Vol. 9 | Issue 8

NEWS CYBER SECURITY

August 2024

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Prepare Your Kiddos for a Safe Return to School

What to know: As the new school year starts up, and with an increasing reliance on digital devices and online resources, it's essential for parents to prioritize their child's cyber safety.

Here are some key tips to help keep your child safe online.

- **Discuss online safety.** Have an open conversation with your child about the importance of online safety. Explain the risks of sharing personal information and the importance of using strong, unique passwords.
- **Monitor online activity.** Keep an eye on your child's online activity. Use parental controls and monitoring tools to set appropriate boundaries and track their internet usage.
- **Educate about phishing scams.** Teach your child to recognize phishing emails and messages. Explain that they should never click on links or download attachments from unknown sources and to always verify the sender's identity.
- **Set up privacy settings.** Review and adjust privacy settings on your child's devices, apps, and social media accounts. Limiting the amount of personal information they share online can help protect their privacy and prevent cyberbullying.
- **Encourage safe social media use.** Discuss the importance of responsible social media use. Advise your child to be cautious about who they interact with online and to avoid sharing sensitive information like their school's name or their location.
- **Report suspicious activity.** Teach your child to report any suspicious emails, messages, or online behavior to you or their school's IT department immediately. Early reporting can help prevent potential cyber threats.

More info and tips: https://www.cisa.gov/topics/physical-security/school-safety/school-safety-and-cybersecurity

Internet of Things

The Internet of Things (IoT) refers to the network of physical devices - such as home appliances, security systems, smart thermostats, and even wearable fitness trackers - that are connected to the internet and can communicate with each other. These devices collect and share data, making our lives more convenient and efficient. However, the convenience of IoT comes with potential cybersecurity risks that families need to be aware of.

Cyber awareness tips for a safe IoT-enabled home:

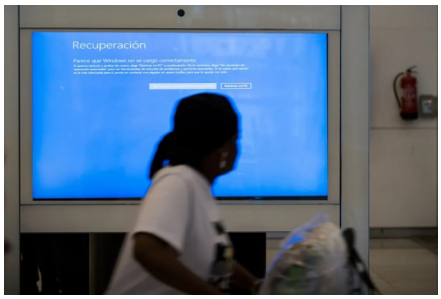
- **Change Default Passwords:** IoT devices often come with default usernames and passwords, which are easy targets for hackers. Change these immediately to strong, unique passwords for each device.
- **Secure Your Wi-Fi Network:** Your Wi-Fi network is the gateway to all your IoT devices. Make sure it is secure by using a strong password and encryption. Avoid using default passwords provided by your internet service provider.
- **Regularly Update Firmware:** Manufacturers release firmware updates to patch security vulnerabilities. Ensure that your IoT devices are set to update automatically or check for updates regularly to keep them secure.
- **Disable Unnecessary Features:** Many IoT devices come with features you may not use. Disable any unnecessary features to reduce potential entry points for hackers. For example, if you don't use remote access, turn it off.
- **Educate Your Family:** Ensure that all family members understand the importance of IoT security. Teach them to recognize suspicious activity and to follow best practices, like not sharing passwords.
- **Be Cautious with Voice Assistants:** Voice-activated assistants like Amazon Alexa or Google Home can be convenient but also pose privacy risks. Be mindful of the information you share with these devices and review their privacy settings.

While IoT devices offer great convenience and can enhance your home's functionality, they also require careful management to ensure your family's safety. Stay vigilant and make cybersecurity a family priority.

More on IoT: https://staysafeonline.org/resources/7-tips-for-a-safer-internet-of-things

In the News

US cyber agency CISA says malicious hackers are 'taking advantage' of CrowdStrike outage



(Zack Whittaker | July 19, 2024)

As much of the world slowly gets back online after an outage caused by cybersecurity giant CrowdStrike led to global travel and business gridlock, malicious actors are also trying to exploit the situation for their own gain.

U.S. cybersecurity agency Cybersecurity and Infrastructure Security Agency (CISA) said in a statement Friday that though the CrowdStrike outage was not linked to a cyberattack or malicious activity, it has "observed threat actors taking advantage of this incident for phishing and other malicious activity."

CISA warned individuals to "avoid clicking on phishing emails or suspicious links," which can lead to email compromise and other scams.

It's not uncommon for malicious actors to exploit chaotic situations to carry out cyberattacks, especially campaigns that can be easily created and customized at short notice, like email or text phishing.

One security researcher on X, formerly Twitter, said malicious actors were already sending phishing emails using a variety of domains that impersonate CrowdStrike. One of the emails posted falsely claimed it could "fix the CrowdStrike apocalypse" if the recipient paid a fee worth several hundred euros to a random crypto wallet.

In reality, the only working fixes are either to repeatedly restart affected computers in the hope that they stay on long enough for the newly fixed update to download and install, or manually remove the defective file from every bricked computer.

Full Story: https://techcrunch.com/2024/07/19/us-cyber-agency-cisa-says-malicious-hackers-are-taking-advantage-of-crowdstrike-outage/

A Few More Cyber News Stories:

North Korean Hackers Targeted Cybersecurity Firm KnowBe4 with Fake IT Worker
https://www.infosecurity-magazine.com/news/north-korean-hackers-targeted

The biggest data breaches in 2024: 1 billion stolen records and rising
https://techcrunch.com/2024/07/16/2024-in-data-breaches-1-billion-stolen-records-and-rising

Mandrake Spyware Infects 32,000 Devices Via Google Play Apps
https://www.infosecurity-magazine.com/news/mandrake-spyware-infects-32000

CYBER CHALLENGE

Spot the Phish: Kid's Edition

This Month's Challenge

For this month's challenge, let's see how well your kiddos can spot a phish!

This short module from KnowBe4 looks at the fundamentals of phishing - what it is, as well as what it looks like - and provides examples from scenarios to which your kids can relate.

Then, they'll have a chance to put their learning to the test! (Expected duration: 10 minutes)

Let me know if you share it with a youngster in your life; and bonus points for letting me know how they do! Good luck!

https://training.knowbe4.com/modstore/view/0654978b-22b8-4b91-808d-af71060a8692