NEWS
CYBER SECURITY
Vol. 11 | Issue 1
January 2026

| Page 2 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Data Privacy is in Everyday Decisions

What to know: The way we create, store, share, and reuse information has a direct impact on how well sensitive data is protected. Most data incidents don't start with a malicious actor. They start with data quietly ending up where it shouldn't.

Data privacy risks often show up through:

- **Unintentional data leakage** (oversharing, misdirected files, public links).
- **Insider risk** (well-meaning actions that bypass safeguards).
- **Fast-moving work** (makes it easy to skip a double-check).

None of these require bad intent. They only require a moment of inattention.

Here's where we see issues most often:

- **Email & collaboration tools**
  Auto-complete mistakes, forwarding, or links with broader access than intended.
- **Cloud storage & shared drives**
  Files that live longer – and reach farther – than expected.
- **Access & permissions**
  Old access that was never removed, or access granted "just in case."
- **Personal devices or accounts**
  Convenience that blurs the line between work and personal use.

A few simple habits make a real difference:

- **Pause before you share**. Double-check recipients, permissions, and link settings.
- **Limit access intentionally**. Give access only to those who truly need it – and remove it when they don't.
- **Store data thoughtfully**. Use approved locations and avoid spreading sensitive files across tools
- **Speak up early.** If something doesn't feel right, it's okay to ask or report it.

Data privacy isn't one big decision – it's dozens of small ones made every day. Being intentional about where information goes is one of the simplest and most effective ways we protect data.

In the News

Criminals Using Altered Proof-of-Life Media to Extort Victims in Virtual Kidnapping for Ransom Scams

(FBI PSA | December 05, 2025)

"The Federal Bureau of Investigation (FBI) warns the public about criminals altering photos found on social media or other publicly available sites to use as fake proof of life photos in virtual kidnapping for ransom scams. The criminal actors pose as kidnappers and provide seemingly real photos or videos of victims along with demands for ransom payments.

THE SCAM

Criminal actors typically will contact their victims through text message claiming they have kidnapped their loved one and demand a ransom be paid for their release. Oftentimes, the criminal actor will express significant claims of violence towards the loved one if the ransom is not paid immediately. The criminal actor will then send what appears to be a genuine photo or video of the victim's loved one, which upon close inspection often reveals inaccuracies when compared to confirmed photos of the loved one. Examples of these inaccuracies include missing tattoos or scars and inaccurate body proportions. Criminal actors will sometimes purposefully send these photos using timed message features to limit the amount of time victims have to analyze the images.

TIPS TO PROTECT YOURSELF

- When posting missing person information online, be mindful that scammers may contact you with fake information regarding your loved one.
- Avoid providing personal information to strangers while traveling.
- Establish a code word only you or your loved ones know that you can use to communicate.
- Scammers portray a false sense of urgency. Stop and think; do the kidnapper's claims make sense?
- Screenshot or record proof of life photos whenever possible.
- Always attempt to contact your loved one before considering paying any ransom demand."

Full Story: https://www.ic3.gov/PSA/2025/PSA251205

A Few More Cyber News Stories:

Featured Chrome Browser Extension Caught Intercepting Millions of Users' AI Chats
https://thehackernews.com/2025/12/featured-chrome-browser-extension.html

4B+ records, including numerous LinkedIn profiles, exposed
https://cybernews.com/security/database-exposes-billions-records-linkedin-data

Doxers Posing as Cops Are Tricking Big Tech Firms Into Sharing People's Private Data
https://www.wired.com/story/doxers-posing-as-cops-are-tricking-big-tech-firms-into-sharing-peoples-private-data

