NEWS CYBER SECURITY

Vol. 10 | Issue 1

January 2025

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Happy New Year! Let's Outsmart Scammers in 2025

What to know: The new year is here, and while you're setting your resolutions, don't forget to make one about staying cyber aware.

The year has changed, but much of our guidance remains the same.

Return to these basics again and again this year to stay atop cyber threats:

- **Pause Before You Click:** Got an email, text, or message asking you to click a link? Take a second to think. Scammers love urgency – don't give in. Hover over links and verify they're legit before clicking.
- **Verify the Source:** Unexpected email from your "bank"? A surprise offer that's "too good to be true"? Contact the organization directly through their official website or phone number – not through links in the message.
- **Guard Your Personal Info:** No one legit will ever ask for sensitive info like passwords, Social Security numbers, or bank account details via email or text. If they do, it's a red flag!
- **Use Strong Passwords:** Make sure your passwords are unique and tough to crack. Better yet, use a password manager to keep them secure.
- **Enable Multi-Factor Authentication (MFA):** Add an extra layer of security to your accounts. Even if a scammer gets your password, MFA can block their access.
- **Stay Alert for Phishing:** Look for typos, odd email addresses, or generic greetings like "Dear User." AI is going to make this tough. But if something feels off, trust your instincts.
- **Keep Software Updated:** Scammers exploit outdated systems. Update your devices regularly to patch security gaps.

More on protecting yourself in '25: https://blog.ssa.gov/resolve-to-protect-yourself-from-scams-this-new-year

Data Privacy

January is the perfect time to lock down your personal information, with Data Privacy Week (January 27–31) at the end of this month to remind us all: our data is valuable – we should treat it that way.

Data privacy is the practice of safeguarding your personal information – like your name, contact details, social security number, and financial records – so it's only accessible to those who need it. In a world where we share so much online, keeping that data private is more important than ever.

When your data is compromised, it can lead to identity theft, financial loss, or even physical danger. Scammers, hackers, and other bad actors are constantly on the lookout for ways to exploit your personal info. That's why taking steps to protect your data is a must!

Here are some easy ways to keep your private information, well… private:

- **Review Privacy Settings:** Take a few minutes to check the privacy settings on your social media, apps, and devices. Limit what you're sharing publicly.
- **Think Before You Share:** Avoid oversharing personal information on social media – like your birthday, location, or vacation plans. Scammers love that stuff.
- **Delete Old Accounts:** Don't leave forgotten accounts lingering; they can become targets for data breaches.
- **Monitor Financial Accounts:** Check your bank and credit card statements frequently to catch any suspicious activity early.
- **Shred Paper Documents:** Physical documents containing personal information should be shredded to prevent identity theft.
- **Secure Your Devices:** Set up passwords or PINs on all your devices – phone, tablet, laptop, etc. And use biometrics (fingerprint, facial recognition) if available.
- **Avoid Using the Same Password for Everything:** It's tempting, but using the same password across multiple sites increases your risk. Mix it up!
- **Be Cautious About Free Trials:** Some free trials may ask for more than just your payment info; watch for personal data requests and read the fine print.

More privacy tips and info about Data Privacy Week: https://www.staysafeonline.org/data-privacy-week

In the News

Texas Tech University System data breach impacts 1.4 million patients

(Bill Toulas | December 16, 2024)

The Texas Tech University Health Sciences Center and its El Paso counterpart suffered a cyberattack that disrupted computer systems and applications, potentially exposing the data of 1.4 million patients.

The organization is a public, academic health institution that is part of the Texas Tech University System, which educates and trains healthcare professionals, conducts medical research, and provides patient care services.

The organization announced that, in September 2024, it suffered a cyberattack involving sensitive data theft.

"In September 2024, the HSCs identified issues that resulted in a temporary disruption to some computer systems and applications," reads the notice.

"Immediately after identifying these issues, the HSCs took steps to ensure the security of the network and began an investigation. The investigation confirmed that a cybersecurity event caused the technology issues, resulting in access to or removal of certain files and folders from the HSCs' network between September 17 and September 29, 2024."

In a filing with the U.S. Department of Health and Human Services Office for Civil Rights, the Texas Tech University Health Sciences Center reports that the breach exposed the combined data of 1,465,000 people.

Full Story: https://www.bleepingcomputer.com/news/security/texas-tech-university-system-data-breach-impacts-14-million-patients

A Few More Cyber News Stories:

US Arrests Army Soldier Over AT&T, Verizon Hacking
https://www.securityweek.com/us-arrests-charges-army-soldier-suspected-of-extorting-att-verizon

The biggest cybersecurity and cyberattack stories of 2024
https://www.bleepingcomputer.com/news/security/the-biggest-cybersecurity-and-cyberattack-stories-of-2024

How to Lose a Fortune with Just One Bad Click
https://krebsonsecurity.com/2024/12/how-to-lose-a-fortune-with-just-one-bad-click

CYBER CHALLENGE

Privacy Pirates

This Month's Challenge

For this month's challenge, let's give those little ones in our lives a chance to see if they know how to handle private data online.

Privacy education must go beyond "don't talk to strangers"; kids today need to be taught how to safely and responsibly judge and manage their privacy in a wide range of contexts.

Here's an overview of online privacy issues, as well as suggestions for playing the game with children and extension activities: https://mediasmarts.ca/sites/mediasmarts/files/guides/privacy-pirates-guide.pdf

This challenge is for kids 7-9yrs old (or adult kids if you'd like). Let me know how they (or you) do!

https://mediasmarts.ca/sites/default/files/games/privacy_pirates/en/story.html