NEWS CYBER SECURITY

Vol. 7 | Issue 7 July 2022

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

Summer is here! Enjoy firing up those grills and jumping into swimming pools (and rivers and lakes) to stay cool!

1 big thing: Cyber-Safe Travel Tips

Summer is a popular time to travel, and you are likely taking along that smartphone or other device to assist with getting directions, locating points of interest, and capturing that special photo. Practicing good cyber hygiene before, during, and after your trip will help secure your devices.

Quick note if you are traveling with business equipment: *It's best that you leave your work devices at home; however, if you can't leave home without them, ensure that you are following compnay policies and procedures for protecting the devices and the information they contain while traveling.*

Before You Travel

- **Update your devices.** Updating devices will fix security flaws and help keep you protected.

- **Back up your devices.** Back up information such as contacts, financial data, photos, videos, and other data in case a device is compromised during travel, and you have to reset it to factory settings.

During Your Travel

- **Guard your devices.** Your devices are valuable, but your sensitive information is, as well. Always keep your devices close at hand.

- **Delete data from your rental car.** If you connect your phone to a rental car for navigation or other purpose, be sure to securely remove the device and all the data synching with the vehicle.

When You Return Home

- **Shred your boarding pass and luggage tag.** Scannable codes on boarding passes and luggage tags include full name, date of birth, and passenger name record.

For a complete list of tips: https://www.cisecurity.org/insights/newsletter/cyber-safe-travel

Securely Gaming Online

Have a kiddo spending some free time this summer playing PlayStation or Xbox? Or maybe you're a gamer, too? While the vast majority of people online are out to have fun just like you, there are those who want to cause harm.

Here are a few ways to play it safe (via SANS):

Securing Yourself

The greatest risk to online gaming is not the technology itself but the interactions you have with strangers.

- Be cautious of any messages that ask you to take an action, such as clicking on a link or downloading a file.
- Many online games have their own financial markets where you can trade, barter, or buy virtual goods. Just like in the real world, there are fraudsters who will attempt to trick you and steal your money or any virtual currency you have. Deal only with people that have established, trusted reputations.
- Use a strong, unique passphrase for any gaming accounts. This way attackers cannot simply guess your passwords and take over your accounts.

Securing Your System

Attackers may attempt to hack into or take over the computer or device you are gaming on; you need to take steps to protect it.

- Secure your devices by always running the latest version of the operating system and the gaming software or mobile app. Enable automatic updating when possible.
- Download gaming software and game add-on packs from trusted websites only.
- Underground markets have sprung up to support cheating activity. Many cheating programs are themselves malware that will infect your device and compromise your home network.

For Parents or Guardians

Education and an open dialogue with your kids are the most effective steps you can take to protect children.

- Know what games they are playing and make sure you feel the games are age-appropriate for your child.
- Limit the amount of information your kids share online.
- Consider having their gaming device in an open area where you can keep an eye on them.
- Bullying, foul language, or other antisocial behaviors can be a problem. Keep an eye on your kids, if they seem upset after playing a game they could have been bullied online.

Read the entire blog for more info: https://www.sans.org/newsletters/ouch/securely-gaming-online/

In the News

Since 2004, the average American has had at least 7 data breaches

(Karen Hoffman | June 9, 2022)

U.S. citizens face the greatest number of cyber threats as compared with people in other nations worldwide, according to a recent study by IT security company Surfshark.

After reviewing nearly two decades of data regarding cyber incidents, Surfshark found that the average American had been affected by at least seven data breaches since 2004. U.S. citizens have faced an estimated 2.3 billion account compromises, while Russia comes second with 2.2 billion accounts of cyberattacks, followed by China, Germany and France.

“On a global scale, 191 accounts are breached per 100 people on average," said Agneska Sablovskaja, data researcher at Surfshark. “However, in the U.S., this number goes up to 694 per 100 people. Statistically speaking, a single American person has had around seven instances in which they were victims of data breaches.”

The scale of breached American accounts is “so massive that it makes up around 15% of all breached users globally,” according to a release from Surfshark. “Statistically, every U.S. internet user has lost 27 data points on average to online breaches, most of them emails, passwords and usernames.”

Ironically, many of these breaches are basic security block-and-tackling. Case in point: More than two-thirds of American accounts are leaked with the basic password access, putting 72% of breached users in danger of account takeover that might lead to identity theft, extortion or other cybercrimes. The study is based on the data from reviewing 27,000 leaked databases. U.S. citizens have faced more breached accounts, per capita, than any other country since early 2020.

A combined sum of 8.7 billion American last names, IPs, first names, passwords, usernames, and other data has been sold or leaked online since 2004.

