NEWS CYBER SECURITY

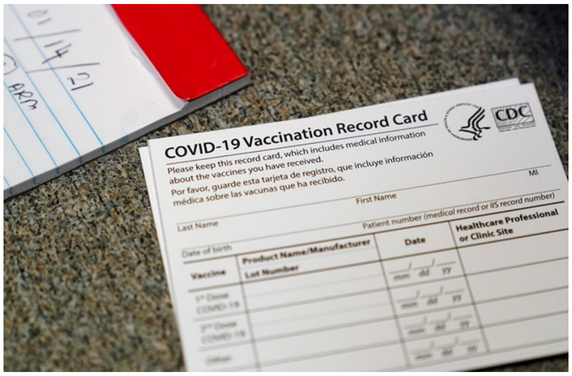
Vol. 6 | Issue 4

April 2021

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

Welcome to the TXDPS Cyber Security Newsletter!

We hope this newsletter finds you healthy and well; ready and able to enjoy the springtime!



You may have already seen these tips in February's edition of DPS News, but now that Texas has opened up COVID-19 vaccines to all adults, we wanted to share this again.

As tempting as it is, please don't share your vaccine card on social media. It's a common way to celebrate and memorialize the occasion while feeling connected to others. But, the self-identifying information on it makes you vulnerable to identity theft.

Let's say you get your COVID-19 shot, and you are excited to share the news and encourage others to do the same. So you take a selfie holding your vaccination card and post it to Facebook, Instagram, or another social media platform. Harmless, right?

Unfortunately, you just made yourself vulnerable to cyber crimes. Your card has your full name and birthday on it, as well as information about where you got your vaccine and who gave it to you. If your social media privacy settings aren't set to High, you are giving valuable information away for anyone to use. For example, scammers can use this information to open credit cards in your name with just a few more bits of information that may be already floating around on the dark web.

If you've already posted your card to social media, the BBB encourages you to take the picture down. They also suggest these tips for safely sharing vaccine news online:

- **Share your vaccine sticker or use a profile frame instead**. If you want to post about your vaccine, there are safer ways to do it. You can share a photo of your vaccine sticker or set a frame around your profile picture.

- **Review your security settings.** Check your security settings on all social media platforms to see what you are sharing and with whom. If you only want friends and family to see your posts, be sure that's how your privacy settings are configured.

- **Be wary of answering popular social media prompts**. Sharing your vaccine photo is just the latest social trend. Think twice before participating in other viral personal posts, such as listing all the cars you've owned (including makes/model years), favorite songs, and top 10 TV shows. Some of these "favorite things" are commonly used passwords or security questions.

Cyber Risk Management

For this month's highlight of cyber risk controls, we are taking a look at a crowd favorite - documentation!

A big part of risk management includes documentation such as policies and procedures. Policies set the expectation, and then procedures are developed to ensure compliance with those expectations.

Adhering to policy is critical, not only for governance and compliance purposes, but for the following as well:

- Mitigating risks and lowering our agency's exposure to risk
- Protecting our agency from malicious external and internal users
- Contributing and aligning to our agency's goals
- Providing a roadmap to our staff of what to do and when to do it

Did you know Cyber has its own chapter in DPS's General Manual? It's Chapter 25, and it is riveting! In all seriousness, please take a few minutes to read it over and familiarize yourself with our Cyber policies. Doing so will help you understand why we ask the things we ask of you and will set us all up for more success keeping cyber threats at bay. In fact, some of the topics we've mentioned previously in this section of the newsletter, such as data classification and media protection, are included in those policies.

Also note that we are working on new policies and updating current ones. Cyber Security policies are meant to be continually updated to adapt with evolving threats, exploits, technology, business and IT requirements and serve to ensure that all individuals within its scope understand their responsibility in reducing the risk of compromise and take appropriate security measures to safeguard DPS resources.

