NEWS

CYBER SECURITY

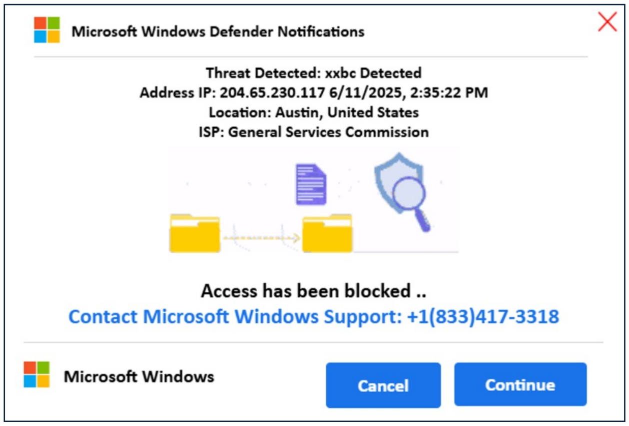
Vol. 10 | Issue 9

September 2025

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Don't Fall For Scareware Scams and Infect Your Computer



Microsoft Windows Defender Notifications

Threat Detected: xxbc Detected
Address IP: 204.65.230.117 6/11/2025, 2:35:22 PM
Location: Austin, United States
ISP: General Services Commission

Access has been blocked ..

Contact Microsoft Windows Support: +1(833)417-3318

Microsoft Windows

What to know: It's a tried and true scam that just keeps working. Luring you into calling "Microsoft Support" and allowing scammers to access your laptop. Not good.

Why it matters: Allowing scammers to access your devices is a major breach and obviously puts you at risk. As a reminder, scareware is designed to trick you into clicking on fake alerts, calling a "support" line, or downloading harmful software. It looks urgent when it pops up in your browser, but it's a scam. *Don't fall for it!*

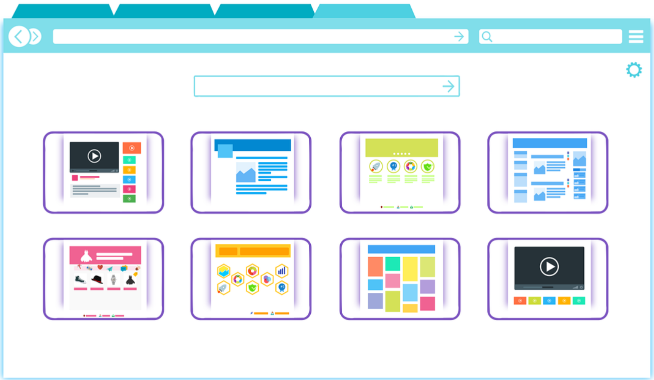
What we're seeing: Many reports mention pop-ups showing up after clicking ads or links on news sites or while browsing online. These are often legit sites with shady ads embedded – it happens.

What to do:

- **Pause** before reacting – take a moment to assess the pop-up without clicking anything.
- **Ignore** scare tactics – real security warnings don't ask you to call numbers or download unfamiliar software.
- **Capture and report** anything strange – a quick screenshot and an email to your cyber team is helpful, if you can do so safely.
- **Exit the browser** – close the entire browser using the "X" on the browser window, not the pop-up (closing the individual pop-ups may actually generate more of them). If the scareware page seems to be full screen, you can get out by holding ESC key.
- **Stay alert** on high-traffic sites – even trusted websites can show risky ads.
- **Reach out** if you're unsure – your cyber team would much rather hear from you than have you second-guess.

More on scareware (because this will happen at home, too): https://www.malwarebytes.com/cybersecurity/basics/scareware

Secure Web Browsing



We all use the internet a little differently – some for research, some for shopping, and sometimes just to unwind. And while the web is an incredible resource, it also comes with risks that aren't always obvious.

Here's the thing: even run-of-the-mill browsing can create security gaps, especially on company devices. While it's not uncommon for people to check the news or quickly look up a recipe, it's much safer to keep work devices focused on work. Why? Because the more casual clicks and pop-ups you encounter, the more chances attackers have to slip something through.

Five ways to browse more securely:

- **Stick to trusted sites –** Bookmarks are your friend. Save sites you know are legitimate instead of typing them in or clicking search results.
- **Be pop-up wary –** If a window screams for urgent action ("Call now!"), it's most likely a scam. Close the tab instead of interacting.
- **Update regularly –** Browsers and extensions push security updates often. Restarting your browser keeps those protections active.
- **Limit add-ons –** Extensions can be helpful, but too many can slow you down or even create security risks. Install only what you truly need.
- **Separate work and play –** When you want to browse freely, use a personal device. It keeps agency systems more secure and keeps your personal activity private.

Go deeper: https://www.cisa.gov/resources-tools/training/tips-stay-safe-while-surfing-web-part-1-web-browser-settings

In the News

New WhatsApp Scam Poses Serious Risk: Hackers Can Hijack Your Chats

(Mayura Kathir | September 2, 2025)

“Users of the popular messaging app WhatsApp are being targeted by a new, highly deceptive scam that grants attackers full access to victims’ contacts, chat history, and media files.

Cybercriminals are exploiting the app’s device linking feature to hijack accounts, then using the compromised profiles to spread further malicious links to unsuspecting friends and family.

