CYBER SECURITY NEWS
Vol. 6 | Issue 3
March 2021

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

Welcome to the TXDPS Cyber Security Newsletter!

Created by DinosoftLab from Noun Project

It's already tax season! And while the deadline to file isn't until next month, many of you may already be filing your taxes. Be careful! Cybercriminals absolutely love tax season.

The enormous amounts of valuable personal and financial information shared online during this time of year make it a haven for thieves – and they are doing everything they can to take full advantage of the opportunity tax season brings them. They are masters at social engineering. So, during this time of increased potential for having your personal information exposed, it's critically important to stay safe online.

Here are four ways cybercriminals try to take advantage of taxpayers during tax season:

- **IRS impersonation scams**: Callers claiming to be IRS employees might call and insist that you owe money, and that it must be paid as soon as possible via gift card or wire service. If the call isn't picked up, they leave an emergency callback message. The IRS will never call you to demand immediate payment. They will mail you a bill if you owe money.

- **Marked increase in phishing, email, malware and phone schemes**: Watch for unsolicited emails, texts, social media posts, fake websites or phone calls that might prompt you to click a link or share personal and financial information. Cybercriminals can use such information to steal your money and/or your identity. Unfamiliar links or attachments can also contain viruses, spyware or other malware that get installed on your computer or mobile device without your knowledge.

- **Fraudulent tax returns**: File your tax return as soon as possible. The IRS only accepts one tax return per Social Security number. If you file early, it becomes impossible for a fraudster to submit another return with your personal information.

- **Tax preparer fraud**: The overwhelming majority of tax preparers provide honest services, but some individuals might target unsuspecting taxpayers, and the result can be refund fraud and/or identity theft. The IRS reminds anyone filing a tax return that their preparer must sign it with their IRS preparer identification number.

Please keep the advice previously shared to protect yourselves from scams top of mind (use strong passwords, keep your devices updated, think before you click, etc.). Also, please note the IRS is now offering an Identity Protection PIN (IP PIN). An Identity Protection PIN (IP PIN) is a six-digit number that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps them verify your identity when you file your electronic or paper tax return.

The IRS has been using this PIN automatically when you are a confirmed victim of identity theft, but starting this year, anybody can voluntarily opt into the IP PIN program as a proactive way to protect yourself from tax-related identity theft.

For more information on this tool from the IRS, please visit: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

Cyber Risk Management

As a reminder, this section of the newsletter is used to inform you all about cyber risk controls meant to be preventative and proactive. In that spirit, we want to let you know we've created a section on our main SharePoint page of "Cyber How-Tos" to better equip you with useful guidance. And we need your help!

Please take some time to look over the "How-Tos". We'd love your feedback and want to hear ideas on what would be beneficial to you. We genuinely want this to be a place you can visit to feel confident in your ability to help us fortify DPS's cyber security posture, get your questions answered, and refresh your memory when cyber security procedures fade a bit (hey, it happens...so I hear...). We'll be continually adding to this section and working on improving it based on your feedback so please make sure to check back every so often!

Oh, and feel free to poke around the entire Cyber SharePoint page while you're there. You can read our Cyber team's vision and mission statements, bookmark the approved software list, check out the newsletter archives, access your cyber security awareness training, and more. We welcome your feedback on what you'd like to see on that page as well.

Please send your feedback to GRP_Cyber_Risk@dps.texas.gov.

We want to take this opportunity to give you a heads up about some exciting news for DPS staff! Well, we think it's exciting, anyway.

There is a change coming for VPN users in the way you authenticate to the DPS network that'll make it easier on you overall. "VPN authentication" sounds like nerdy "exciting news" but...it really should make the way you access it less cumbersome. And everybody likes an easier way to do things, right?

Currently, as a VPN user, you click on the AnyConnect icon and sign in with your username and password. Every 90 days, you have to install a new certificate. With the new VPN, you'll never have to install a new certificate again! Woo! Other changes include a different login screen and the use of multifactor authentication, using a PIN to get logged into VPN.

