Vol. 11 | Issue 2

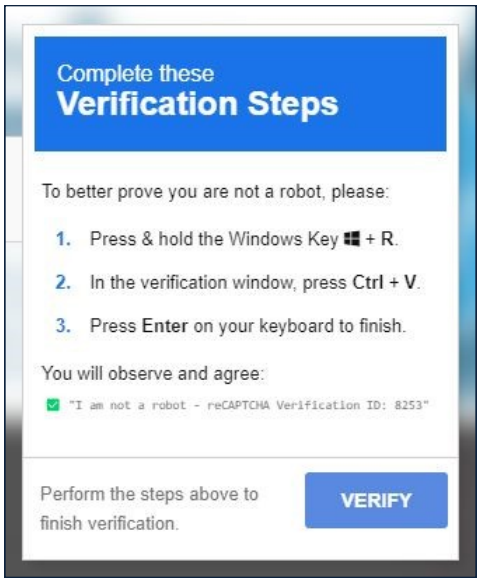
NEWS CYBER SECURITY

February 2026

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Fake CAPTCHA Pages Are Being Used to Spread Malware



What to know: There's been an increase in fake CAPTCHA attacks recently targeting users. These scams may look like normal "I'm not a robot" verification checks – but they're designed to trick you into running malicious commands on your computer.

How it works: Instead of a simple checkbox, the fake page may prompt you to follow the steps pictured above. That is not a real CAPTCHA process – it's malware delivery!

Why it matters: If followed, these steps can install malware that steals credentials, browser session data, and sensitive agency information.

To stay protected:

- Be cautious of CAPTCHAs that appear unexpectedly.
- Never paste or run commands a website provides.
- Close the tab if anything feels unusual.
- Report suspicious activity to your cybersecurity team right away.

Bottom line: CAPTCHAs may ask you to click images or solve a puzzle, but they should never ask you to run commands on your device. If it asks you to paste text into your computer, it's a trap.

Synthetic Media Threats

Synthetic media is any audio, video, image, or text that's created or altered using AI. Deepfakes are one example – but today, synthetic media also includes AI-generated voices, fake photos, fabricated screenshots, and realistic content designed to look or sound authentic.

With generative AI becoming widely available, this type of content is only going to become more common in everyday life.

Synthetic media can be used to:

- **Impersonate people** in scam calls or voice messages that sound real.
- **Spread misinformation** through convincing videos or images shared online.
- **Enable fraud** with fake "proof" like altered screenshots, documents, or recordings.
- **Manipulate emotions** by creating urgent, believable stories meant to trigger quick reactions.

The challenge is that these fakes don't have to be perfect – they just have to be believable long enough to get someone (you) to click, pay, share, or respond.

A few habits can go a long way:

- **Pause before reacting** to emotional or urgent content.
- **Verify through another channel** if someone is asking for money, info, or action.
- **Be cautious with unexpected audio/video**, even if it looks familiar.
- **Look for context** – where did it come from, and can it be confirmed elsewhere?
- **Trust your instincts** if something feels "off," even slightly.

Synthetic media is becoming part of the modern digital world. Staying safe doesn't require spotting *every* fake – just each of us slowing down and verifying before we act or share.

More on synthetic media: https://www.isaca.org/resources/isaca-journal/issues/2025/volume-1/the-rise-of-deepfakes-a-deep-dive-into-synthetic-media-and-its-implications

In the News

149M Logins from Roblox, TikTok, Netflix, Crypto Wallets Found Online

(Deeba Ahmed | January 23, 2026)

"A massive database containing over 149 million stolen usernames and passwords has been taken offline after sitting wide open on the internet for weeks. Cybersecurity researcher Jeremiah Fowler discovered the exposed cache, noting that the exposure 'highlights the global threat' of data theft because it allowed anyone with a web browser to view and search the records. This research was published by ExpressVPN and shared with Hackread.com.

A One-Stop Shop for Hackers

The database, totalling 96 GB, was not just a static pile of old leaks. While Fowler spent nearly a month trying to alert the hosting provider, he noticed the collection was actually growing in real-time. The sheer variety of the stolen data is what makes this discovery so troubling. The records included accounts for:

- **Social Media:** Facebook (17M logins), Instagram, TikTok, and X.
- **Streaming and Games:** 3.4M Netflix logins, plus HBOmax, Disney+, and Roblox.
- **Financials:** Banking portals, credit card accounts, and 420,000 Binance crypto logins.
- **Sensitive Sites:** Dating apps and OnlyFans accounts, affecting both creators and customers.

The database contained 48 million Gmail accounts, roughly 4 million Yahoo logins, 1.5 million for Microsoft Outlook, and 900,000 for Apple's iCloud. Even more concerning, it contained login details for government (.gov) domains from multiple countries. Fowler noted that even limited access to these accounts could allow hackers to impersonate officials or slip into secure government networks."

Full Story: https://hackread.com/logins-roblox-tiktok-netflix-crypto-wallets-found

A Few More Cyber News Stories:

Nike investigates data breach after extortion gang leaks files
https://www.bleepingcomputer.com/news/security/nike-investigates-data-breach-after-extortion-gang-leaks-files

New PayPal Scam Sends Verified Invoices With Fake Support Numbers
https://hackread.com/paypal-scam-verified-invoices-fake-support-numbers

Have I Been Pwned: SoundCloud data breach impacts 29.8 million accounts
https://www.bleepingcomputer.com/news/security/have-i-been-pwned-soundcloud-data-breach-impacts-298-million-accounts

CYBER CHALLENGE

Phishing Websites

This Month's Challenge

For this month's challenge, let's see how well you do spotting a malicious website.

Just like many other things, AI is making it easier to mimic legitimate websites. It's important you slow down while browsing the web and interacting with links in an email. Just because a website looks familiar doesn't mean it's safe.

Let me know how you do. I'll be honest...a few of these almost got me. The red flags aren't obvious nor are they pointed out. This is to show you just how tough spotting these can be.

Good luck!

https://www.liveaction.com/spot-the-phish