NEWS
Cyber Security
Vol. 6 | Issue 5
May 2021

Page 2 | Page 3 | Page 4 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

Happy May everyone, we are almost half way through the year! Hopefully the rain lets up soon and we begin to see sun!

Now that tax season has come to an end, I'm hoping everyone securely filed their taxes and has a nice refund to pay off their Christmas presents!

In this edition of the newsletter Cyber Security wants to highlight the importance and awareness of potential phishing attacks.

In recent news, in February and March 2021 unidentified cyber actor(s) leveraged the upcoming REAL ID compliance deadline to conduct a multi-state phishing campaign, according to Department of Homeland Security reporting. The phishing messages led to "spoofed" websites that appeared to be the state's Department of Motor Vehicles (DMV) or Department of Transportation (DOT) offices, and were designed to harvest personal information.

Defining the REAL ID Act: This act was passed in 2005 and sets standards that state drivers' licenses and ID cards must meet in order to be accepted by the federal government for official purposes. The deadline for compliance was scheduled for October 21st of this year, but has since been postponed to May 3, 2023 due to the pandemic.

Regardless of the deadline change, fraudsters love to take advantage of upcoming deadlines in order to create a sense of urgency, claiming that a person must complete their forms to avoid legal action. Keep in mind that DMV and DOT offices will never contact you directly and ask you to provide personal information.

Here are common ways you might experience a phishing attack:

- Deceptive phishing: This type of phishing will be your most common attack, this is where fraudsters impersonate a legitimate company in an attempt to steal your personal data.

- Spear Phishing: In this ploy, fraudsters customize their attack emails with your name, position, or company in an attempt to trick you into believing that they have a connection with you.

- Vishing attacks: this is categorized as a phishing attack; however, this attack dispenses with sending out an email and instead goes for placing a phone call. An attacker can perpetrate a vishing campaign by setting up a (VoIP) server to mimic various entities in order to steal sensitive data and/ or funds.

****US-CERT partners with the Anti-Phishing Working Group (APWG) to collect phishing email messages and website locations to help people avoid becoming victims of phishing scams. You can report phishing to APWG by sending email to phishing-report@us-cert.gov. Learn more here: https://us-cert.cisa.gov/report-phishing**

Cyber Risk Management

Remote work has become more mainstream over the last year, so this month we are focusing on simple tips for secure remote access.

A good mindset to take is to remember that cyber threats exist everywhere. It can be easy to let your guard down when working from the comfort of your home or another remote location, but security risks are still present! The more people working remotely, the larger the attack surface is for cyber attackers. As with all security threats, it helps to know what you should defend against.

Here are some critical threats to keep an eye out for:

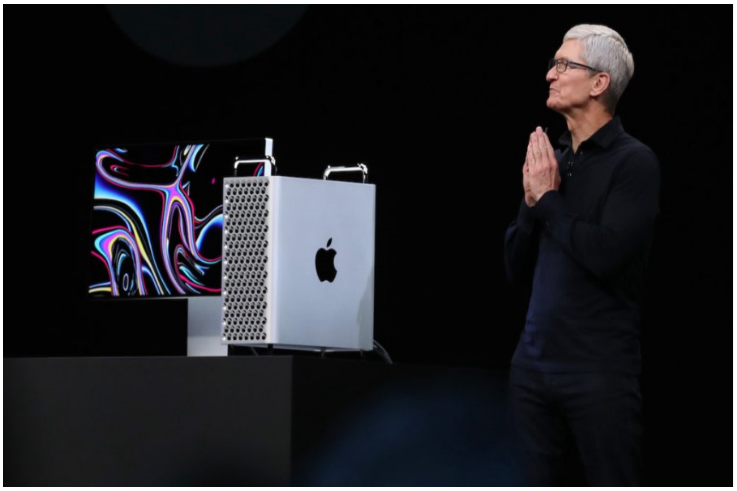
- Phishing Attacks—The easiest way for an attacker to get into a system is to trick an employee into sharing information.
- Easy Logins and Passwords– Many remote access endpoints only require a user ID and password, so maintaining a complex password that is difficult to guess will help mitigate this risk. If two-factor authentication is required, that is even better protection.
- Removable Media—Plugging in any unknown USB drives to your computer could potentially allow malware to infect your computer, and therefore the department's network, without any other steps.

