Vol. 8 | Issue 8

CYBER SECURITY NEWS

August 2023

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

Will this heat ever end? Asking for a friend. Hope this newsletter finds you well!

1 big thing: Cyber awareness training, what's the big deal anyway?

What to know: State and local governments are required by law to provide annual cyber awareness training to staff and contractors. We have to report our compliance percentage by August 31 each year; our goal is 100% completion and compliance.

But, why does it matter: Last year, around 75% of all breaches involved the human element, which includes social engineering attacks, errors or misuse. Those fancy cyber tools only help so much. (source: Verizon's DBIR Report)

Learning how to recognize these cyber attacks and scams will help protect our families from criminals looking to capitalize on our overall lack of cyber awareness. Cybercriminals also try to take advantage of our natural curiosity and willingness to be helpful. They'd would rather ask us (and trick us) for our information than hack a system to get it. Knowing this and preparing for this makes us less vulnerable to deception.

As our lives are now digital, being cyber aware also empowers us all to fulfill our mission of protecting and serving our fellow Texas residents. Cyber awareness training is a useful tool to do just that.

Social Engineering

Despite sounding like technology, "social engineering" involves personal interactions and pulling on emotional strings to garner sensitive information: "engineering" human feelings for personal gain.

There are several methods of social engineering that scammers use to deceive their victims, but here are a few of the most common.

Pretexting: Scammers often make up some sort of fictional story, or *pretext* for the situation which justifies their proceeding actions and requests. For example, a scammer may impersonate an authoritative *character* (like a boss or executive) and come up with a *situation* that threatens to adversely affect the victim (like an overdue car loan or tax evasion).

Vishing: In the age of texting and emails, it feels like real-time communication is a little harder and more fast-paced. Scammers know this, and thus like to engage victims via Voice Phishing, or *vishing*. They often use this method to create a state of panic that hinders rational thinking in the victim and doesn't give the victim time to think due to the fast-paced conversation on the phone.

False Urgency: As a cherry on top, scammers like to create a *false sense of urgency* when forming the pretext. For example, if you were told that your bank account was going to be closed in 24 hours unless you took action, what would you do?

Effective scammers can emotionally manipulate their victims while crafting a believable scenarios. Here are a few questions to ask yourself when dealing with suspicious activity:

- **"Did I expect this?"** Free tickets to a Kendrick Lamar concert or accusations of fraud don't just pop up out of the blue. Take to think it through before going along with the scammer's carefully crafted pretext.
- **"Is this the official number of the organization they claim to be?"** If you get a text message with a number to call, you should triple-check that the number mentioned is the organization's official number.
- **"Am I being rushed into a decision?"** It's very unrealistic for an organization to contact you and then pressure you to take immediate action . Don't let yourself go into a panic because of the fake brevity.
- **"Are they asking for payment or access to my personal info? What for?"** Why does Hulu require your Social Security number? Short answer – they don't. Be wary of giving out your credit card number, banking account credentials, or PII (Personally Identifiable Information) over the phone. Always ask why the organization needs it.

With a massive rise in vishing scams and fraud, it's important to stay vigilant and calm. If an unknown person is badgering you for information over the phone, you don't have to respond immediately. Take your time, and if you deem the situation too suspicious, you can always hang up without consequence and instead call the organization's official phone number for any clarifications.

Learn more about social engineering attacks here: https://www.ibm.com/topics/social-engineering

(by Intern Jai)

In the News

Google has an 'Enhanced Safe Browsing' feature. Should you use it?

(Intern Macy | July 27, 2023)

What is Google's "Enhanced Safe Browsing?"

Due to the constant stream of phishing, scamming, and internet crimes, Google has come out with an extra layer of protection for its users. According to Google, when Enhanced Safe Browsing is turned on for Chrome and Gmail, there will be extra steps to warn you when going on suspected scammer sites. To do this, they use their updated Google database of suspected scam sites and compare it to the ones you are visiting.

You'll know it's working when Google sends you a red warning screen when they think you are on a site that's impersonating your bank or other important web pages. They can even scan documents to see if you are downloading a file that may be a scam. If you don't have it turned on, Google still tries to check the security of your browsing, but if a crook creates a fresh scam site minutes after another one is blocked then they might miss it.

What are the negatives?

Google will know even more about the sites you are visiting and collect little visuals of them as well. The information is supposed to strictly be used for improving your security while browsing according to Google. The privacy tradeoff should be decided by the user.

How else can I boost my security?

Be sure to keep your browser up to date, don't reuse passwords, and turn on two-factor authentication!

Crooks can even find ways to replace official business phone numbers on Google maps and Google searches. When you dial their number, they may trick you into handing over credit card and personal information. The best way to combat this is by directly visiting the official business site for the real number instead of just clicking on the number listed on maps/search.

Read full story (source): https://www.washingtonpost.com/technology/2023/07/21/google-enhanced-safety-browsing/

A Few More Cyber News Stories:

Texas' TikTok ban hit with First Amendment lawsuit
https://www.cnn.com/2023/07/13/business/tiktok-ban-texas-lawsuit/index.html

New SEC Rules Require U.S. Companies to Reveal Cyber Attacks Within 4 Days
https://thehackernews.com/2023/07/new-sec-rules-require-us-companies-to.html

Vulnerabilities exposed Peloton treadmills to malware and DoS attacks
https://www.hackread.com/peloton-treadmill-vulnerabilities-malware-dos-attack

CYBER CHALLENGE

Spot the Deepfake

This Month's Challenge

For this month's challenge, let's put your knowledge about deepfakes to the test!

This is a quick, 10-question quiz to see how well you can spot real media versus media generated by AI.

And this goes beyond pictures. Videos and voices are being faked, too.

Would you be able to tell if your son or daughter was really on the other end of the line asking for help? Or if that political candidate was truly caught on video? Is it real or is it digitally created?

Let me know how you do and send me a sentence or two about one thing you learn! Good luck!

https://www.spotdeepfakes.org/