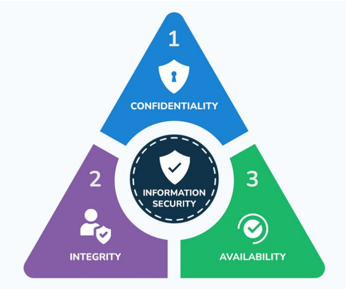
NEWS
CYBER SECURITY
Vol. 10 | Issue 2
February 2025

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Let's Revisit the CIA Triad - The Foundation of Data Security



What to know: "CIA" stands for Confidentiality, Integrity, and Availability. One of the most essential frameworks in cybersecurity is the CIA Triad - a model designed to guide security policies and safeguard information. Let's take a quick look at each component.

Confidentiality - Keeping Data Private
This means making sure information is only accessible to authorized individuals. You don't want just anyone accessing your data. Consider the impact of your data being leaked; identify theft, fraud, and damage to personal or corporate reputation, for example.

Protecting confidentiality involves using encryption, strong passwords, and access controls.

Integrity: Keeping Data Accurate and Unaltered
This means making sure data remains accurate, complete, and trustworthy over its entire lifecycle. You don't want your data altered or corrupted. Consider the impact of your data being changed and incorrect; inaccurate financial records, corrupt medical test results, or manipulated stock data, for example.

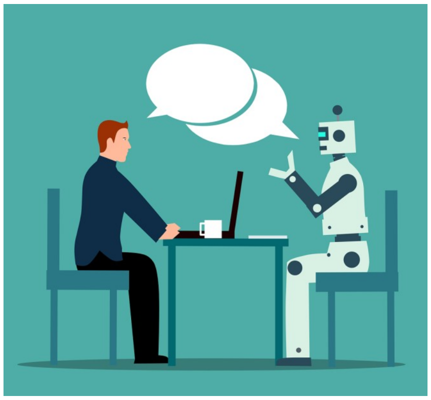
Protecting data integrity involves using methods such as data validation, hashing, and regular backups.

Availability: Ensuring Data is Accessible When Needed
This means making sure data is available to authorized users when required. You don't want your data to be unavailable when you need to access it. Consider the impact of your data being inaccessible; work grinding to a halt, financial loss, and customer dissatisfaction, for example.

Availability relies on maintaining proper infrastructure, regular system maintenance, and protection against disruptions such as cyberattacks or hardware failures.

Achieving an ideal balance of these three components is a unique, evolving challenge; but done right, helps keep data secure.

AI and Misinformation



Artificial Intelligence (AI) is revolutionizing technology and the way we live, but it's also being misused to create increasingly sophisticated scams and spread misinformation. From fake social media posts to realistic AI-generated audio and video deepfakes, it's becoming harder to tell what's real online.

Here are a few examples to watch out for:

News Too Good (or Shocking) to Be True

- Be wary of sensational headlines, unbelievable sales, or overly dramatic claims. Always check the source before sharing or acting on the information.

Conflicting Information Across Sources

- If one source reports something sensational , but other trusted sources don't mention it, the story might be false or exaggerated.

Deepfakes and Voice Scams

- AI-generated videos and audio clips can convincingly mimic real people. If you receive an unusual request from someone you know, double-check through another communication method.

Overly Refined Images

- AI-generated visuals can look almost perfect, but may have subtle flaws - like unnatural eye reflections, awkward hands shapes or mismatched backgrounds.

Phishing Emails with AI-Polished Language

- Scammers now use AI to craft convincing and professional-looking emails. Look for subtle red flags, like odd email addresses, urgent language, or unexpected attachments.

Customer Service Chatbots

- Fake chatbots with groomed responses might try to trick you into providing sensitive information. Always verify you're on an official company website.

Be sure to talk with family and friends about the risks of AI-generated scams and misinformation.

Go Deeper: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

In the News

Millions Impacted by PowerSchool Data Breach

(Ionut Arghire | January 25, 2025)

PowerSchool, which provides education software and services to more than 16,000 K12 schools and school districts in the US, Canada, and tens of other countries worldwide, informed its customers on January 7 that hackers stole their information from the PowerSchool Student Information System (SIS) service.

The attackers accessed the SIS service through the PowerSource customer support portal, stealing the names, contact information, dates of birth, medical information, Social Security numbers, and other information of both students and educators, PowerSchool said in an incident notice.

While details on how the incident occurred were not shared publicly, PowerSchool previously told its customers that 'a compromised credential' was used to access PowerSchool SIS.

"This credential, which was tied to a maintenance account, gave the threat actor(s) broad and deep access to many PowerSchool customers' data," the Menlo Park City School District (MPCSD) said in an incident notice.

PowerSchool engaged with Canadian firm CyberSteward to negotiate with the attackers and ensure that the stolen data is not shared publicly, suggesting that "PowerSchool paid the ransom and received reasonable assurances that the data was deleted," MPCSD said.

The school district revealed that the attackers stole the information of all individuals enrolled or working with MPCSD since 2009, and that the compromised information also includes parent/guardian/ emergency contact names, ID numbers, disability information, gender, race and ethnicity, and more.

Full Story: https://www.securityweek.com/millions-impacted-by-powerschool-data-breach

A Few More Cyber News Stories:

Scam Yourself attacks: How social engineering is evolving
https://www.helpnetsecurity.com/2025/01/21/scam-yourself-attacks

Subaru Starlink flaw let hackers hijack cars in US and Canada
https://www.bleepingcomputer.com/news/security/subaru-starlink-flaw-let-hackers-hijack-cars-in-us-and-canada

Tesla Gear Gets Hacked Multiple Times in Pwn2Own Contests
https://www.darkreading.com/vulnerabilities-threats/tesla-gear-hacked-multiple-times-pwn2own-contests

CYBER CHALLENGE

AI or Not AI?

This Month's Challenge

For this month's challenge, let's see how well you do telling the difference between AI-generated images and real images.

Some of these may be a little obvious. But some are really tough!

Let me know how you do. I'll be very impressed with a 100% accuracy rate.

Good luck!

https://sightengine.com/ai-or-not?version=2024Q1