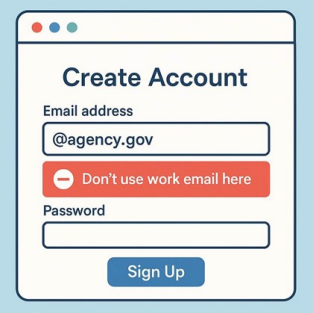
Vol. 10 | Issue 8

NEWS CYBER SECURITY

August 2025

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Don't Use Company Email Addresses to Create Personal Accounts



What to know: There has been a recent surge in credential leaks involving business email addresses.

The common thread? People using their work email address to sign up for personal accounts on third-party websites. When those sites get breached – and many do – the stolen login info includes your organization email domains, putting your entire workplace at risk.

What's happening:

- **Breached websites** - sites you use for personal reasons are frequent targets.
- **Credential dumps** - attackers steal login info, and if your work email was used, it's now exposed.
- **Password reuse = bigger risk** - reusing passwords means attackers could try those same credentials to access your actual work accounts.

Why it matters: Once your work email shows up in a leak, it opens the door to phishing, targeted scams, and automated login attempts – all pointed at company systems.

How to protect yourself :

- **Use a personal email** for non-work-related accounts.
- **Create unique passwords** for every account – both personal and professional.
- **Use a password manager** to help keep things organized and secure.
- **Pause before signing up** – not every site needs your info.

If you use your work email for personal accounts, you're not just risking your own info – you're exposing your workplace to avoidable threats. Keeping work and personal accounts separate is a small step that goes a long way.

In the News

Microsoft SharePoint attacks ensnare 400 victims, including federal agencies

(Matt Kapko | July 24, 2025)

"The fallout from an attack spree targeting defects in on-premises Microsoft SharePoint servers continues to spread nearly a week after zero-day exploits were discovered, setting off alarms across the globe. More than 400 organizations have been actively compromised across four waves of attacks, according to Eye Security.

Multiple government agencies, including the Departments of Energy, Homeland Security and Health and Human Services, have been hit. The California Independent System Operator, which operates some of the state's wholesale electric grid, was also impacted.

As more victims confirm varying levels of compromise from the attack spree, researchers are learning and sharing more details about post-exploit activities. One of the China-based attackers behind the initial wave of attacks, Storm-2603, deployed Warlock ransomware starting July 18, Microsoft Threat Intelligence said Wednesday in an updated blog post.

The Chinese government-affiliated threat groups Linen Typhoon and Violet Typhoon — which have been active for at least a decade — are also actively exploiting the zero-day vulnerabilities, Microsoft said. Linen Typhoon has focused on stealing intellectual property and Violet Typhoon is an espionage threat group. Storm is a moniker Microsoft uses for threat groups in development."

Full Story: https://cyberscoop.com/microsoft-sharepoint-attacks-400-victims-us-agencies

A Few More Cyber News Stories:

Over 5.4 Million Affected in Healthcare Data Breach at Episource
https://www.infosecurity-magazine.com/news/54-million-affected-episource

NASCAR notifies data breach victims after cybercriminals demand $4 million ransom
https://www.comparitech.com/news/nascar-notifies-data-breach-victims-after-cybercriminals-demand-4-million-ransom

FBI seizes $2.4M in Bitcoin from new Chaos ransomware operation
https://www.bleepingcomputer.com/news/security/fbi-seizes-24m-in-bitcoin-from-new-chaos-ransomware-operation

CYBER CHALLENGE

Word Search

This Month's Challenge

For this month's challenge, let's take it back to the basics and refresh our cyber vocabulary.

Anybody enjoy a good ol' word search puzzle? Hopefully not just me.

Let me know if this is way too basic or if there were actually a few terms you needed to brush up on.

Enjoy!

https://securityawareness.dcsa.mil/cdse/multimedia/games/wordfinds/index.html?request=cyber-1

D	Z	A	Z	A	T	R	R	S	I	Z	V	O	D	E	S	B	F
E	A	G	M	N	F	E	Y	O	M	P	A	S	S	W	O	R	D
X	W	C	B	T	V	K	N	A	W	I	Y	J	T	W	V	T	F
T	N	K	O	I	B	C	O	C	K	P	S	U	O	F	S	C	V
Q	Z	H	G	V	A	N	J	B	R	N	H	H	F	I	L	Y	C
V	I	S	H	I	N	G	V	J	L	Y	R	I	I	L	D	V	A
P	N	C	E	R	R	L	V	U	D	U	P	G	S	N	Y	I	H
U	E	R	L	U	Y	K	Q	I	R	B	E	T	W	H	G	B	D
U	Y	G	P	S	W	L	J	K	S	W	H	T	I	X	I	D	L
M	G	O	Z	P	W	H	P	Y	P	M	U	F	O	O	E	N	Z
T	C	Y	B	E	R	S	E	C	U	R	I	T	Y	O	N	C	G
M	T	E	U	F	H	V	G	N	X	R	O	C	Y	Y	T	W	M
A	R	I	K	G	D	L	H	E	M	H	A	C	K	E	R	H	B
L	O	X	V	V	U	L	N	E	R	A	B	I	L	I	T	Y	D
W	J	I	X	P	F	I	R	E	W	A	L	L	X	Y	F	Q	M
A	A	O	Q	W	M	S	D	G	N	E	T	W	O	R	K	L	H
R	N	V	O	P	A	S	S	P	H	R	A	S	E	T	H	E	M
E	H	A	A	Q	I	K	R	A	N	S	O	M	W	A	R	E	K