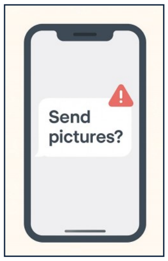
NEWS
CYBER SECURITY
Vol. 10 | Issue 12
December 2025

| Page 2 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Sextortion Awareness Matters - It Can Save Lives



What to know: *Sextortion* is when someone uses intimate images or videos – often ones they trick a person into sharing – to blackmail for money, more content, or control.

What's especially heartbreaking is that many victims, especially teens, feel too embarrassed or scared to ask for help. In the worst cases, some have felt so trapped they took their own lives. This isn't just a cyber issue – it's a safety and mental health concern that affects families everywhere.

Here's a short, helpful video that explains sextortion clearly and could be a useful conversation starter for families with teens: https://www.youtube.com/watch?v=ZnqmaenfOqY.

What you can do:

- **Learn the basic signs.** Sudden anxiety, device secrecy, or withdrawal may be indicators.
- **Remind kids (and adults!) that this can happen to anyone.** It's not their fault.
- **If targeted:** don't respond, don't pay, and capture screenshots. Attackers usually back off when ignored.
- **Report it.** Visit https://www.dhs.gov/know2protect/how-to-report for more info on how to report an incident.

To bring this up to your child, try - "I was reading about online safety and found out there's this one scam that's tricking thousands of teens – even really smart ones. The video explains it perfectly. Can I show you real quick?" Then show the video above (or find an online resource you like.)

Other quick talking points for parents and guardians:

- "If anyone online pressures you for pictures, you can always come to me - no trouble."
- "People pretend to be other kids online. If something feels off, let me know."
- "If someone threatens you, stop replying and come get me right away."

Yes, this can be a little awkward, but it's well worth being uncomfortable for a few minutes.

More resources: https://www.dhs.gov/know2protect

In the News

Holiday scams 2025: These common shopping habits make you the easiest target

(Malwarebytes Lab | November 20, 2025)

"Every year, shoppers get faster, savvier, and more mobile. We compare prices on the go, download apps for coupons, and jump on deals before they disappear. But during deal-heavy periods like Black Friday, Cyber Monday, and the December shopping rush, convenience can work against us.

Quick check-outs, unknown websites, and ads promising unbeatable prices make shoppers easy targets.

Shopping scams can steal money or data, but they also steal peace of mind. Victims often describe a mix of frustration, embarrassment, and anger that lasts for a long time. And during the holidays when you're already stretched thin, the financial and emotional fallout lands harder, spoiling plans, straining trust, and adding anxiety to what should be a joyful and restful time.

During the holidays, deal-chasing behavior spikes. Nearly 9 in 10 mobile consumers hand over emails or phone numbers in the name of savings—often without realizing how much personal data they're sharing.

- 79% sign up for promotional emails to get offers.
- 66% download an app for a coupon, discount, or free trial.
- 58% give their phone number for texts to get a deal.

This constant 'data for deals' exchange normalizes risky habits that scammers can easily exploit through fake promotions and reward campaigns."

Full Story: https://www.malwarebytes.com/blog/news/2025/11/holiday-scams-2025-these-common-shopping

A Few More Cyber News Stories:

ClickFix attack uses fake Windows Update screen to push malware
https://www.bleepingcomputer.com/news/security/clickfix-attack-uses-fake-windows-update-screen-to-push-malware

DoorDash hit by new data breach in October exposing user information
https://www.bleepingcomputer.com/news/security/doordash-hit-by-new-data-breach-in-october-exposing-user-information

$262 million stolen in account takeover fraud schemes this year, FBI says ahead of holiday season
https://therecord.media/millions-in-account-takeover-fbi-warns-ahead-of-holidays

CYBER CHALLENGE

Spot the Phish

This Month's Challenge

For this month's challenge, let's practice spotting phishing messages. We do this often because we need the reps. Especially now that we have a Report Phish button – we need to know what to report!

You'll have 10 messages to look over and decide whether they are a phishing attempt or a legitimate message.

https://phishingquiz.withgoogle.com