Vol. 10 | Issue 3

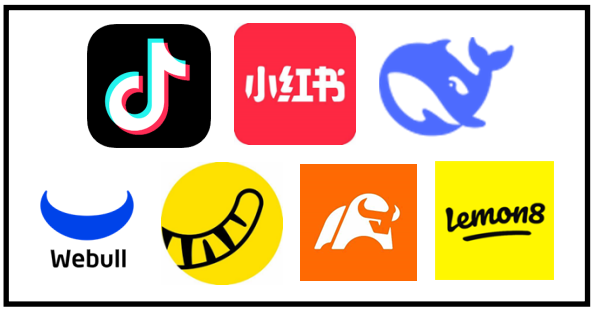
NEWS CYBER SECURITY

March 2025

| Page 2 | Page 3 | Challenge |

# Welcome to the TXDPS Cyber Security Newsletter

**One big thing: Yes, TikTok Is Still Prohibited On State Devices; Now Other Apps Are Too**




**What to know:** While TikTok has managed to avoid a full federal ban (for now), it remains prohibited on all state-issued devices in Texas, as well as personal devices used to conduct state business.

**Governor Greg Abbott recently released a proclamation** banning additional Chinese AI and social media applications that pose a security risk to the State of Texas.

**The latest addition to the state's prohibited technologies list:**

- **Rednote** - gained popularity during TikTok's federal ban; app is completely unsafe as it transmits submitted data over plain text and is a possible malware vector.
- **DeepSeek** - Chinese-owned AI and chatbot app; concerns include government influence, surveillance, and propaganda as well as data collection and privacy concerns.
- **Webull, Tiger Brokers, Moomoo** - financial trading apps; each collect significant sensitive personal and financial information which is freely shared with Chinese Communist Party.
- **Lemon8** - social media app owned by Bytedance; collects significant amount of personal and device-specific information which is made freely available to the Chinese Communist Party.

These bans aim to mitigate potential cybersecurity risks, such as data harvesting and foreign influence on state networks. If you use a state-issued device (or a personal device for state business), ensure these apps are not installed and avoid accessing them via web browsers.

The Prohibited Technologies list is routinely updated. You can find the most up-to-date listing on DIR's website: https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies

# Insider Threats

When we think about cyber threats, we often picture faceless hackers in dark rooms; maybe even in other countries. But what if the threat is coming from *inside the house*...or in this case, the office? That's what we call an "insider threat" - a risk that comes from employees, contractors, or anyone with inside access to an organization's systems and data.

Not all insider threats are malicious. Sometimes, it's just carelessness — like an employee clicking on a phishing email or using a weak password; or accidentally exposing sensitive data by mistyping an email address.

Other times, it *is* malicious — someone intentionally leaking data, stealing intellectual property, or compromising systems for personal gain. Either way, insider threats are a big deal.

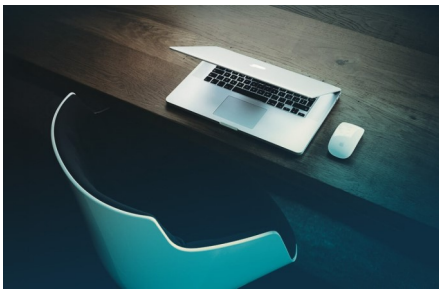
**Key ways to help with insider threats:**

- **Report suspicious activity:** If you notice unusual behavior, like unauthorized access attempts, unusual data transfers, or coworkers accessing sensitive information they shouldn't have, report it immediately. If you see something, say something.
- **Follow security policies:** Adhering to company policies, especially those regarding data handling, password management, and access controls is crucial to prevent accidental data leaks or security breaches.
- **Security awareness training:** Actively participate in regular cybersecurity training to stay updated on best practices and recognize potential threats. (I hear this Cyber Newsletter is great!)
- **Be mindful of phishing attempts:** Be cautious about clicking on suspicious links or opening attachments in emails, and report any potential phishing attempts.
- **Resist the urge to allow "piggybacking":** It's in our nature to be helpful and kind, but holding the door open for others to enter a secure area puts us all at risk. It might be awkward, but it's best to have everybody badge into a secured space.
- **Practice good password hygiene:** Use strong, unique passwords for all accounts, enable multi-factor authentication (MFA), and don't share login credentials. Ever.
- **Monitor personal devices:** Be aware of the risks associated with using personal devices for work and follow company guidelines for accessing company data on personal devices.

**Read more from CISA about insider threats:** https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

# In the News

## No, you're not fired – but beware of job termination scams



(Phil Muncaster | February 18, 2025)

"...employment and work-from-home scams are...popular among cybercriminals (and even some state-aligned threat actors). The schemes typically lure the user by offering amazing jobs or casual employment opportunities. But in reality, all the scammers usually want is your personal and financial information. In some cases, victims may even end up unwittingly receiving and re-shipping stolen goods, or allowing their bank accounts to be used for money laundering.

However, less-well known is the employment termination scam. This turns the idea on its head: using the threat of losing your job rather than the lure of gaining a new one to catch your attention. So what do they look like and how can you stay safe?

What do job termination scams look like?

At their simplest, job termination scams are a type of phishing attack designed to trick you into handing over your personal and financial information, or on clicking on a malicious link which could trigger a malware download. Social engineering tactics used in phishing aim to create a sense of urgency in the victim, so that they act without thinking things through first. And you can't get more urgent than a notice informing you that you have been dismissed.

It could arrive in the form of an email from HR, or an authoritative third-party outside the company. It may tell you that your services are no longer required. Or it may claim to include details about your colleagues that are too hard to resist reading. The end goal is to persuade you to click on a malicious link or open an attachment, perhaps by claiming that it includes details of severance payments and termination dates."

Full Story: https://www.welivesecurity.com/en/scams/no-youre-not-fired-beware-job-termination-scams

### A Few More Cyber News Stories:

US employee screening giant DISA says hackers accessed data of more than 3M people
https://techcrunch.com/2025/02/25/us-employee-screening-giant-disa-says-hackers-accessed-data-of-more-than-3m-people

New Phishing Attack Targets Amazon Prime Users to Steal Login Credentials
https://gbhackers.com/new-phishing-attack-targets-amazon-prime-users

Beware: PayPal "New Address" feature abused to send phishing emails
https://www.bleepingcomputer.com/news/security/beware-paypal-new-address-feature-abused-to-send-phishing-emails

CYBER CHALLENGE

# Cyber Whodunit?

## This Month's Challenge

For this month's challenge, let's see how strong your detective skills are.

In this cyber-twist of the game Whodunit, your organization has experienced a major data leak. Important secret information has somehow gotten into the hands of a competitor or adversary.

It's up to you to figure who did it, how, and where it happened.

There are seven mysteries. See how many you can solve.

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

https://securityawareness.usalearning.gov/cdse/multimedia/games/whodunit/index.htm