How the Scam Works

The attack begins with a seemingly innocent message from a friend’s number saying, “Hi, I accidentally found your photo!” accompanied by a shortened link.

The URL typically leads to a counterfeit Facebook login page, cleverly designed to mimic the real site’s look and feel. When the victim enters their Facebook credentials, the attacker captures them and uses them to trigger WhatsApp’s device linking process. Once the attacker initiates device linking, WhatsApp sends a QR code or six-digit code to the victim’s registered device.

Because the attacker already controls the victim’s Facebook session, they can intercept or manipulate the verification process, linking the victim’s WhatsApp account to the attacker’s device. The result is full remote access to all of the victim’s chats, shared media, contacts list, and group memberships.

After successfully controlling a WhatsApp account, attackers can impersonate the victim and message everyone in their contact list.”

Full Story: https://gbhackers.com/whatsapp-scam

A Few More Cyber News Stories:

Blog operators selling fake New Mexico driver’s licenses
https://www.klfy.com/news/border-report/blog-operators-selling-fake-new-mexico-drivers-licenses

Jaguar Land Rover ‘severely disrupted’ by cybersecurity incident
https://therecord.media/jaguar-land-rover-disruption-cyber-incident

Claude AI chatbot abused to launch “cybercrime spree”
https://www.malwarebytes.com/blog/uncategorized/2025/08/claude-ai-chatbot-abused-to-launch-cybercrime-spree

Cyber Crossword Puzzle

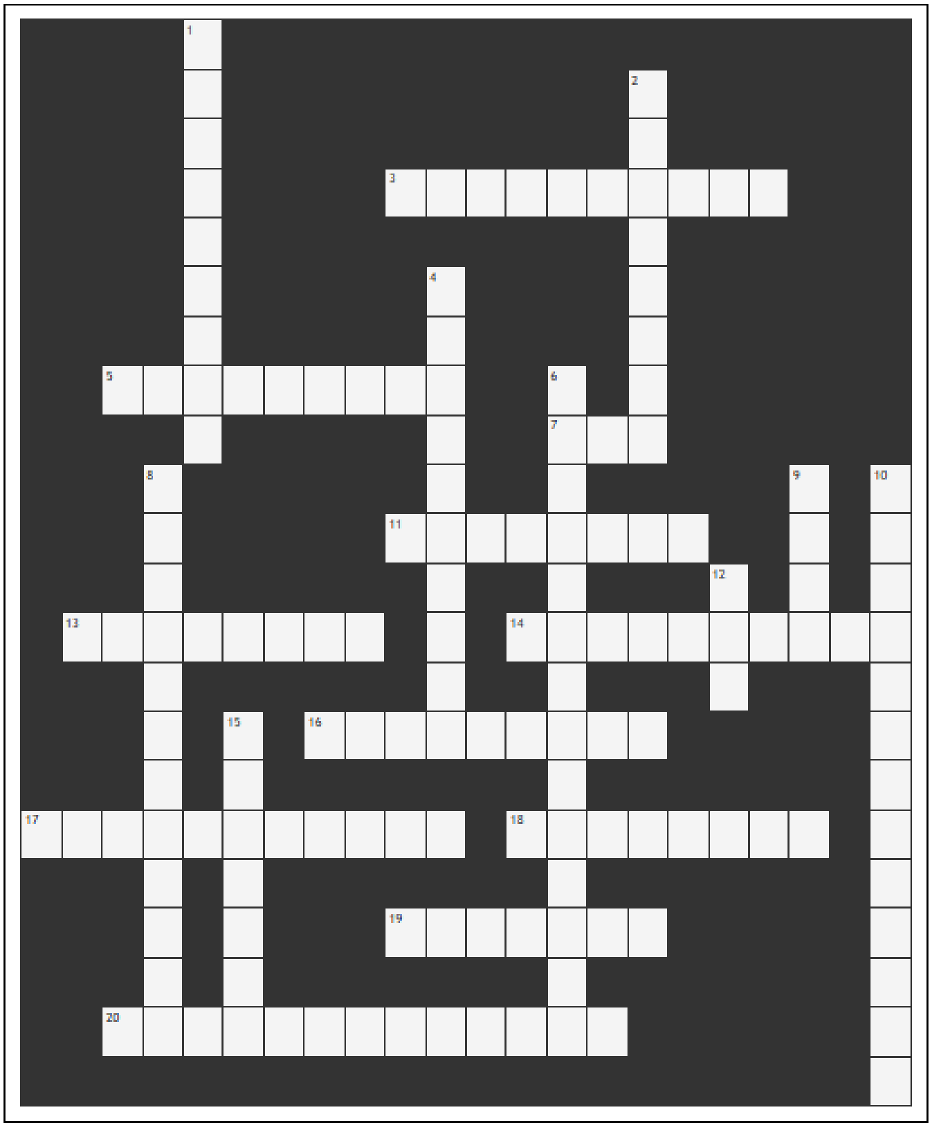
This Month's Challenge

For this month's challenge, let's keep going with puzzles.

Do all of these words sound familiar?

Have fun!

https://securityawareness.dcsa.mil/cdse/multimedia/games/crosswords/cybersecurity-crossword/index.html#


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20