NEWS
CYBER SECURITY

Vol. 10 | Issue 4

April 2025

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Tax Season Scams Are Here

What to know: Tax season is prime time for cybercriminals. Scammers impersonate the IRS, steal personal data, and trick taxpayers into handing over refunds.

The big picture: Phishing emails, fake tax preparers, and refund fraud are at an all-time high. Stay alert and protect your financial information.

How to stay safe at home:

- **Watch for phishing:** The IRS won't email, text, or DM you. Ignore urgent messages demanding payment or personal info.
- **Use strong passwords:** Secure tax accounts with unique, complex passwords and enable multi-factor authentication.
- **File early:** The sooner you file, the less time scammers have to steal your refund.
- **Verify tax preparers:** Check credentials and reviews before sharing sensitive information.
- **Use secure networks:** Avoid filing taxes over public Wi-Fi. Stick to trusted, encrypted connections.

Bottom line: Cybercriminals love tax season—don't make their job easier. Stay vigilant and protect your data.

Hybrid Work Environments

As agencies across the state continue to adopt and adapt to different work environments, it's important to remember that cybersecurity travels with us — whether we're at home, in a coffee shop, a work trip abroad, or back in the office. Good cybersecurity practices should follow us, no matter where we're working.

Cyber threats aren't unique to remote/hybrid work, but we all need to continue to focus on precautions to protect sensitive data as we move between home and the office.

Here are some simple ways to stay secure while working remotely:

- **Use a VPN when working outside the office** – A Virtual Private Network (VPN) encrypts your connection, keeping sensitive work data safe from prying eyes.
- **Enable Multi-Factor Authentication (MFA**) – Adding an extra layer of security beyond your password makes it much harder for unauthorized users to access your accounts.
- **Keep your devices and software updated** – Regular updates fix vulnerabilities and keep your system secure against the latest threats.
- **Be mindful of phishing attempts** – Cybercriminals may try to trick you into clicking malicious links or revealing credentials. If an email seems suspicious, don't click - report it.
- **Secure your home network** – Using a strong Wi-Fi password and enabling encryption helps prevent unauthorized access to your internet connection.
- **Lock your device when stepping away** - Whether at your desk in the office or working remotely, always secure your workstation when not in use.

By keeping cybersecurity habits consistent wherever you work, you help maintain a strong security posture across environments. Cybersecurity isn't just about the technology - it's about the small daily actions we all take to protect agency data.

More info: https://dir.texas.gov/news/cybersecurity-practices-remote-work
https://www.staysafeonline.org/articles/stay-secure-while-you-work-from-home

In the News

AI can steal your voice, and there's not much you can do about it

(Kevin Collier | March 10, 2025)

"Most leading artificial intelligence voice cloning programs have no meaningful barriers to stop people from nonconsensually impersonating others, a Consumer Reports investigation found.

Voice cloning AI technology has made remarkable strides in recent years, and many services can effectively mimic a person's cadence with only a few seconds of sample audio. A flashpoint moment came during the Democratic primaries last year, when robocalls of a fake Joe Biden spammed the phones of voters telling them not to vote. The political consultant who admitted to masterminding the scheme was fined $6 million, and the Federal Communications Commission has since banned AI-generated robocalls.

A new survey of the six leading publicly available AI voice cloning tools found that five have easily bypassable safeguards, making it simple to clone a person's voice without their consent. Deepfake audio detection software often struggles to tell the difference between real and synthetic voices.

Generative AI, which mimics human qualities such as their appearance, writing and voices, is a new and rapidly evolving technology, and the industry has few federal regulations. Most ethical and safety checks in the industry at large are self-imposed. Biden had included some safety demands in his executive order on AI, which he signed in 2023, though President Donald Trump revoked that order when he took office.

Voice cloning technology works by taking an audio sample of a person speaking and then extrapolating that person's voice into a synthetic audio file. Without safeguards in place, anyone who registers an account can simply upload audio of an individual speaking, such as from a TikTok or YouTube video, and have the service imitate them."

