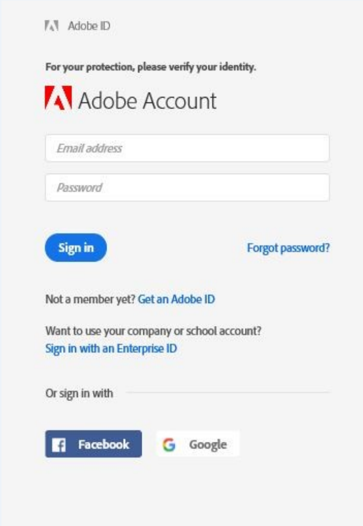
Receiver Email address

Password

□ Stay signed in   This PDF is protected

Uncheck on public devices.

Sign in with your receiving email and password.



For your protection, please verify your identity.

Email address

Password

Not a member yet? Get an Adobe ID

Want to use your company or school account?
Sign in with an Enterprise ID

Or sign in with

</Closing Comments>

Thank you for taking the time out of your day to read the newsletter. As always, I hope you found this month's newsletter informative, interesting, and useful. Remember, you can only defend against threats when you are knowledgeable about them. I realize cybersecurity is not the most liked topic, but it is important to understand the dangers you and your family face when online and how your actions and the actions of others can affect the Agency and your personal life.

I have covered a lot of topics this newsletter. I added the Momo Challenge information to this newsletter because of all the hype I have heard about it recently. Thankfully there are no confirmed cases of this being true, so it falls under the category of Internet Hoax. There are several hoaxes out there you should be aware of. The Momo Challenge is getting hype around the world because people are not well educated about Internet hoaxes and because of fear of what children are exposed to online. Educating yourself and your children about these hoaxes will help you identify legitimate threats online. If you decide to research more on this topic, please email me anything interesting you find and I'll include it in future newsletters.

Earlier today (5 March 2019) a friend of mine told me about a SPAM phone call she received. It was a call about student loan forgiveness. They had some information about her already and they were trying to pressure her into filling out the forms right then. The sense of urgency along with some information are classic tactics used to convince the victim the person on the phone is legitimate. They were going to email her the link to fill out the form but their high pressure tactic made my friend suspicious. She asked them to follow up with her via email or another call when she had more time. This all happened a few days ago and there has been no follow up. When a call like this is legitimate, the caller will almost always follow up. My friend used the perfect tactic when dealing with the caller. Delaying action and having time to evaluate the legitimacy of calls like this is the best way to handle them.

Knowing about cyber dangers are all part of Cybersecurity Awareness Continuation 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 a reminder, feel free to share this newsletter with friends and family. The better educated everyone is on cyber issues the safer everyone is. You can see previous issues of the website at this public facing DPS site:

http://www.dps.texas.gov/InformationTechnology/Cyber/index.htm

In closing, hope you enjoyed the newsletter and good luck with the Cyber Challenges. And as always, **THANK YOU FOR YOUR CYBER VIGILANCE.**

Kirk