That's the high-level overview. IT will be sending out more information soon with instructions and screenshots and details. So please be on the lookout for that email.

Robo/Spam Calls

As we all know, robocalls and vishing (voice phishing over the phone) have become an increasing annoyance in our everyday lives. Whether the calls are on our home phones, cell phones, or office phones, we've all been bombarded with calls that were phishing for personal information, alerting you of financial issues, threatening arrests if you don't send money, or just plain trying to sell you something that you didn't ask for. Many times it's easy to figure out what's going on and to just hang up. But occasionally, it may not be that clear. Many people have been victimized by these scams.

To help you determine whether you are being scammed or not, here are some tips:

- Think before you speak. Scammers want you to act - and give out information - before you think things through. The person on the end of the line may sound sincere and trustworthy, but that doesn't mean they're legitimate.
- Have your guard up with automated calls. Be particularly skeptical of scare tactics, prizes, and special offers.
- Be aware that caller ID can be easily spoofed (impersonated) by scammers.
- Verify phone numbers before calling back. If you're given a toll-free number to call, look up the correct number yourself, either online or using the back of your credit card, for example.
- Use a different phone to call back. Attackers have ways to keep the line open even if you hang up and try to call your bank's correct number. You think you've reached the bank, but you're still connected to the scammer.
- Perform an Internet search for the phone number of the caller or the one that they give you over the phone. There are many websites that track whether individual phone numbers are suspicious.
- Note that organizations such as the IRS will never make first contact with you over the phone.
- If a bank is supposedly contacting you, hang up and call the number listed on your card or their website.

You may remember a notice we sent out a few weeks ago regarding these type of vishing attempts here at DPS.

To recap, here's the experience of a DPS employee so you know what to look out for:

"I started my day off with a panic because I got a call this morning from someone claiming to be from the Texas Medical Board working in conjunction with the FBI saying I was under some major investigation, and they believed my license and personal info was being used for drug trafficking purposes. I was told not to inform anyone about this, even those closest to me, or the investigation would be compromised, I would be arrested and charged, lose my job, etc etc. It was disconcerting to say the least.

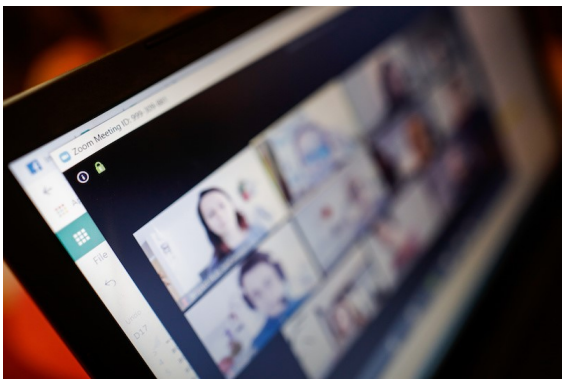
After insisting I be provided information to verify this claim, he provided a badge number, and I googled the number from which he called me; it went to the TMB. I got off the phone without providing info, saying I would call him back to ensure the number was legitimate."

The simplest advice for staying safe on the phone is "when in doubt, hang up." Stay alert out there.

In the News

Home-Office Photos: A Ripe Cyberattack Vector

(Elizabeth Montalbano | March 3, 2021)



Threat actors can use personal information gleaned from images to craft targeted scams, putting personal and corporate data at risk.

That photo that appears when someone disables his or her Zoom video, or those photos of a remote worker's home office shared on Instagram may seem innocuous and playful. However, they could become ammunition for threat actors to launch targeted scams and put personal and critical data at risk, a cybersecurity researcher has warned.

Jason Nurse, an associate professor in cybersecurity at the University of Kent, and a visiting academic at the University of Oxford, cautioned that personal photos and information shared via various online platforms used by remote workers can expose not only the employee, but also corporate networks, to threats from savvy attackers who are looking to exploit personal data. He shared his thoughts in a post published Wednesday on Sophos Naked Security blog.