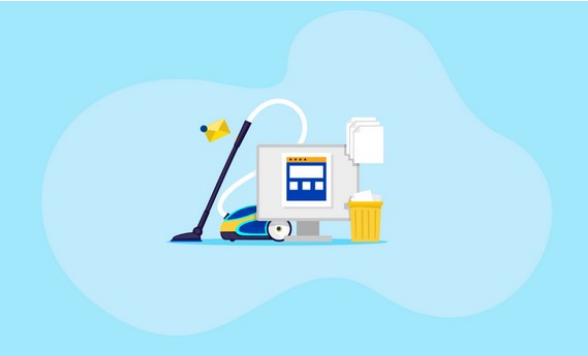
To accompany the policies, we are also working on a Standards Library. These standards will be more detailed documents that will help us all understand and adhere to the policies and will also assist with procedure development. They will be published on our SharePoint site and announced in a future publication of this newsletter when they become available.

It may be helpful to know that each division here at DPS has a representative who provides feedback on our Cyber policies. This group is known as the Cyber-PAC (Policy Advisory Council) and is a non-voting review body tasked with integrating operational perspectives into Department security compliance documentation. Cyber isn't alone in a dark room concocting ways to directly hamper your job tasks, *cue evil laugh*; we actually seek to enhance security policy documentation by facilitating an inter-Divisional review program, aligning policies with business functions and requirements and ensuring policies are realistic and achievable.

More info on the Cyber-PAC, including the group's charter, can be found on our Cyber SharePoint page.

If you have any questions about our policies, please reach out to GRP_Cyber_Risk@dps.texas.gov.

Digital Spring Cleaning



Spring is not just a good time for cleaning your house or apartment, it's also a good time to clean up your technology and cyber footprint.

Throughout the year, especially around the holidays and during tax season, you extend your cyber footprint by paying bills, shopping, using social media, and many other digital activities whether for business or personal use. Digital spring cleaning removes clutter from your life while at the same time protecting you and your loved ones.

While spring cleaning, you often make a list to ensure you don't forget to clean the spots you don't normally think about, like behind the sofa or on top of the fridge. To help you spring clean your technology and cyber footprint, the Center for Internet Security created this checklist to help you through the process. And just like spring cleaning your house, you can assign these tasks to your family.

Passwords

- □ Review your passwords, updating them as needed, and ensuring they are strong.
- □ Establish a unique password for each account.
- □ Consider using a password manager if you haven't in the past.
- □ Remember to use Multi-Factor Authentication (MFA) on accounts wherever it is available, especially on accounts that have financial information such as online banking, credit card, and retirement accounts.

Email

- □ Review all your email accounts.
- □ Be sure that there is no personally identifiable information stored in your mailbox.
- □ Review and update your contacts. Delete contacts that are no longer necessary or current.
- □ Review and update email filters.
- □ Enable MFA whenever possible.

Stale Mobile Device Apps

- □ Review your mobile device apps and remove those you no longer use.

Social Media

- □ Review social media accounts and associated privacy settings.
- □ Review any photos or videos and delete those that you no longer need or want to make viewable.
- □ Search yourself online to see what comes up.
- □ Don't just delete a social media app that you're no longer using, delete your entire profile.
- □ Be sure you are familiar with the privacy settings in your social media accounts.

Backups

- □ Review your backup routines.
- □ Test your backups and validate they are being successfully completed.
- □ Make sure you can restore from a backup.

Update Devices

- □ Make sure all applications, operating systems, and devices (computers, phones, tablets, smart devices, TVs, etc.) are updated, and are set to update on a regular basis.

Disposal

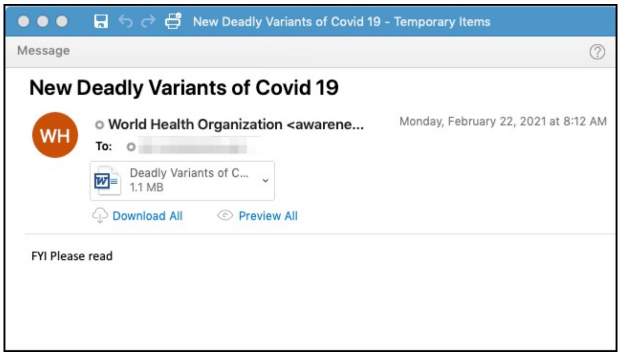
- □ Properly shred or destroy all unnecessary paper documents or files.
- □ Dispose of old electronic equipment (laptops, monitors, phones, tablet, smart devices, etc.)