Here are some tips to ensure secure remote work:

1) Only use DPS-issued workstations or mobile devices to connect to the DPS network. Personally-owned devices are not authorized on the network.
2) Never transfer sensitive DPS data onto a personally-owned device. Your personal devices don't have the same security configurations that our DPS devices have, which makes that data more vulnerable to be leaked.

3) Always use a secure VPN to connect to DPS network resources. This protects DPS data in transit from unauthorized disclosure and retains the same security protections as if you were plugged into the DPS network.
4) Check the Approved Software List or contact the Service Desk for approval before installing any software on your device.
5) Install system updates when you are notified that they are available. Software updates or patches can include new or enhanced features, improve software stability, add security measures, and remove outdated features.
6) As always, don't open or click on suspicious emails.
7) Store your device in a secure location and lock your device when not in use. Never leave your device unattended in a public place.
8) Report any suspected security incidents to Cyber Security immediately upon discovery.

Apple Patches/ Chase Phishing



Apple patched what noted Mac security researcher Patrick Wardle described to SC media as the “ worst macOS bug in recent memory.” An adware group had already been using the bug in the wild.

The newly discovered bug, patched in macOS 11.3, allowed hackers to circumvent much of Apple’s built-in malware detection for programs downloaded from the internet. MacOS knows to apply additional scrutiny to downloads by activating the “com.apple.quarantine” attribute.

The problem stemmed from how Macs install programs. Macs have the ability to wrap a normal installation bundle around a script instead of a traditional program. When a developer uses that technique, and when those bundles lacked a metadata file called “Info.plist” or a suitable alternative, macOS ignores the com.apple.quarantine attribute. In short, a user could double click on a sketchy program and install it without any of the roadblocks Apple designed to get in the way.

Full Story : Apple Patch Story

Chase Bank was impersonated in two recent phishing attacks designed to spoof real-life account scenarios in an attempt to fool victims.

In the first phishing scenario, threat actors sent an email titled “Your Credit Card Statement is Ready” with the sender name “JP Morgan Chase” with HTML stylings similar to the genuine emails sent from Chase, according to the report. The email included links for the victim to see their statement and make payments.

The second phishing attack begins with an email titled “URGENT : Unusual sign-in activity” and claimed that the sender was “Chase Bank Customer Care”.

The email included a link that claimed to be for customers to verify their account to restore access and used a common tactic by scammers to use different “from” and “reply-to” addresses.

The links take potential victims to a phishing page that resembles the Chase login portal and asks for their banking account credentials. Researchers surmised that the URL for the page was likely purchased and hosted using NameSilo, which provides hosting, email, and SSL solutions to customers.

“Services like this are beneficial for millions of people around the world, but unfortunately also lower the bar for cyber criminals looking to launch successful phishing attacks“ .

Full story : JP Morgan Chase Phishing Attack

In the News

Babuk Ransomware Gang Targets Washington D.C. Police

(Lisa Vaas | April 27th, 2021)

The Bubuk gang of threat actors claims to have stolen more than 250 gigabytes of data from Washington D.C. Metropolitan Police Department (MPD) on Monday, including police reports, internal memos, and arrested people's mug shots and personal details.

According to Vice, the attackers published the claim and the data on the official Babuk site. They also criticized the MPD's security, and taunted the law enforcement agency by saying that "We find 0 day before you" in its demand note and threatened to publish yet more data if their extortion demands aren't met.

The MPD hasn't acknowledged that files were locked, as happens with ransomware. If it turns out that files were in fact encrypted, that would make this yet another double-extortion attempt, where operators not only lock up files, but also steal data and threaten to leak it if the ransom isn't paid.

Babuk has a history of posting stolen files as a way of applying thumbscrews so victims will pay up: A tactic that's worked. According to McAfee, Babuk is a newcomer to this particular crimeware niche, having only been discovered in 2021. But the ransomware has already been lobbed at least five big enterprises, with one score: it walked away with $85,000 after one of those targets ponied up the money, McAfee researchers said. It's victims have included Serco, an outsourcing firm that confirmed that it had been slammed with a double extortion ransomware attack in late January.