With more workers online than ever due to the COVID-19 pandemic, people have gotten so comfortable with sharing photos and other personal information online that they may not be aware of how it can be misused, Nurse said.

Moreover, the pandemic in general has been stressful for everyone as people try to juggle their everyday lives amid the disruption to daily routine, which means that people have their guard down more than ever when cyber attackers come calling.

"While the sharing of such photos may seem harmless and even a must-do at the time, the reality is that we are, once again, falling into the age-old trap of oversharing," he wrote in the post. "We are forgetting to ask ourselves: What might a criminal or fraudster do with this information?"

The answer is quite a lot, Nurse surmised. That's because the more a threat actor knows about a person, the more he or she and the company they are working for are vulnerable to attack, he said.

Full Story: https://threatpost.com/home-office-photos-cyberattack-vector/164460/

A Few More Cyber News Stories:

CISA orders US agencies to address Microsoft flaws exploited by suspected Chinese hackers
https://www.cyberscoop.com/dhs-microsoft-exchange-flaws-patch-china/

Army warns of QR code scams amid pandemic
https://www.cyberscoop.com/qr-code-pandemic-security-hack-army-contact/

Hackers are finding ways to hide inside Apple's walled garden
https://www.technologyreview.com/2021/03/01/1020089/apple-walled-garden-hackers-protected

CYBER CHALLENGE

Game Time!

