NEWS
CYBER SECURITY
Vol. 11 | Issue 3
March 2026

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: It’s Tax Season and Scams Are Sure to Follow

What to know: As we start filing our taxes, cybercriminals are revving up phishing emails, phone scams, and fake IRS notices to steal personal and financial information. These schemes often spike in March and April, so vigilance is key.

A few ways scammers will target us:

- **Phishing emails:** Cybercriminals send messages claiming to be the IRS or tax software companies, urging immediate action to “avoid penalties” or “get your refund.”
- **Phone scams:** Scammers may call threatening legal action or impersonating IRS agents demanding payment.
- **Malware and links:** Links in emails or texts can download malware that steals login credentials or sensitive files.
- **Personal data requests:** Social Security numbers, bank account details, and W-2s are prime targets.

How to protect your data:

- **Only use official IRS websites** (irs.gov) and verified tax software.
- **Don’t click links or open attachments** in unsolicited emails or texts about taxes.
- **Verify phone calls independently** - hang up and call the IRS directly if in doubt.
- **Use strong, unique passwords** for any tax accounts and enable multi-factor authentication.
- **Consider freezing your credit** if you suspect fraud or identity theft.

More on tax-scam awareness: https://www.irs.gov/individuals/taxes-security-together

PDF Attachments

Many organizations regularly receive legitimate emails with attachments from external entities as part of their business process. Opening PDF attachments can feel routine.

That routine is exactly what attackers rely on.

What to know: PDFs can carry malware. They may contain malicious links, hidden downloads, or fake login pages designed to steal credentials.

Why this isn't simple: Standard advice like "don't open attachments from unknown senders" doesn't always apply here. Some roles legitimately receive emails from unfamiliar counties, courts, and investigators, for example. Case numbers may be real. The message may be brief and include a PDF attachment.

That's normal. The key isn't panic; it's pause.

The biggest red flag: A credential prompt inside a PDF is a major warning sign. If a PDF asks for your credentials to view the document – stop. Then report it to your cyber team.

Other things to watch out for:

- A "View Secure Document" button or other links inside the PDF.
- Slightly misspelled or unusual sender domains.
- Urgent threats with little context.

When in doubt, verify using a trusted phone number, not one listed in the suspicious email.

The bottom line: Security incidents can happen because someone didn't know better. But they often happen because something looked routine.

Pause. Inspect. Then open. Or ask for help.

More on malicious PDFs: https://blog.checkpoint.com/research/the-weaponization-of-pdfs-68-of-cyberattacks-begin-in-your-inbox-with-22-of-these-hiding-in-pdfs

In the News

How fake party invitations are being used to install remote access tools

(Stefan Dasic | February 2, 2026)

"'You're invited!'

It sounds friendly, familiar and quite harmless. But in a scam we recently spotted, that simple phrase is being used to trick victims into installing a full remote access tool on their Windows computers—giving attackers complete control of the system.

What appears to be a casual party or event invitation leads to the silent installation of ScreenConnect, a legitimate remote support tool quietly installed in the background and abused by attackers.

Here's how the scam works, why it's effective, and how to protect yourself.

The email: A party invitation
Victims receive an email framed as a personal invitation—often written to look like it came from a friend or acquaintance. The message is deliberately informal and social, lowering suspicion and encouraging quick action.

In the screenshot below, the email arrived from a friend whose email account had been hacked, but it could just as easily come from a sender you don't know.

So far, we've only seen this campaign targeting people in the UK, but there's nothing stopping it from expanding elsewhere.

Clicking the link in the email leads to a polished invitation page hosted on an attacker-controlled domain.

The invite: The landing page that leads to an installer
The landing page leans heavily into the party theme, but instead of showing event details, the page nudges the user toward opening a file…"

Full Story: https://www.infosecurity-magazine.com/news/32m-phishing-emails-detected-2025

A Few More Cyber News Stories:

Crims hit a $20M jackpot via malware-stuffed ATMs
https://www.theregister.com/2026/02/19/crims_atm_jackpotting

Panera Bread breach affected 5.1 Million accounts, HIBP Confirms
https://securityaffairs.com/187556/data-breach/panera-bread-breach-affected-5-1-million-accounts-hibp-confirms.html

Attackers Weaponize Signed RMM Tools via Zoom, Meet, & Teams Lures
https://www.netskope.com/blog/attackers-weaponize-signed-rmm-tools-via-zoom-meet-teams-lures

CYBER CHALLENGE

Spot the Phish

This Month's Challenge

For this month's challenge, let's keep practicing spotting a phishing email.

You'll be presented with 5 messages and challenged to pick the phish.

This may be a little too easy … but let's see!

If you would, take a little time to read the breakdown after you answer each question. I think it does a pretty good job and explaining what to look for in phishing emails. That info will serve you well!

Good luck! Let me know how you do.

https://www.marconet.com/spot-the-phish