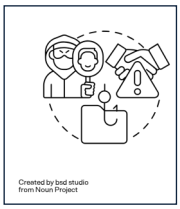
Vol. 10 | Issue 6

NEWS CYBER SECURITY

June 2025

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Hacking Doesn't Always Mean Breaking Into a System



What to know: When we think of hacking, we usually imagine someone breaking into a system. But **social engineering** is different - it's about tricking *you*, not the technology.

These scams rely on emotions and use trust, fear, and urgency to get people to do things they normally wouldn't. It's less about fancy tools and more about knowing how people tick. Here's a great example of utilizing a social engineering skillset from the movie Oceans 8: https://www.youtube.com/watch?v=OkBaZLq7gnU.

Yes, new tools like AI are giving these scammers an upgrade.

- Fake voices and videos (called deepfakes) can mimic real people.
- Chatbots can send messages that sound perfectly human.
- Public info from social media is scraped to help make scams feel personal.

But, remember, **social engineering doesn't always involve a computer**. Scammers might:

- Knock on your door claiming to be from a utility company.
- Text pretending to be your bank needing to confirm your account.
- Call to claim a loved one is in trouble and needs money.

It's all about building trust quickly—and taking advantage of that moment.

Here are a few ways to stay safe:

Take a Pause – Scammers use panic to push quick decisions. Slow down and think.

Double-Check – Never trust a call, email, or text at face value. Use a known contact method to confirm.

Limit Sharing – Be careful what you post online. It can be used against you.

Spot the Red Flags – Bad grammar, urgent requests, and weird links are all warning signs (Note: AI is making this harder to spot.)

Trust Your Gut – If something feels off, it probably is.

In the News

AI-Generated TikTok Videos Used to Distribute Infostealer Malware

(News | May 22, 2025)

"A new malware campaign has been observed using TikTok's viral nature and vast user base to spread information-stealing malware such as Vidar and StealC.

TikTok Videos Deliver Malware via PowerShell

According to a new advisory by Trend Micro, this latest social engineering effort marks a shift from traditional malicious tactics, exploiting the platform's reach and user trust to spread harmful software via seemingly innocuous video content.

Unlike previous campaigns that depended on malicious websites and JavaScript injections, this attack operates entirely within TikTok.

The campaign features short-form videos, likely created with AI tools, that instruct users to execute PowerShell commands. These commands, presented as methods to activate popular software like Microsoft Office or Spotify, initiate a malware infection chain.

What sets this tactic apart is its use of verbal and visual guidance in the videos. The commands are never embedded in text or links, making them harder for traditional security systems to detect. Viewers are coaxed into typing the commands themselves, making them unwitting participants in the malware installation.

Trend researchers traced the campaign to accounts including @gitallowed, @zane.houghton and @digitaldreams771.

These accounts, now inactive, published similar AI-voiced videos with minor variations in camera angles and payload URLs, suggesting automation was used in their creation."

Full Story: https://www.infosecurity-magazine.com/news/ai-tiktok-videos-infostealer

A Few More Cyber News Stories:

Hackers Targets Coinbase Users Targeted in Advanced Social Engineering Hack
https://gbhackers.com/hackers-targets-coinbase-users

Cybercriminals camouflaging threats as AI tool installers
https://blog.talosintelligence.com/fake-ai-tool-installers

Cybercriminals Are Turning Ordinary Citizens Into Money Mules in a New 'Rent-a-Bank-Account' Scam
https://gbhackers.com/cybercriminals-are-turning-ordinary-citizens

CYBER CHALLENGE

Spot the Deepfake

This Month's Challenge

For this month's challenge, let's practice spotting deepfake images of people's faces.

"As criminals become more adept at using AI to create convincing fake images and videos, it's more important than ever to know what's real and what's not. This distinction protects us from financial scams, reputational damage, and the spread of misinformation, while preserving our trust in online information and the integrity of our digital interactions. Some are easy to detect – others aren't. Take our quiz to test your skills at spotting deepfakes!"

There are a total of 10 images. Let me know how you do!

https://quiz.iproov.com/