Vol. 8 | Issue 4

CYBER SECURITY NEWS

April 2023

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

We hope this month's newsletter finds you well...and stocked up on allergy meds for all that Spring in the air!

1 big thing: Our Cyber team is looking for summer interns!

What to know: If you know a high school or college student interested in the opportunity to learn about cyber security, gain hands-on experience, and contribute to developing and implementing security measures to protect our agency, then please check out these job postings and then share away!

Please note: The candidates must be available to work on-site (in Austin) for the internship and be at least 17 years of age.

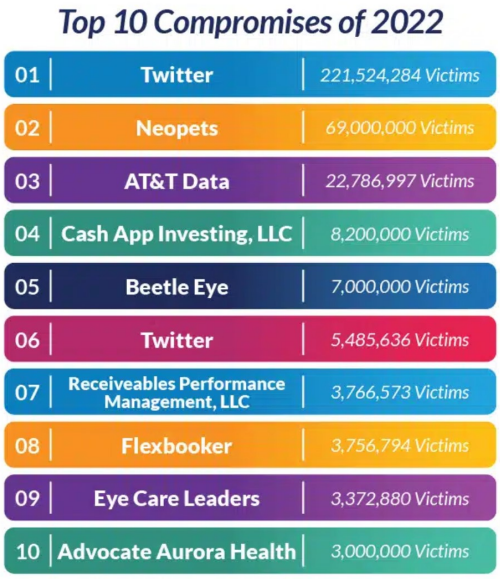
Available positions:

- Unpaid High School Intern posting: Cyber High School Intern
- Unpaid College Intern posting: College Cyber Security Intern
- Paid College Intern posting: College Cyber Security Intern

Breaches

Cybersecurity breaches have become a regular occurrence in recent years. So much so that we are no longer surprised by them, unfortunately.

In 2022 alone, there were over 1,800 data breaches reported*, with a total of over 420 million victims. This number of data breaches was the second-highest number in a single year...only 60 events short of 2021's all-time high in compromises.



The most common types of breaches include:

- **Data breaches:** This is when someone gains unauthorized access to your data, such as your customer information, financial information, or intellectual property.
- **Malware attacks**: This is when someone infects your computer or network with malware, such as ransomware or spyware.
- **Social engineering attacks**: This is when someone tricks you into giving them your personal information, such as your passwords or credit card numbers.

To see a global, live map of active cyber attacks, check out this website: https://threatmap.checkpoint.com

If you are the victim of a cybersecurity breach, there are a few things you can do to minimize the damage:

- **Report the breach to the authorities**. If your breach is significant, you will need to report it to the authorities, such as the Federal Trade Commission (FTC) or the Department of Justice (DOJ).
- **Monitor your credit reports**. If your breach exposed your personal information, such as your Social Security number, you should monitor your credit reports for any suspicious activity.
- **Change your passwords**. If your breach exposed your passwords, you should change them on all of your accounts.

*Source: https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises

In the News

Scammers use AI to enhance their family emergency schemes

(Alvaro Puig | March 20, 2023)

You get a call. There's a panicked voice on the line. It's your grandson. He says he's in deep trouble – he wrecked the car and landed in jail. But you can help by sending money. You take a deep breath and think. You've heard about grandparent scams. But darn, it sounds just like him. How could it be a scam? Voice cloning, that's how.

Artificial intelligence is no longer a far-fetched idea out of a sci-fi movie. We're living with it, here and now. A scammer could use AI to clone the voice of your loved one. All he needs is a short audio clip of your family member's voice – which he could get from content posted online – and a voice-cloning program. When the scammer calls you, he'll sound just like your loved one.

So how can you tell if a family member is in trouble or if it's a scammer using a cloned voice?

Don't trust the voice. Call the person who supposedly contacted you and verify the story. Use a phone number you know is theirs. If you can't reach your loved one, try to get in touch with them through another family member or their friends.

Scammers ask you to pay or send money in ways that make it hard to get your money back. If the caller says to wire money, send cryptocurrency, or buy gift cards and give them the card numbers and PINs, those could be signs of a scam.

If you spot a scam, report it to the FTC at ReportFraud.ftc.gov.

Source: https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes

A Few More Cyber News Stories:

The FBI's BreachForums bust is causing 'chaos in the cybercrime underground'
https://cyberscoop.com/breachforums-arrest-cybercrime-underground

Twitter says source code was leaked on GitHub, now it's trying to find the culprit
https://www.theverge.com/2023/3/27/23657928/twitter-source-code-leak-github

Beware: Fake IRS tax email delivers Emotet malware
https://www.malwarebytes.com/blog/news/2023/03/beware-fake-irs-tax-email-delivers-emotet-malware

CYBER CHALLENGE

Ultimate Challenge

This Month's Challenge

For this month's challenge, let's step up the difficulty a bit. I was asked by a few of you to provide a more challenging experience. So..let's see if this does the trick!

Inspired by real military missions, this interactive experience will see if you have what it takes to become an elite cyberwarrior.

I, admittedly, have not reached the final stage of this one (yet!). So I can't speak to how long this might take. But I'll get it done!

Can *you* make it to the Ultimate Challenge? If so, send me a screen shot and get some praise!

https://www.cybermission.tech/