Vol. 8 | Issue 11

NEWS CYBER SECURITY

November 2023

| Page 2 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

Winter is coming! Well, kind of. This is still Texas after all. The holiday season is on its way though!

One big thing: The Hacker Within

An insider threat can happen when someone close to an organization with authorized access misuses that access to negatively impact the organization's critical information or systems. This person does not necessarily need to be an employee – third-party vendors, contractors, and partners could pose a threat as well.

Insider threats can be unintentional or malicious, depending on the threat's intent. *Unintentional insider threats* can be from a negligent employee falling victim to a phishing attack. A *malicious threat* could be from intentional data theft, corporate espionage, or data destruction.

What Motivates a Malicious Insider?

- Desire for money or power
- Grudge against the organization, colleagues, or managers
- Job dissatisfaction or personal problems
- Corporate espionage

What Behaviors are Suspicious?

- Trying to obtain confidential information that's not appropriate for their role
- Removing assets from the workplace without permission
- Copying or printing information unnecessarily
- Talking openly about confidential matters
- Sending information to personal email accounts or using USB devices without permission

How to Help Protect Against Insider Threats

- Report suspicious activity. If you notice anyone acting suspiciously, report it to your Cyber team.
- Promote cyber awareness. Stay informed about the latest threats and best practices.
- Exercise caution with sensitive data. Handle it responsibly, ensuring it's only shared with those who need it and stored securely. Verify the legitimacy for any requests for sensitive information.
- Secure your credentials. Use strong, unique passwords and enable multi-factor authentication.
- Be cautious online. Avoid clicking links or downloading attachments from unknown sources.

Go deeper: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

In the News

Activist Hackers Are Racing Into the Israel-Hamas War–for Both Sides

(Lily Hay Newman | October 9, 2023)

Since the conflict escalated, hackers have targeted dozens of government websites and media outlets with defacements and DDoS attacks, and attempted to overload targets with junk traffic to bring them down.

After an attack on Israel by Hamas on Saturday, Israel declared war and fighting escalated throughout the weekend. As the death toll mounts on both sides and the Israeli Defense Force (IDF) prepares an offensive, hacktivists in the region and around the world have joined the fight.

Within hours of Hamas militants and rockets entering Israel, such "hacktivist" attacks started to spring up against both Israeli and Palestinian websites and applications. In the short period since the conflict escalated, hackers have targeted dozens of government websites and media outlets with defacements and DDoS attacks, attempts to overload targets with junk traffic and bring them down. Some groups claim to have stolen data, attacked internet service providers, and hacked the Israeli missile alert service known as Red Alert.

"I saw at least 60 websites get DDoS attacks," says Will Thomas, a member of the cybersecurity team at the internet infrastructure company Equinix who has been following the online activity. "Half of those are Israeli government sites. I've seen at least five sites be defaced to show 'Free Palestine'–related messages."

Most prominently seen in the war between Russia and Ukraine, it is increasingly common for both ideologically motivated hackers and cybercriminals to remotely join the chaos on either side of an escalating conflict by attacking government systems or other institutions.

Read full story: https://www.wired.com/story/israel-hamas-war-hacktivism/

A Few More Cyber News Stories:

Hostile Takeover: Malicious Ads via Facebook
https://www.gdatasoftware.com/blog/2023/10/37814-meta-hijacked-malicious-ads

Hackers 'don't break in anymore, they log in,' expert explains
https://finance.yahoo.com/video/hackers-dont-break-anymore-log-210812209.html

Apple Ships Major iOS, macOS Security Updates
https://www.securityweek.com/apple-ships-major-ios-macos-security-updates

