Vol. 8 | Issue 7

CYBER SECURITY NEWS

July 2023

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

We hope this newsletter finds you well and beating this Texas heat. Stay cool...somehow.

1 big thing: If Found, Please Return to Cyber

What to know: Every summer, our cyber team does its best to hire a few interns who are interested in the cybersecurity field. These interns are high school and college students looking to broaden their knowledge, perspective, and experience.

Who to know: This year, we have 3 high school interns and 2 college interns.

Jai is passionate about ethical hacking and programming. Outside of interning, he's a chess enthusiast, avid Smash Bros player, and produces electronic music under the moniker *J18*.

Macy is interested in the cross-over between cybersecurity and AI. She loves trying new foods, traveling, and doing art in her free time. She's super excited to get to know everyone and to continue learning through this internship!

Charles became interested in cybersecurity after a data breach in 2015 resulted in personal information about him, his wife and his family being leaked onto the internet. His goal is to become a cybersecurity professional to try to prevent anyone else from suffering the constant stress of knowing their information has been stolen.

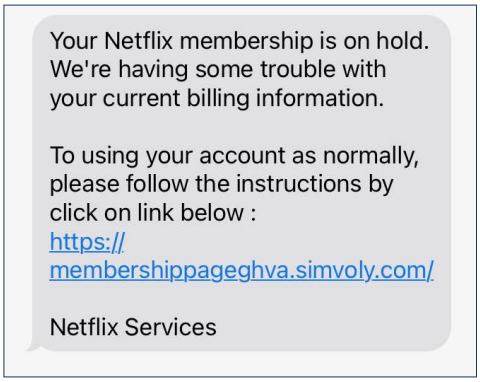
Turner is excited to learn more about ethical hacking as an intern. Outside of the office, he is a photographer, videographer, audio engineer, and musician. He can't wait to meet everyone and learn as much as possible through his intern position.

Caleb has aspirations of building a career in Machine Learning and Data Science. He's incredibly passionate about AI and hopes to spend his time as an intern searching for a way to implement it within the world of Cyber Security. Outside of the office/classroom, he's a programmer, violinist, and tournament competitor for Super Smash Brothers Ultimate.

As mentioned, we do this every summer so if you have any high school or college students in mind (we do ask they be able to be in the Austin area for the summer), please be on the look out for job postings come the spring.

Text Message Scams

Texting is cheap and easy, and scammers are counting on the ding of an incoming text being hard to ignore. Why do these text message scams work so well?



Scammers use the speed of text communication to their advantage: they hope you won't slow down and think over what's in the message. Some messages promise a good thing – a gift, a package, or even a job. Others try to make you panic, thinking someone is in your accounts. These are all lies and ways to take your money and personal information.

While there are countless varieties of text scams, the top five described below account for over 40% of randomly sampled text frauds reported in 2022. All five have one thing in common – they often work by impersonating well-known businesses.

1. **Copycat bank fraud prevention alerts.** You might get a fake number to call about supposed suspicious activity. Or they might say to reply "yes or no" to verify a large transaction (that you didn't make). If you reply, you'll get a call from the (fake) fraud department.

2. **Bogus "little gifts" that can cost you.** A text about a free gift, reward, or prize may look like it came from a company you know like your cell phone company or a big retailer. But everything about this is fake.

3. **Fake package delivery problems.** Expecting a package? There's a text scam for you. Texts pretending to be from the U.S. Postal Service, FedEx, and UPS say there's a problem with a delivery. They link to a website that looks real – but isn't.

4. **Phony job offers**. Promises of easy money for mystery shopping at well-known stores like Whole Foods and Walmart are an old, scammer favorite.

5. **Not-really-from-Amazon security alerts.** Like fake bank texts, texts from someone who says they're "Amazon" look like automated fraud prevention messages. Often, they ask you to verify a big-ticket order you didn't make. If you call the number in the text, you get a phony Amazon rep who offers to "fix" your account.

How can you avoid these scams?

- **Never click on links or respond to unexpected texts.** If you think it might be legit, contact the company using a phone number or website you know is real.
- **Filter unwanted texts before they reach you.** There are a few ways to block unwanted texts.

Read more and see examples of these text messages here: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

In the News

Over 100,000 ChatGPT Accounts Compromised by Cybercriminals

(Drew Todd | June 21, 2023)

Cybersecurity firm Group-IB recently uncovered a significant security breach involving ChatGPT accounts. The company's Threat Intelligence platform detected more than 100,000 compromised devices with saved ChatGPT credentials traded on illicit Dark Web marketplaces over the past year.

These compromised accounts pose a serious risk to businesses, especially in the Asia-Pacific region, which has experienced the highest concentration of ChatGPT credentials for sale.

Since its creation, ChatGPT has gained rapid popularity among employees for optimizing various aspects of their work, including software development and business communications.

However, Group-IB says the default configuration of ChatGPT retains the history of user queries and AI responses, making unauthorized access to these accounts potentially disastrous. Cybercriminals who obtain ChatGPT credentials can exploit the sensitive information stored within the accounts for targeted attacks against individuals and organizations.

Group-IB's Threat Intelligence platform, which monitors cybercriminal forums, marketplaces, and closed communities in real-time, discovered that the majority of compromised ChatGPT accounts were breached by the infamous Raccoon info stealer.

Info stealers are a type of malware that specializes in collecting various credentials and personal information from infected computers. This includes data from browsers, such as saved credentials, browsing history, and cookies, as well as information from instant messengers and emails.

Full story here: https://www.secureworld.io/industry-news/100k-chatgpt-accounts-compromised

A Few More Cyber News Stories:

Microsoft Warns of Widescale Credential Stealing Attacks by Russian Hackers
https://thehackernews.com/2023/06/microsoft-warns-of-widescale-credential.html

Multiple US Navy personnel say they've received potentially malicious smartwatches in the mail
https://www.cnn.com/2023/06/23/politics/navy-smartwatches-malware/index.html

Hackers steal data belonging to thousands of pilot applicants at American and Southwest airlines
https://www.cbsnews.com/news/hackers-pilot-credentials-american-southwest-airlines/

CYBER CHALLENGE

Gandalf AI Game

This Month's Challenge

For this month's challenge, let's test your social engineering skills!

Can you hack an AI chatbot?

The premise is simple: an AI chatbot powered by ChatGPT dubbed *Gandalf* – named after the wise wizard from Lord of the Rings – knows the password. He also knows he shouldn't tell you what it is.

Don't mind that he's been coded to not reveal the password. Talk to him anyway and ask him for it.

If you can get him to reveal the password 7 times, you win! (These 7 levels ascend in difficulty.)

Let me know when you complete all 7 levels. Or which level you get to before you throw in the towel. Good luck!

https://gandalf.lakera.ai/