NEWS
CYBER SECURITY
Vol. 8 | Issue 9
September 2023

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

It's almost fall, y'all! Football season is back and so is pumpkin-spiced everything! Where's my scarf?

1 big thing: Cybersecurity tips for students going back to school

What to know: As your students head back to classrooms, from elementary to college, now is a good time to check you are doing all you can to make sure they are safe online.

Make sure to do these five things (via Malwarebytes):

Use multi-factor authentication (MFA)
MFA is an additional layer of security, after you enter your username and password. This could be a code generated by an app, a push notification you need to accept, a physical key you plug into your computer, or similar. Use it wherever it is offered to you.

Use strong passwords
By "strong", we mean the best possible password string you can come up. If, for example, your school IT administrator sets a maximum password length of 10 and allows a mix of alphabets and numbers, then make your password 10 characters long with the maximum complexity you can. And while we're on the subject of passwords, remember to use a unique password for each of your online accounts.

Be wary of links and attachments
When it comes to phishing and malware campaigns, danger doesn't just lurk in emails. It's on social media, SMS, chat platforms, gaming platforms, and other online watering holes, too.

Share with caution
Limit what you share, be smart about what info you allow apps to access, and think twice about sharing private photos.

Lock down your files
Play your part by locking down the devices you bring to school, such as your smartphone and laptop. Make sure there's at least a password or code that stops anyone from casually picking up your device, and then opening it.

(More resources for teachers and students shared at the end of the newsletter.)

Phishing Lures

Let's take it back to the basics and talk about phishing, the most popular attack vector used by cybercriminals.

"Phishing" refers to the practice of sending fake communication pretending to come from a reputable source that aims to trick you into revealing sensitive information, such as your login credentials and financial information.

While phishing takes many forms, the end goal of the attackers is always the same - to compromise your accounts or your device in the hopes of stealing data that can be turned into money.

Phishing emails start with a lure to hook victims. Messages pose as trustworthy communications from a company or organization you know or trust. They may appear to be sent from a bank, credit card company, social media, or an e-commerce platform. The fraudulent emails often tell a story, a plausible one, to trick you into clicking on a link, sending personal info or opening a malicious attachment.

How to tell if you're falling victim to a phishing attack:

Check the Sender

- Do you recognize the sender's email address?
- Is the email unexpected or unsolicited?

Check the Content

- Is the greeting generic? ("Dear Customer")
- Is the person asking you to click on a link to avoid something bad or receive something of value?
- Does the message ask you to provide personal information or your username and password?

Check the Tone

- Does the message contain any threatening language?
- Does the message sound urgent, aiming to panic you into acting quickly?

Check the Hyperlinks

- Hover over the link; does it direct you to a different website?

Check the Attachment

- Has the sender included an attachment that you did not expect or that makes no sense in the overall context of the message?
- Is that attachment in the form of a .exe, .pdf, .docx or .xlsx file?

Source: https://www.bitdefender.com/blog/hotforsecurity/back-to-basics-on-cyber-awareness-month-how-to-tell-if-youre-falling-victim-to-a-scam-or-phishing-attack/

In the News

Dallas to pay vendors $8.6M for their ransomware recovery services

(Matt Kapko | August 14, 2023)

The initial cleanup from a May ransomware attack that took most of Dallas' services offline and disrupted operations for weeks bears a heavy financial cost for the city's taxpayers.

The Dallas City Council on Wednesday approved a payment of almost $8.6 million to pay vendors for services linked to the cyberattack. The city did not name all of the vendors but previously identified CrowdStrike as its incident response partner.

The bill covers invoices from "various vendors for emergency purchases of hardware, software, professional services, consultants and monitoring services," the city said in a statement.

The attack also raised significant personal data privacy concerns for city employees and their family members. The personal data of more than 26,000 individuals was compromised as part of the attack, including names, addresses, social security numbers and medical and health information, according to a data security breach report Dallas filed last week.

Dallas said it didn't confirm files containing sensitive information on individuals were compromised until June 14. The threat actor intruded the city's network and exfiltrated data between April 7 and May 4, Dallas said in an update earlier this month.

The city filed the data breach disclosure almost two months after it first learned PII was exposed.

Read full story: https://www.cybersecuritydive.com/news/dallas-8-million-ransomware-recovery

A Few More Cyber News Stories:

AI Steals Passwords by Listening to Keystrokes With Scary Accuracy
https://www.darkreading.com/attacks-breaches/ai-model-can-replicate-password-listening-to-keystrokes

Sneaky Amazon Google ad leads to Microsoft support scam
https://www.bleepingcomputer.com/news/security/sneaky-amazon-google-ad-leads-to-microsoft-support-scam

Researcher says they were behind iPhone pop-ups at Def Con
https://techcrunch.com/2023/08/14/researcher-says-they-were-behind-iphone-popups-at-def-con/

CYBER CHALLENGE

Don’t Get Hooked!