Full Story: https://www.nbcnews.com/tech/security/ai-voice-cloning-software-flimsy-guardrails-report-finds-rcna195131

A Few More Cyber News Stories:

New Arcane infostealer infects YouTube, Discord users via game cheats
https://www.bleepingcomputer.com/news/security/new-arcane-infostealer-infects-youtube-discord-users-via-game-cheats

Warning over free online file converters that actually install malware
https://www.malwarebytes.com/blog/news/2025/03/warning-over-free-online-file-converters-that-actually-install-malware

Phishing campaign impersonating Booking.com targets hospitality sector with malware
https://therecord.media/booking-phishing-hotels-malware-campaign

CYBER CHALLENGE

Spot the Red Flag

This Month's Challenge

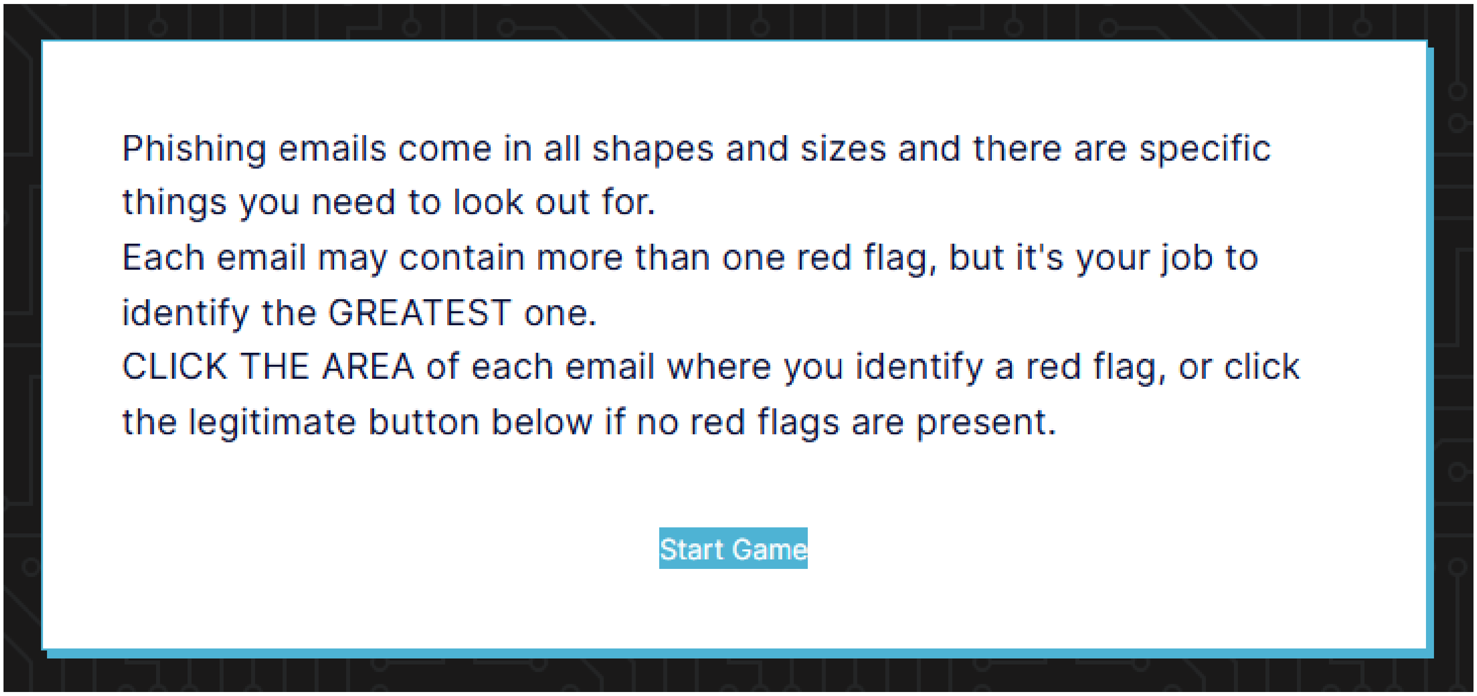
For this month's challenge, let's see how well you can identify red flags in phishing emails.

Each email may contain more than one of the telltale signs of a phishing email, but identify the *greatest* one in that particularly message.

Or, mark the email as "legitimate" if you don't spot anything suspicious.

Let me know how you do! And...bonus points for sending me a list of the red flags you identify and at least 4 additional red flags not used in this challenge. Good luck!

https://app.livingsecurity.com/player?contentid=2v8oU5IkcbHj8fMWUzHTMs



Phishing emails come in all shapes and sizes and there are specific things you need to look out for.
Each email may contain more than one red flag, but it's your job to identify the GREATEST one.
CLICK THE AREA of each email where you identify a red flag, or click the legitimate button below if no red flags are present.