Vol. 10 | Issue 7

NEWS CYBER SECURITY

July 2025

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Summer Travel? Don't Take A Vacation From Cyber Awareness

What to know: Vacations are relaxing (most of the time) – but hackers don't take time off. When you're on the road (or in the air), your personal devices are more exposed than usual.

When traveling, your phone, tablet, and laptop are constantly connecting to unfamiliar networks and devices. That makes them prime targets for:

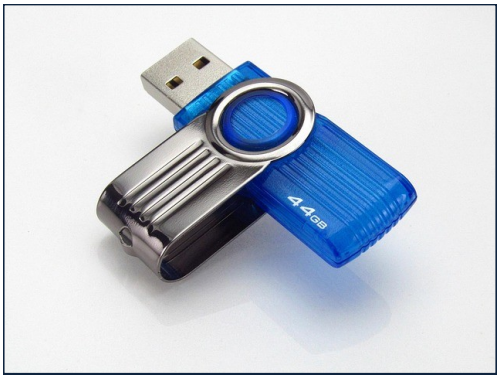
- *Wi-Fi snooping* on public or hotel networks.
- *Juice jacking* from USB charging stations.
- *Device theft* or loss with saved credentials still active.
- *Malware* from downloading apps or files while abroad.

Here are a few simple habits that go a long way:

- **Use a VPN on public Wi-Fi** – it encrypts your traffic.
- **Avoid public USB charging stations** – use a wall plug instead.
- **Enable full-device encryption and screen locks.**
- **Update your devices** before you leave – security patches matter.
- **Pack only what you need** – leave unnecessary tech at home.
- **Be cautious with pop-ups, downloads, or unfamiliar apps** – especially overseas.

More tips: https://www.staysafeonline.org/articles/vacation-and-travel-security-tips

USBs: Small Device, Big Risk



Whether we like it nor not, each of us now rely on technology to make work faster, easier, and more portable.

But one of the smallest tools that may be on your desk (both at home and at work) – the USB drive – can carry serious risks if not used wisely.

Whether it's a personal flash drive you've had for years or one you found lying around, plugging it into a work device can put the entire agency at risk. Even something as innocent as charging your phone through a work laptop can introduce threats.

So what's the risk?

USB flash drives can carry hidden malware that installs itself the moment the device is plugged in. No need to open a file. No need to click anything.

Attackers know this – and often leave infected drives in public spaces (like parking lots or restrooms) hoping someone picks one up and plugs it in. It's called "USB baiting," and unfortunately, it works. We are curious creatures and just can't seem to help ourselves.

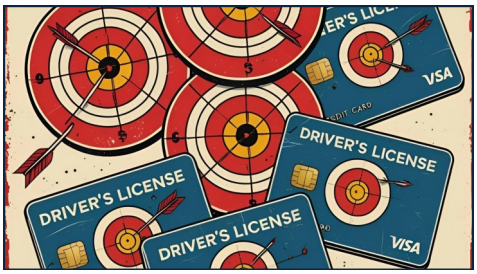
To keep our systems and data safe:

- **Don't plug in found USB drives – ever.**
  Even at home, it's not worth the risk. Fight that urge.
- **Do not use personal USBs for work.**
  Transferring files between home and work can create unintended vulnerabilities.
- **Use secure, approved tools for file transfers.**
  Shared drives or collaboration platforms (SharePoint, for example) are safer and supported.
- **Ask before you connect.**
  Not sure if a device is safe? Cyber can help. It's always better to check first.

Bottom line: A USB flash drive may look harmless, but it can quietly open the door to malware, data theft, and network compromise. When it doubt, just leave it out.

In the News

Weaponized DMV-Themed Phishing Scam Targets U.S. Citizens to Steal Personal and Financial Data



(Aman Mishra | June 24, 2025)

"A highly coordinated phishing campaign impersonating various U.S. state Departments of Motor Vehicles (DMVs) has emerged as a significant threat, targeting citizens across multiple states with the intent to harvest personal and financial data.

This sophisticated operation employs SMS phishing, commonly known as smishing, by sending alarming text messages from spoofed numbers that often appear to originate from local DMV agencies.

These messages typically warn of unpaid toll violations or threats of license suspension, citing fictitious legal codes to bolster credibility, and urge victims to click on malicious links to resolve fabricated fines.

Technical analysis has revealed that many of these spoofed numbers trace back to origins in the Philippines, showcasing the attackers' adept use of SMS spoofing techniques to enhance the scam's legitimacy.

Upon clicking the links, victims are directed to meticulously crafted fake DMV websites tailored to match their state's branding, such as those for Pennsylvania, Georgia, Texas, California, New Jersey, New York, and Florida."

Full Story: https://gbhackers.com/weaponized-dmv-themed-phishing-scam-targets-u-s-citizens

A Few More Cyber News Stories:

US Homeland Security warns of escalating Iranian cyberattack risks
https://www.bleepingcomputer.com/news/security/us-homeland-security-warns-of-escalating-iranian-cyberattack-risks

Aflac duped by social-engineering attack, marking another hit on insurance industry
https://cyberscoop.com/aflac-cyberattack-insurance-sector-scattered-spider

364,000 Impacted by Data Breach at LexisNexis Risk Solutions
https://www.securityweek.com/364000-impacted-by-data-breach-at-lexisnexis-risk-solutions

CYBER CHALLENGE

Spot the Phish

This Month's Challenge

For this month's challenge, let's see how well you can identify a phishing email. Yes...more phishing email practice!

You'll have 8 emails to look at and decide whether they are genuine or phishing scams.

Good luck! Let me know how you do.

https://www.egress.com/blog/phishing/spot-the-phish