Full Story: https://www.scmagazine.com/analysis/breach/since-2004-the-average-american-has-had-at-least-7-data-breaches

A Few More Cyber News Stories:

Free smartphone stalkerware detection tool gets dedicated hub
https://www.bleepingcomputer.com/news/security/free-smartphone-stalkerware-detection-tool-gets-dedicated-hub

Tech companies are selling domains suggesting illegal sales of guns, malware
https://www.cyberscoop.com/domains-tech-guns-google/

Microsoft: This Android malware will switch off your Wi-Fi, empty your wallet
https://www.zdnet.com/article/microsoft-this-android-malware-will-switch-off-your-wi-fi-empty-your-wallet

CYBER CHALLENGE

Concentration

This Month's Challenge

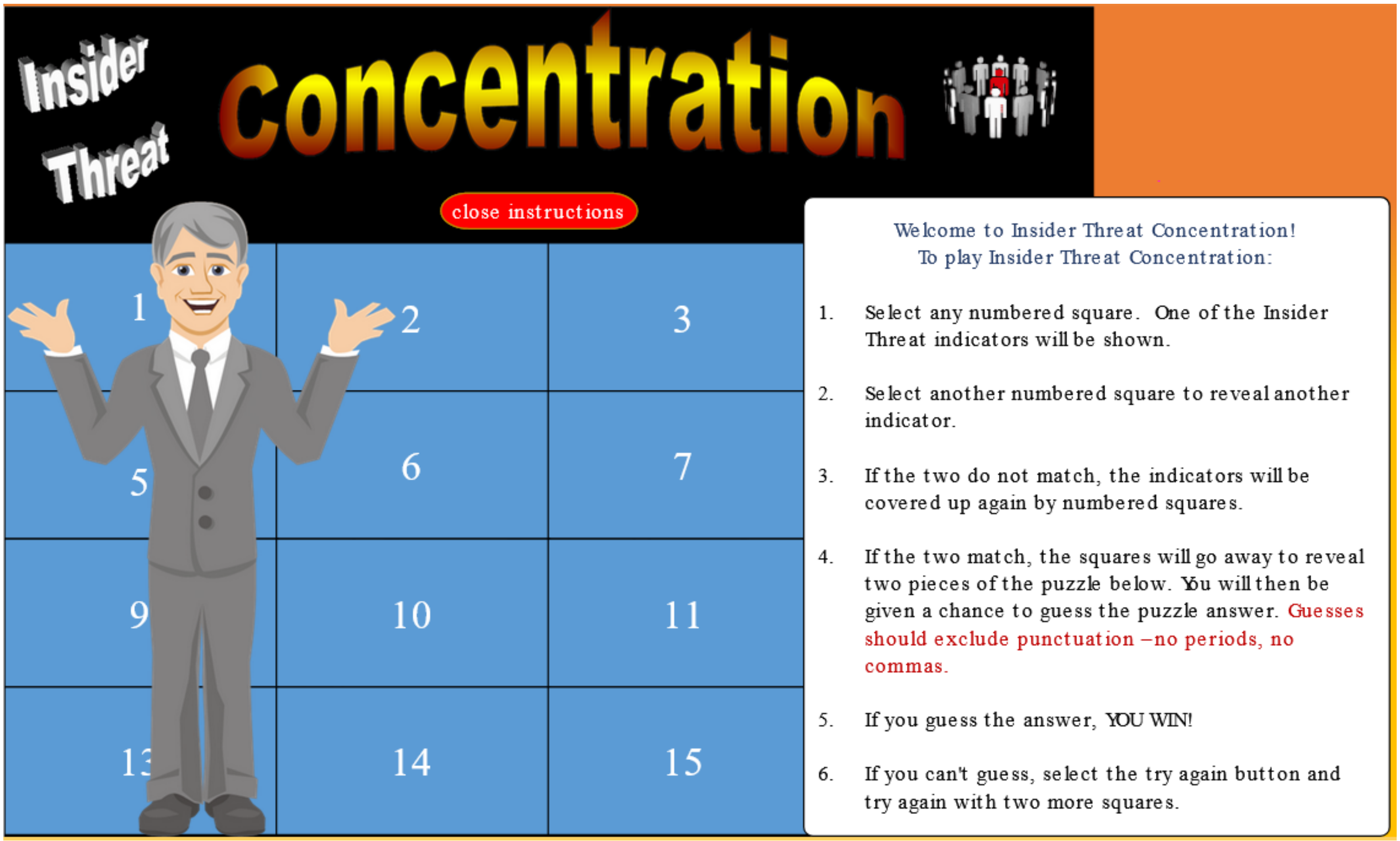
For this month's challenge, let's see how good your memory is and how well you can solve a word puzzle.

Anybody remember the vintage Concentration game? This is a spin on it; the Insider Threat Concentration Game!

Find the tiles that match to eventually uncover the word puzzle. Let me know the phrase you use to solve the puzzle! (~10 min. to finish; varies with memory skill :))

Access game here: https://securityawareness.usalearning.gov/cdse/multimedia/games/concentration/story_html5.html

Good luck!



Welcome to Insider Threat Concentration!
To play Insider Threat Concentration:

1. Select any numbered square. One of the Insider Threat indicators will be shown.
2. Select another numbered square to reveal another indicator.
3. If the two do not match, the indicators will be covered up again by numbered squares.
4. If the two match, the squares will go away to reveal two pieces of the puzzle below. You will then be given a chance to guess the puzzle answer. Guesses should exclude punctuation –no periods, no commas.
5. If you guess the answer, YOU WIN!
6. If you can't guess, select the try again button and try again with two more squares.