NEWS CYBER SECURITY

Vol. 8 | Issue 3

March 2023

| Page 2 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

Hopefully we've turned the corner into springtime, and the beautiful Texas weather provides some joy!

Malware, or malicious software, is a type of software that is designed to damage or disrupt computer systems. It can be spread through a variety of methods, including email attachments, infected websites, and social media. Once it infects a device, malware can be used to steal personal information, track user activity, or even take control of the device and can have a devastating impact on individuals and businesses.

Some of the most common types of malware include:

- **Viruses**. A virus is a type of malware that can replicate itself and spread to other computers. It can be used to delete files, steal personal information, or even take control of the infected computer.

- **Trojan Horses**. A Trojan horse is a type of malware that appears to be a legitimate software program but is actually malicious. It also can be used to steal personal information or allow hackers to gain access to the infected computer.

- **Ransomware**. Ransomware is a type of malware that encrypts files on the infected computer and demands payment in exchange for the decryption key. It can be extremely difficult to remove and can cause significant data loss as it spreads through a network.

Tips to help prevent malware infections:

- **Keep Your Software Up-to-Date**. One of the most effective ways to prevent malware infections is to keep your software up-to-date. Software updates often include security patches that address vulnerabilities that could be exploited by malware.

- **Use Antivirus Software**. Antivirus software can help to detect and remove malware infections. Be sure to keep your antivirus software up-to-date and perform regular scans.

- **Be Careful When Opening Email Attachments**. Email attachments can be a common way for malware to be spread. Be cautious when opening attachments from unknown senders.

- **Be Wary of Suspicious Websites**. Be careful when browsing the internet and avoid downloading software from untrusted sources.

Source: ChatGPT (Artificial Intelligence responding to a prompt, lightly edited)

In the News

Criminals Stole Thousands of Texans' Identities and Ordered Fraudulent Driver's Licenses

(Teresa Woodard | Feb. 27, 2023)

DALLAS — Texas.gov bills itself as the "official website of the state of Texas."

It was not hacked and did not suffer a breach.

But, it did fall victim to fraud.

Texas Department of Public Safety Chief Steve McCraw said an "Asian organized crime group" was able to find personal data belonging to thousands of Texans of Asian descent on the dark web.

McCraw said those criminals then used that data to create accounts on Texas.gov – where official driver's licenses can be renewed, or a replacement can be ordered.

DPS said it mailed at least 2,400 replacement driver's licenses to what it now believes are members of that organized crime group.

The group, according to DPS, could then sell those licenses to Chinese nationals who are illegally in the country and desperate to have some sort of valid identification.

During a hearing of the Texas House subcommittee on appropriations that is responsible for the agency's budget, DPS said it would begin notifying victims through letters this week.

The Texas attorney general's website has an entire page explaining what to do if your identity is stolen.

Full Story: https://www.wfaa.com/article/news/local/texas/texans-identities-stolen-fraudulent-drivers-licenses-heres-what-to-do-if-youre-a-victim/287-abec4d05-a63b-4bfd-8ec0-751a8e54f99c

A Few More Cyber News Stories:

'I want to destroy whatever I want': Bing's AI chatbot unsettles US reporter
https://www.theguardian.com/technology/2023/feb/17/i-want-to-destroy-whatever-i-want-bings-ai-chatbot-unsettles-us-reporter

White House: No More TikTok on Gov't Devices Within 30 Days
https://www.securityweek.com/white-house-no-more-tiktok-on-govt-devices-within-30-days

"Major" cyberattack compromised sensitive U.S. Marshals Service data
https://www.cbsnews.com/news/us-marshals-office-cyber-attack-compromised-sensitive-data

