NEWS
CYBER SECURITY
Vol. 9 | Issue 1
January 2024

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

Happy New Year!! Wishing each of you a great 2024!

One big thing: New Year, New Cybersecurity You: Five Resolutions for a Safer Online Life

What to know: As we step into the new year, it's the perfect time to reflect on our habits and make resolutions for a healthier and safer lifestyle...to include resolutions to protect ourselves and our families while online.

1. Strengthen Passwords: "I will create strong and unique passwords for all my accounts."

Start the year by revamping your passwords. Avoid using easily guessable information like birthdays or names. Consider using a reputable password manager to keep track of your complex passwords securely.

2. Enable Multi-Factor Authentication (MFA): "I will enable MFA wherever possible to add security."

Multi-Factor Authentication provides an additional level of protection beyond passwords. Whether it's your email, social media, or banking accounts, enable MFA to ensure that even if your password is compromised, unauthorized access remains difficult.

3. Stay Informed about Phishing: "I will educate myself on identifying and avoiding phishing attempts."

Learn to recognize phishing emails and messages by checking for suspicious links, email addresses, and unexpected requests.

4. Regularly Update Software/Apps: “I will keep my devices and applications up-to-date for better security."

Outdated software and apps can be vulnerable to cyber threats. Make it a habit to regularly check for updates on your operating system, antivirus software, and other applications. Set your devices to update automatically if possible to ensure you have the latest security patches.

5. Review Privacy Settings: "I will review/update my privacy settings on social media and other platforms."

Take control of your online privacy by reviewing and adjusting the settings on your social media accounts and other online platforms. Limit the amount of personal information visible to the public and only connect with people you trust.

The Dark Web

In the vast expanse of the internet, there exists a realm known as the "Dark Web." This elusive corner of cyberspace is often associated with mystery and intrigue.

What is the Dark Web?

The World Wide Web is made up of three main layers: the surface web, the deep web and the dark web. When you search the web, read news from a webpage or shop for sneakers online, you're most likely on the surface web. Many people are familiar with this part of the internet.

When you sign in to your email account, you head into the deep web. This part of the web stores information protected by passwords. Your email, bank account and online health records are all on the deep web.

The dark web is part of the deep web. And unlike the other layers of the web, the dark web can't be seen from normal web browsers. Users can only access the dark web using special tools or software (one example is The Onion Router, or "Tor" for short. And just as an onion has many layers, Tor has many levels of encryption). Dark web users are anonymous, and their activity and IP addresses aren't tracked.

What can be found on the Dark Web?

While its name may sound threatening, the dark web is used by some legitimate businesses and organizations. In fact, U.S. military researchers created dark web technology to send and receive messages anonymously.

Some journalists use the dark web to protect the identity of sources or whistleblowers. News organizations also use it to make journalism accessible in places where it's blocked.

Still, because users are anonymous, the dark web is also used as an online black market by criminals for illegal activities like selling stolen information.

According to the 2021 Dark Web Price Index, these are typical prices, in U.S. dollars, of a few goods and services sold on the dark web:

- Cloned credit card with PIN: $30
- Stolen online banking logins, minimum of $2k in account: $120
- Hacked Facebook account: $65
- Hacked Gmail account: $80
- Fake U.S. Green Card: $150
- USA voter database for various states: $100

Read more information and find basic tips on how to stay safe (ignore the sales pitch, please):
https://goodsuite.com/what-lives-on-the-dark-web-how-to-protect-yourself

In the News

Governments spying on Apple, Google users through push notifications - US senator

(Raphael Satter | December 6, 2023)

Unidentified governments are surveilling smartphone users via their apps' push notifications, a U.S. senator warned on Wednesday.

In a letter to the Department of Justice, Senator Ron Wyden said foreign officials were demanding the data from Alphabet's Google and Apple. Although details were sparse, the letter lays out yet another path by which governments can track smartphones.

Apps of all kinds rely on push notifications to alert smartphone users to incoming messages, breaking news, and other updates. These are the audible "dings" or visual indicators users get when they receive an email or their sports team wins a game. What users often do not realize is that almost all such notifications travel over Google and Apple's servers.

That gives the two companies unique insight into the traffic flowing from those apps to their users, and in turn puts them "in a unique position to facilitate government surveillance of how users are using particular apps," Wyden said. He asked the Department of Justice to "repeal or modify any policies" that hindered public discussions of push notification spying.

In a statement, Apple said that Wyden's letter gave them the opening they needed to share more details with the public about how governments monitored push notifications.

"In this case, the federal government prohibited us from sharing any information," the company said in a statement. "Now that this method has become public we are updating our transparency reporting to detail these kinds of requests." Google said that it shared Wyden's "commitment to keeping users informed about these requests." The Department of Justice declined to comment on the push notification surveillance or whether it had prevented Apple or Google from talking about it.

Full Story: https://www.reuters.com/technology/cybersecurity/governments-spying-apple-google-users-through-push-notifications-us-senator-2023-12-06/

A Few More Cyber News Stories:

Municipalities Face a Constant Battle as Ransomware Snowballs
https://www.darkreading.com/cybersecurity-operations/as-ransomware-attacks-abound-municipalities-face-a-constant-battle

Google's New Tracking Protection in Chrome Blocks Third-Party Cookies
https://thehackernews.com/2023/12/googles-new-tracking-protection-in.html

The Anatomy of a Scam: 'Like YouTube Videos and Get Paid' Schemes
https://www.bitdefender.com/blog/labs/the-anatomy-of-a-scam-like-youtube-videos-and-get-paid-schemes

CYBER CHALLENGE

Helpful Awareness Sites

This Month's Challenge

For this month's challenge, let's get really practical.

Take a few minutes to visit each of these sites, then bookmark them. Each of these provide insight and awareness for all things cybersecurity.

https://www.cisa.gov/secure-our-world

https://staysafeonline.org

https://reportfraud.ftc.gov

https://www.cisa.gov/topics/cybersecurity-best-practices

Now, pledge to read these a few times a quarter (scout's honor!) to stay fresh on cyber awareness and protect your family all year.

Then send me a screenshot of these in your Bookmarks. Include a few sentences describing something new you learned from each site.

You got this!