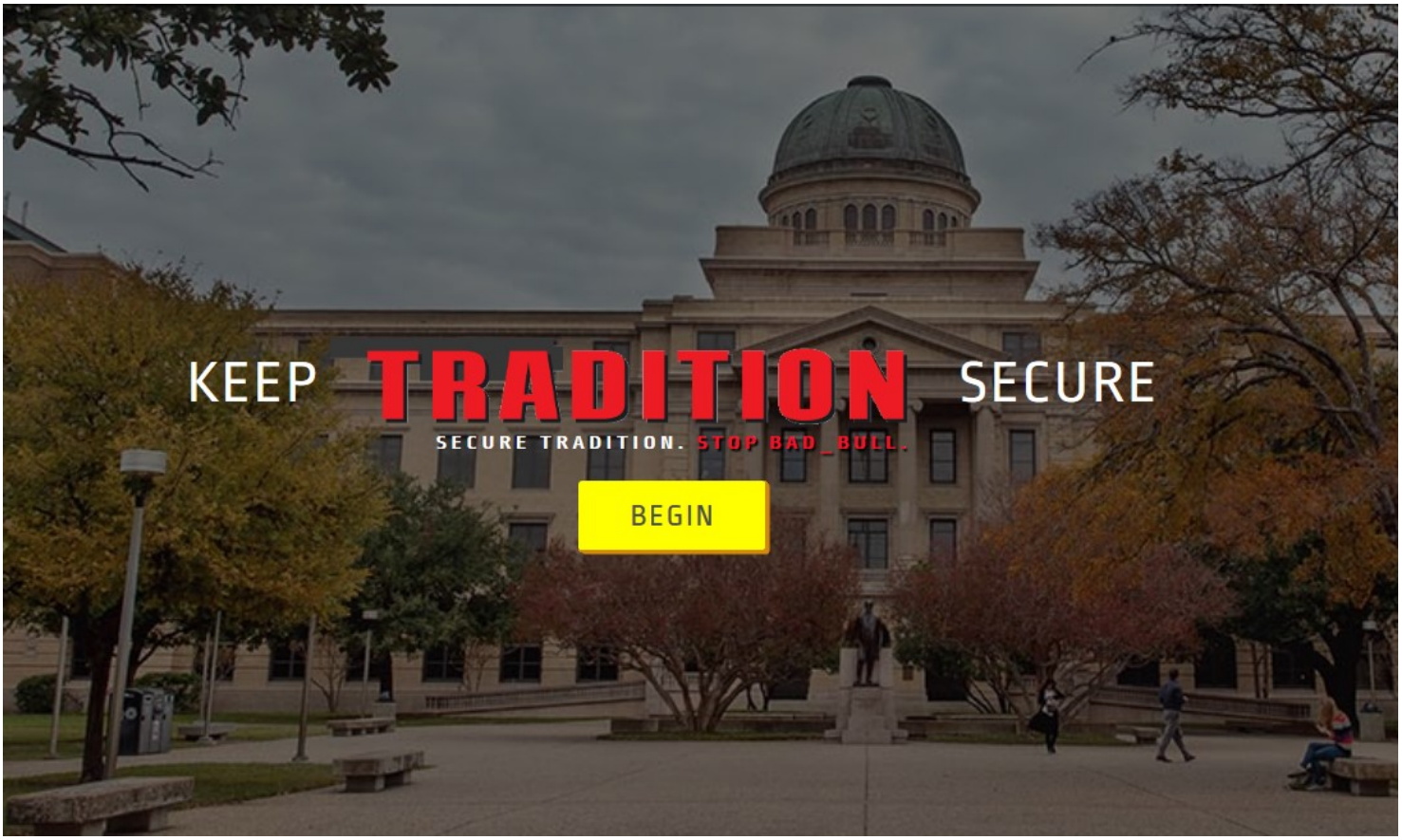
This Month's Challenge

For this month's challenge, let's play a game! This one was created by Texas A&M (hold the Aggie jokes, please) so it's obviously geared a little more toward campus life, but there's still some great stuff here.

The setup: A hacker named "Bad Bull" is threatening Texas A&M's campus traditions. Tracking down this hacker requires answering a series of cybersecurity questions and making your way around campus.

Let me know if you catch the hacker, and if you do, where on campus did you find him?

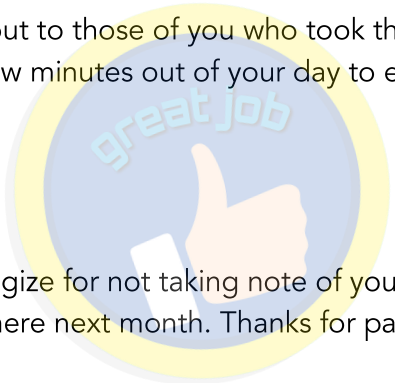
Good luck! (Click the image to get started. Estimated total time to complete: 20 minutes)



If you like this game, they've created many others over the years. Check them out at: https://it.tamu.edu/security/cybersecurity-games/index.php

</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.



We didn't receive any submissions of a completed crossword puzzle!

Though I did have a few chat with me and ask for some hints. I apologize for not taking note of your names. My bad! Remind me who you were, and I'll be sure to drop your name here next month. Thanks for participating!

In response to these cyber newsletters and our annual cyber training, I've been asked several times for some cyber awareness resources 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.

SANS publishes a monthly security awareness newsletter that's easy to download and send to whomever you feel would benefit: https://www.sans.org/security-awareness-training/ouch-newsletter. They also post a "Tip of the Day" explaining a specific cyber awareness topic with steps to take to protect yourself and your family: https://www.sans.org/tip-of-the-day.

The U.S. Federal Trade Commision (FTC) has a wealth of information on privacy, identity, online security and scams: https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

KnowBe4 is a cyber security awareness company who has a great blog to follow (though they try to pitch their products in most articles; just ignore that portion): https://blog.knowbe4.com/

MediaPro is another awareness company with free resources on their site, including a series of light-hearted videos of real-world stories told by cyber security professionals and their parents called "Mom, Don't Click That": https://www.mediapro.com/mom-dont-click-that/

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

Shifting gears now; on a personal note - I have some exciting news, too. If all goes well, by this time in April, my little family will be welcoming a baby boy into the world! We'll have two rambunctious boys soon so please wish me luck. Just wanted to let you know in case you don't hear from me for a bit. Bring on the sleepless nights and baby snuggles!

Thank you for swinging by, and as always, thank you for your cyber vigilance!

- Eric Posadas