CYBER CHALLENGE

Bank Scams

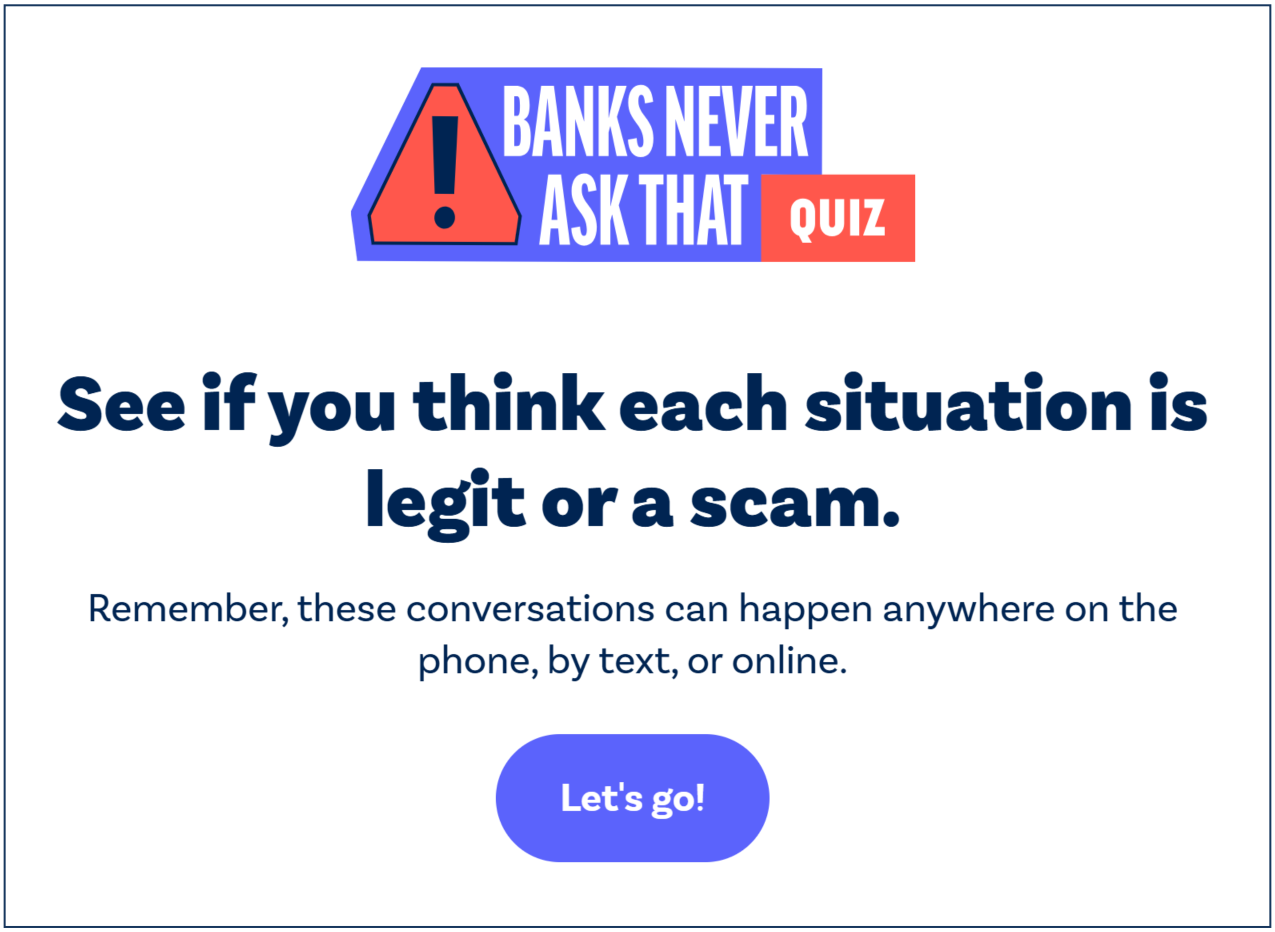
This Month's Challenge

For this month's challenge, let's practice identifying bank scams.

Now that we are passed the holiday season, many of us have credit card balances to pay down and bank statements to reconcile. Scammers know this, too.

In this challenge, you'll be presented with 9 scenarios. Is it a scam? Or is it most likely a legitimate message from your bank?

https://www.banksneveraskthat.com/scam-quiz



See if you think each situation is legit or a scam.

Remember, these conversations can happen anywhere on the phone, by text, or online.