Have fun getting rid of some clutter, and don't forget to clean under your beds!

In the News

Phishers' perfect targets: Employees getting back to the office

(Zeljka Zorz | March 22, 2021)



New Deadly Variants of Covid 19

WH World Health Organization <awarene... Monday, February 22, 2021 at 8:12 AM

To: [redacted]

Deadly Variants of C...
1.1 MB

FYI Please read

Phishers have been exploiting people's fear and curiosity regarding breakthroughs and general news related to the COVID-19 pandemic from the very start, and will continue to do it for as long it affects our private and working lives.

Cybercriminals continually exploit public interest in COVID-19 relief, vaccines, and variant news, spoofing the Centers for Disease Control (CDC), U.S. Internal Revenue Service (IRS), U.S. Department of Health and Human Services (HHS), World Health Organization (WHO), and other agencies and businesses.

Phishers targeting employees

According to Inky researchers, employees who have slowly been returning to work in offices and other company premises can expect cyber crooks to impersonate their colleagues and their company's leadership.

Judging by previously detected campaigns, the attackers will be hitting employees with emails made to look like they are coming from the HR or some other department, or from the CEO.

Lures will likely include:

- Surveys that employees must take regarding their willingness to receive the Covid-19 vaccine (or other related inquiry)
- New internal precautionary measures to "support health and safety"
- Information about changes in rules and new security roles within the company
- Requirements to review and complete new policy sections and guidelines

The emails will contain design elements related to the company (logos, etc.). Links will point to credential harvesting or malware-serving sites on a hijacked domain, and will look like they point to legitimate tools (e.g., Google, Basecamp, SharePoint, etc.). Phishers will try to create a sense of urgency, obligation, and even threaten employees with sanctions to get them to follow the links.

Full Story: https://www.helpnetsecurity.com/2021/03/22/phishers-employees

A Few More Cyber News Stories:

IRS Scam Emails Ask Tax Preparers for EFIN Information
https://securityintelligence.com/news/irs-scam-emails-ask-for-efin

Phishing Campaign Used Fake Office 365 Update Messages
https://www.govinfosecurity.com/phishing-campaign-used-fake-office-365-update-messages-a-16261

COVID-19 vaccine scammers are still lurking
https://www.cyberscoop.com/covid-19-vaccine-scammers-are-still-lurking/

CYBER CHALLENGE

Flex Your Knowledge!