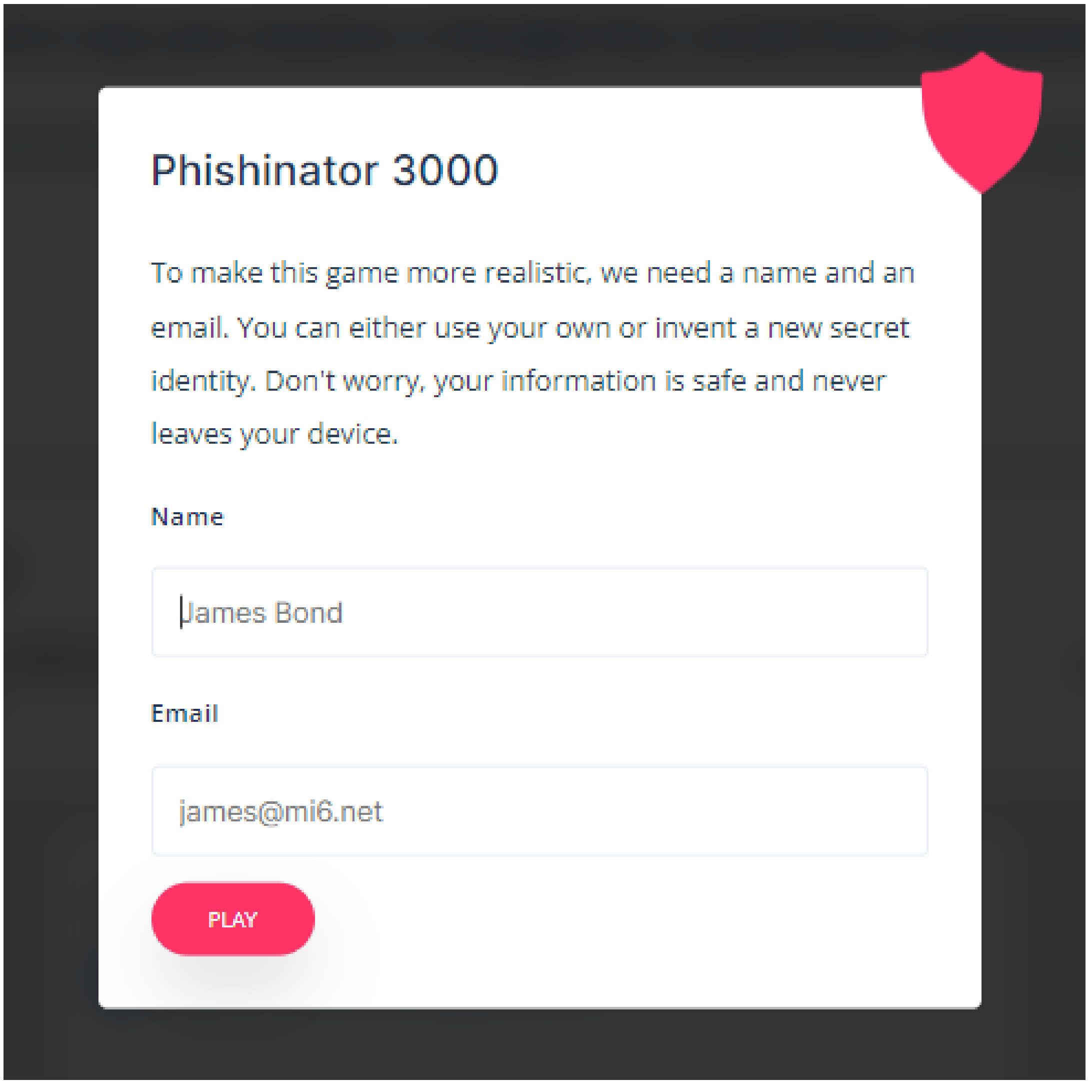
This Month’s Challenge

For this month’s challenge, let’s continue practicing spotting phishing emails. The more reps we can get at this, the more prepared we’ll be!

There are 6 emails to challenge you. Feel free to use a fake email address when prompted for one; it’s just used to mock up the emails presented to you to make them look more realistic.

As always, please let me know how you do. Good luck!

https://attacksimulator.com/cybersecurity-awareness/can-you-spot-phishing/



Phishinator 3000

To make this game more realistic, we need a name and an email. You can either use your own or invent a new secret identity. Don't worry, your information is safe and never leaves your device.

Name

James Bond

Email

james@mi6.net

Resources

Any teachers/students in your family?

CYBER.ORG's goal is to "empower educators as they prepare the next generation to succeed in the cyber workforce of tomorrow." Check out their website for free lessons and other ways they empower educators to teach cyber.

UTSA's Center for Infrastructure Assurance & Security (CIAS) has free cyber card games for educators and a cute CyBear mascot for young learners as well as other great freebies.

CyberStart America is for students in 9th-12th grade; their website provide free access to an immersive cybersecurity training game with over 200 challenges.

Hope these are helpful. Thanks for all you do, and stay safe out there!