CYBER CHALLENGE

Pop Quiz

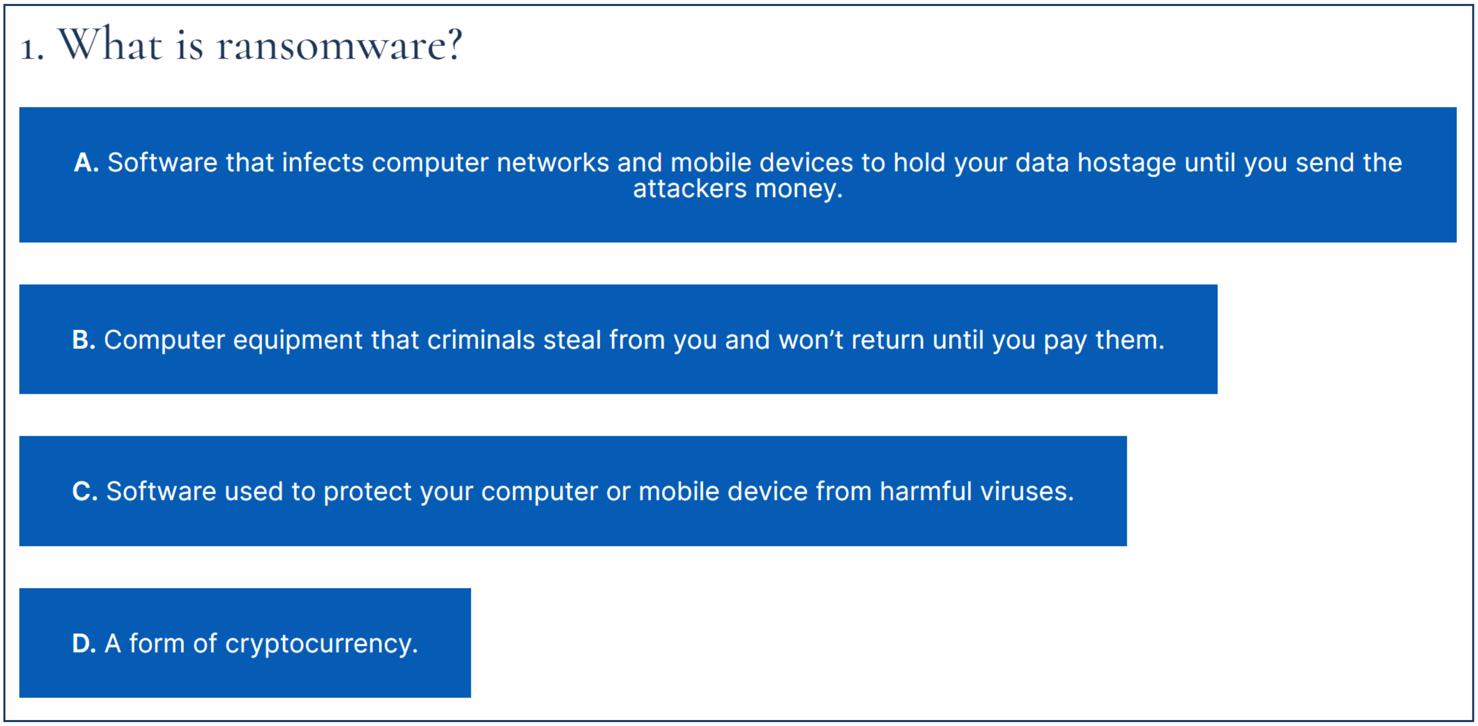
This Month’s Challenge

For this month’s challenge, we take a break from games (I know, I know, I like games, too) to take a little more focused look at ransomware.

Let’s see how much you know and how closely you’ve paid attention to that awareness training over the years!

This is a quick, 5-question quiz to test your knowledge on all things ransomware.
Let me know how you do. Good luck!

https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/ransomware



1. What is ransomware?

A. Software that infects computer networks and mobile devices to hold your data hostage until you send the attackers money.

B. Computer equipment that criminals steal from you and won’t return until you pay them.

C. Software used to protect your computer or mobile device from harmful viruses.

D. A form of cryptocurrency.