Vol. 11 | Issue 4

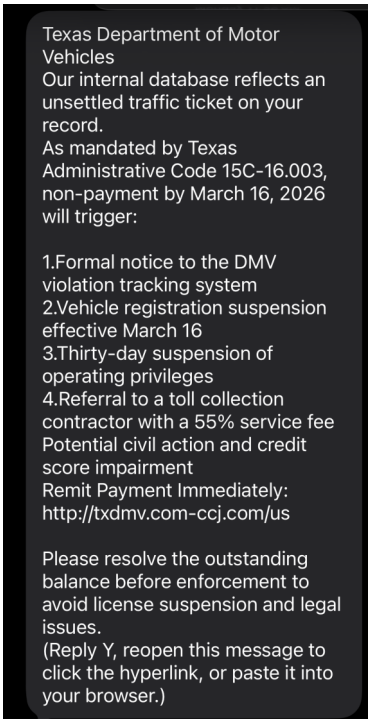
CYBER SECURITY NEWS

April 2026

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: They're baaaaack! Toll Tag and DMV Text Scams Circulating Nationwide



What to know: Smishing messages posing as the DMV, toll agencies, and toll tag providers are making their rounds again—and they're hitting phones nationwide, including here in Texas. Recent warnings from the TxDMV show the campaign has surged again in March.

Even if you haven't used a toll road recently or received a citation, you may still receive one of these because they are sent broadly and at random.

The goal is simple: get you to click the link and provide personal or financial information.

If you receive one of these text messages:

- Don't reply.
- Don't click the click.
- Report as junk/spam.
- Delete the message.
- If unsure, verify through official websites only.

Remember: urgency is often the scam. Take a moment to verify before you act.

Physical Security

When we think about cybersecurity, most of us picture passwords, phishing emails, and suspicious links.

But cybersecurity is not just digital.

Physical security is the protection of people, devices, documents, and workspaces from theft, loss, or unauthorized access. In a hybrid work world, that matters just as much at home as it does in the office.

A laptop left unattended, a badge loaned to a coworker, or sensitive documents sitting in plain view can create the same kind of risk as clicking a bad link. Sometimes the simplest oversights can lead to the biggest problems.

Common Risks to Watch For

A few everyday situations can quickly become cybersecurity issues:

- **Unattended devices** – leaving laptops, phones, or tablets unlocked and visible.
- **Tailgating / piggybacking** – someone following into a secured area without using their own badge.
- **Documents left out** – printed materials visible on desks, printers, or in home workspaces.
- **Lost badges, keys, or USB drives** – small items that can provide access to systems or sensitive information.

Good Habits That Go a Long Way

A few simple practices make a big difference:

- **Lock your screen** anytime you step away, even if it's only for a moment.
- **Keep badges and access cards secure** and report lost items right away.
- **Maintain a clean workspace** at the office and at home.
- **Be aware of your surroundings**, especially in shared spaces or public areas.
- **Store company devices and sensitive documents securely** when not in use.

More on physical security: https://www.staysafeonline.org/articles/why-physical-security-is-still-necessary-for-cybersecurity

In the News

New Social Security Scam Emails Use Fake Tax Documents to Hijack PCs

(Deeba Ahmed | March 7, 2026)

"A new scam is currently targeting thousands of people across the United States, using the name of the Social Security Administration to trick unsuspecting users. This campaign, which was first identified by the security firm LifeLock, arrives just in time for the busy tax season.

As per LifeLock's tweet, the scam works by sending emails that look like official government notifications. As we have generally noticed, scammers rely on this sense of urgency to make people act without thinking. In this case, the same thing happens.

These messages use urgent language such as "Important Disclosures" or "Important Regulatory Information" to grab a person's attention. And, while the sender's name might say Social Security Administration, investigation revealed that the emails do not actually come from a legitimate government domain ending in .gov.

How the trap works

The emails typically include a link or a file that looks like a standard PDF statement. It might have a name like "Social_security_statements_2025.pdf." However, researchers noted that this is not a normal document, and the file uses a tool called Datto RMM.

Normally, RMM (Remote Monitoring and Management) is a helpful tool used by IT experts to fix computers from a distance. But here, it has been turned into a weapon. If a user clicks the link to view the document, it can install a RAT (Remote Access Trojan (RAT).

Further probing revealed that this allows attackers to take full control of a person's device. Once they have access, they can watch what the user is doing and steal private data."

Full Story: https://hackread.com/social-security-scam-emails-fake-tax-doc-hijack-pc

A Few More Cyber News Stories:

An AI-powered phishing campaign has compromised hundreds of organizations
https://cyberscoop.com/huntress-railway-ai-phishing-campaign-compromised-hundreds-of-organizations

One click on this fake Google Meet update can give attackers control of your PC
malwarebytes.com/blog/threat-intel/2026/03/one-click-on-this-fake-google-meet-update-can-give-attackers-control-of-your-pc

LastPass warns of spoofed alerts aimed at stealing master passwords
https://securityaffairs.com/188911/security/lastpass-warns-of-spoofed-alerts-aimed-at-stealing-master-passwords.html

CYBER CHALLENGE

Trivia Twirl

This Month's Challenge

For this month's challenge, let's see how well you do in different domains of cyber awareness.

You'll have the opportunity to flex your knowledge in 6 categories. Can you ace them all?

Let me know how you do!

https://securityawareness.dcsa.mil/cdse/multimedia/games/cybertrivia/index.html