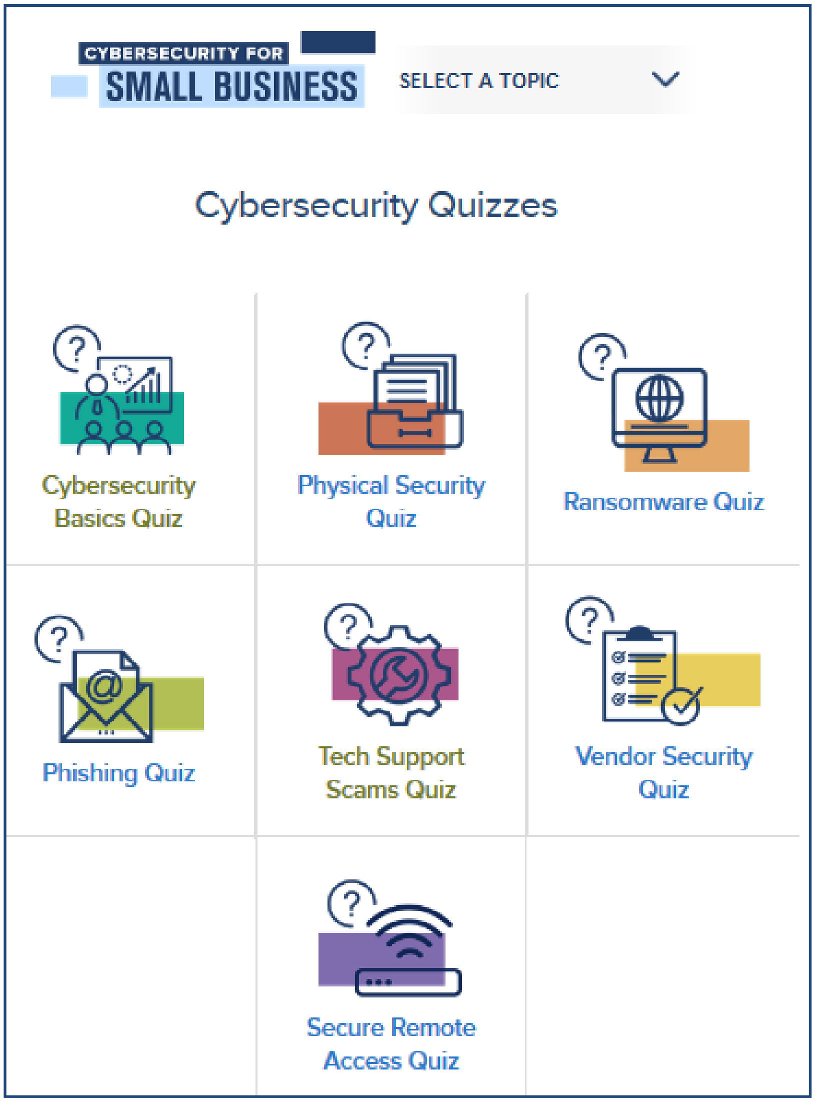
This Month's Challenge

For this month's challenge, step into the shoes of a small business owner, (hey, for all I know, you already are one!) and see if you have what it takes to fully protect your budding business from cyber threats.

The Federal Trade Commission has great cyber security awareness info. A section on their website is dedicated to short cyber security quizzes on a range of topics a business owner would face. Each quiz is only 5 questions long.

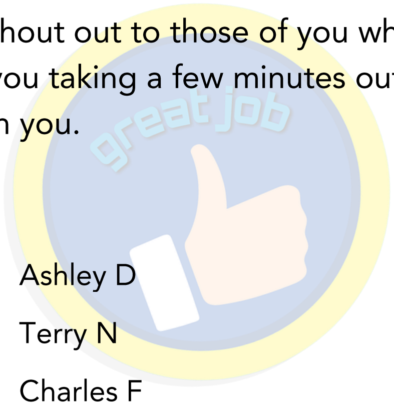
Wait! Don't let the "quiz" word lead to a hard pass. I'm truly curious if any of you can ace all of these. Do you got the cyber knowledge to knock these out and make a Cyber Training Officer proud??

Give them a try, and let me know how it goes. You don't have to ace them all, but I'm confident you can!



</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.



A big THANK YOU to:

Cynthia E
Antoinette R
Pamela F
Faye K
Wesley F
Michael M
Denise M L

Roxie J
Karen S
Jessica H
Amy L A
Danny N
Eddy H
Kymberly H

Ashley D
Terry N
Charles F
Lynni W
Trampas G

If we missed you, let us know!

As I mentioned in last month's newsletter, I'm about to welcome a new baby boy into the world if all goes according to plan. In fact, by the time this makes its way out to you all, I should be changing diapers while half asleep and making sure my toddler doesn't rough up his little brother too much.

If you have any cyber training questions or issues over the next several weeks, please contact GRP_Security_Awareness_Training@dps.texas.gov.

And our new cyber training platform is set up to automatically email you when your cyber training comes due so please be on the look out for that email if your year is almost up. (Yes, this cyber training is an annual requirement.) For help getting started, please check out our "How to Access Security Awareness Training" on our Cyber SharePoint page.

Happy Easter from my family to yours! Thank you for swinging by, and as always, thank you for your cyber vigilance!

- Eric Posadas