CYBER CHALLENGE

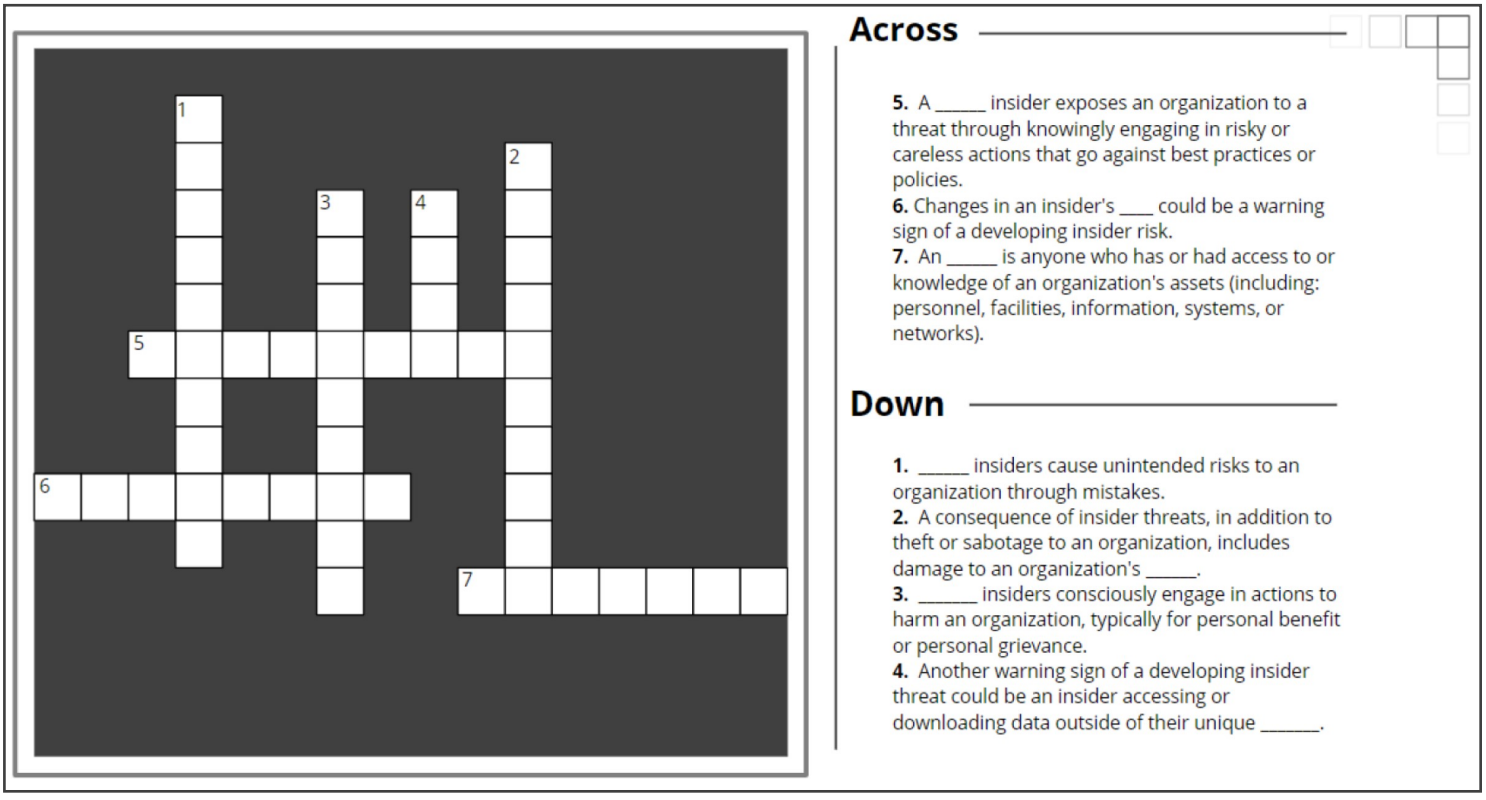
Insider Threat Crossword

This Month's Challenge

For this month's challenge, let's see how good you are at crossword puzzles...and how well you know Insider Threat terminology.

Let me know if you need a hint.

Good luck!



Across

5. A _____ insider exposes an organization to a threat through knowingly engaging in risky or careless actions that go against best practices or policies.
6. Changes in an insider's ____ could be a warning sign of a developing insider risk.
7. An _____ is anyone who has or had access to or knowledge of an organization's assets (including: personnel, facilities, information, systems, or networks).

Down

1. _____ insiders cause unintended risks to an organization through mistakes.
2. A consequence of insider threats, in addition to theft or sabotage to an organization, includes damage to an organization's _____.
3. _____ insiders consciously engage in actions to harm an organization, typically for personal benefit or personal grievance.
4. Another warning sign of a developing insider threat could be an insider accessing or downloading data outside of their unique _____.