"The Babuk gang highlighted the key problem that all organizations face when confronting threats, and that is speed. "In the note to the D.C police or MPD, they wrote 'we find 0 day before you'. This is unfortunately true, but it doesn't even have to be a zero day. The time it takes for known vulnerabilities to get patched on all systems is too long. Defenders that rely on manual security testing methodologies are unable to match the pace of threat actors in the finding security gaps and fixing them."

Full Story: Babuk Ransonware Gang

A Few More Cyber News Stories:

What Covid-19 Taught Us: Prepping Cyber security for the Next Crisis:

Full Story

Ransomware: A Deep Dive into 2021 Emerging Cyber-Risks:

Full Story

Anti-Vaxxer Hijacks QR Codes at Covid-19 Check-In-Sites:

Full Story

Cyber Challenge

Game Time!

This Month's Challenge

For this month's challenge, we get a chance to play as a Chief Information Officer of a business! In this game a video is presented to the user where they can choose a strategy, the way forward, and a defined budget.

The idea: This game is to transform the user into a CIO at Fugle Inc with the power to make decisions to protect confidential company information exposed to possible security problems.

The goal: We want to see how well employees at DPS can make good use of their budget by making the best decisions.

Good luck! (Click the link below to get started. Estimated total time to complete: 30 minutes)

http://targetedattacks.trendmicro.com/

Please let us know how you did, so we can include you in next month's newsletter!

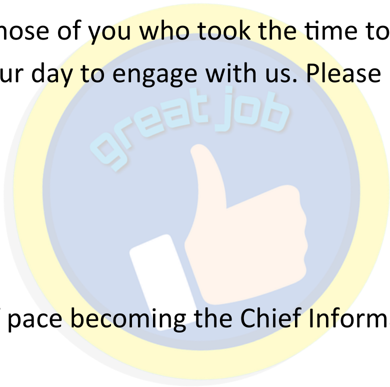
</Closing Comments>

As we close this month's newsletter, we'd like to give a quick shout out to those of you who took the time to engage with our cyber challenge. We fully appreciate you taking a few minutes out of your day to engage with us. Please keep doing so; and get others to join you.

Chris C. and Denise L., we appreciate your time and your cyber vigilance!

I hope you all enjoy this month's Cyber Challenge, it will be a nice change of pace becoming the Chief Information Officer and getting to budget how your Cyber team operates.

Please email our group at **GRP_Security_Awareness_Training** when you've completed the game!



In response to these cyber newsletters and our annual cyber training, I've been asked a few times for some cyber security news references to send family and friends that are free to use and easy to share. I'm really grateful for your interest in spreading the word. Thanks! Here are a few sources I trust and enjoy.

Cybrary This is personally my favorite site to use for general knowledge in Cyber security. It gives many courses to attend, and it will give you a certificate of competition at the end. Someday you will have a bulletin board of all your certificates! https://www.cybrary.it/

Threatpost This site stays very up to date with news happening all over the globe, it also provides different categories for specific cyber security incidents. https://threatpost.com/

The Hacker News is a great way to start getting your foot in the door with Cyber Security, they send articles almost daily to keep people current with the latest attacks hackers are doing. They are very entertaining reads! https://thehackernews.com/

Darkreading is another site our team likes to use, this site allows for readers/subscribers to interact and view conversations with other Cyber security professionals. It's a beneficial tool to help discover issues that are happening to others similar to issues you may be experiencing https://www.darkreading.com/

If you have any other sites you really enjoy, please share them with me, and I'll get the word out!

The Newsletter may seem a little different this month because surprise, it was not Eric this month. My name is Patrick in the Cyber Security Department, working next to Eric. While you may all miss Eric, I can assure you I miss him more! Eric is currently taking care of his new baby boy! I'm sure his hands are full right now, but our cyber team is incredibly happy for him as his family grows. Thank you all for reading and your cyber vigilance as always.

Share and Connect
Newsletter Archive