Vol. 7 | Issue 12

CYBER SECURITY NEWS

December 2022

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

Happy holidays! Fully aware this season isn't joyful for everybody, we hope each of you are able to find a reason to smile this holiday season.

1 big thing: Shop smart and stay safe this holiday season

What to know: 'Tis the season for holiday gifts and shopping! Scammers are well-aware many of us choose to shop online to avoid waiting in lines and sitting in traffic. Be vigilant and avoid falling into their traps.

Follow these tips to help reduce the likelihood of your information falling into the wrong hands:

- **Avoid Using Public Wi-Fi.** While using public Wi-Fi is convenient, it does not protect your private data.
- **Check Shopping Sites.** Browse sites that are well-known and legitimate. It's best to navigate directly to the site using a browser as opposed to clicking a link.
- **Resist the Urge to Click.** Speaking of clicking a link, slow down before you do. Be cautious with offers that look too good to be true. These may be traps.
- **Be Wary of Emails.** This is a scammer's favorite way to stir emotion and set the bait.
- **Strengthen Passwords.** Use strong passwords. This is one of the most secure ways to protect yourself. Use paraphrases that make sense to you and are only known to you.
- **Monitor Your Credit Cards.** Verify your transactions are valid. If something looks suspicious, reach out to the customer service departments of the credit card companies.

Fore more tips and resources: https://www.cisecurity.org/insights/newsletter/shop-smart-and-stay-safe-this-holiday-season

Browsers

Browsers such as Apple Safari, Mozilla Firefox, Google Chrome, or Microsoft Edge are one of the most common ways people interact with the Internet. We use them for reading the news, checking email, shopping online, watching videos, and playing games. As a result, browsers are yet another target for cyber attackers.

Many people assume browsing online is safe if you only visit well-known, trusted websites. However, it is quite easy to accidentally click on or visit an unsafe web page, sometimes without even knowing it. In addition, the very websites you know and trust can be hacked, with cyber attackers installing malicious software on them.

Finally, today's browsers have many new features, which often can be confusing, and if misconfigured, expose you to even more dangers.

Here are key steps to protecting yourself:

- **Updating**: Always use the latest version of your browser. Updated browsers have the latest security patches and are much more secure.
- **Warnings**: Today's browsers can often recognize certain malicious websites designed to cause you harm. If your browser warns you that the website you are about to visit is dangerous, close your browser tab and find what you need on a different website.
- **Syncing**: Don't sync your work browser with your personal browser or any personal accounts. *Syncing* is when you enable browsers on different devices to talk to each other and share your browsing information.
- **Passwords**: Many browsers support the option of saving your passwords to different sites. Instead of storing your passwords in your browser, we recommend you use a dedicated password manager.
- **Plug-ins**: Plug-ins or extensions are small pieces of software added to browsers that can add functionality. However, each new plug-in you add can also add more vulnerabilities. For your work computer, only add plug-ins that are authorized and approved, and just like your browser, keep them updated.
- **Log Off:** When you are finished visiting a website, be sure to log off to remove sensitive login and password information before closing the browser.

Source: https://www.sans.org/newsletters/ouch/browsers

In the News

WhatsApp data leak: 500 million user records for sale online

(Jurgita Lapienyte | November 28, 2022)

Someone is allegedly selling up-to-date mobile phone numbers of nearly 500 million WhatsApp users. A data sample investigated by Cybernews likely confirms this to be true.

On November 16, an actor posted an ad on a well-known hacking community forum, claiming they were selling a 2022 database of 487 million WhatsApp user mobile numbers.

The dataset allegedly contains WhatsApp user data from 84 countries. Threat actor claims there are over 32 million US user records included.

Another huge chunk of phone numbers belongs to the citizens of Egypt (45 million), Italy (35 million), Saudi Arabia (29 million), France (20 million), and Turkey (20 million).

The dataset for sale also allegedly has nearly 10 million Russian and over 11 million UK citizens' phone numbers.

The threat actor told Cybernews they were selling the US dataset for $7,000, the UK – $2,500, and Germany – $2,000.

Such information is mostly used by attackers for smishing and vishing attacks, so we recommend users to remain wary of any calls from unknown numbers, unsolicited calls and messages.

WhatsApp is reported to have more than two billion monthly active users globally.

Upon request, the seller of WhatsApp's database shared a sample of data with Cybernews researchers. There were 1097 UK and 817 US user numbers in the shared sample.

Cybernews investigated all the numbers included in the sample and managed to confirm that all of them are, in fact, WhatsApp users.

A Few More Cyber News Stories:

Meta Reportedly Fires Dozens of Employees for Hijacking Users' Facebook and Instagram Accounts
https://thehackernews.com/2022/11/meta-reportedly-fires-dozens-of.html

Credential Stuffers Steal $300K from DraftKings Customers
https://www.infosecurity-magazine.com/news/credential-stuffers-300k

US offshore oil and gas installation at 'increasing' risk of cyberattack
https://www.theregister.com/2022/11/21/us_oil_gas_cyber_threats

CYBER CHALLENGE

Spot the Signs

This Month's Challenge

For this month's challenge, let's take a look at several popular scams and see if we can spot all the signs that should tip us off to the trickery.

The website also includes the answers (no cheating!) so do the best you can to take a mental note of what you think the red flags are and then check your work with the answer sheet.

Let me know how you do and if you have any questions on them.

Can't wait to hear that you spotted them all! (Completion Time: 20 min)

https://www.scamwatch.gov.au/about-scamwatch/tools-resources/online-resources/spot-the-scam-signs

Dachshund Puppy for Sale

$500

Tas, Australia.

Male pup. 8 weeks old.

Ready to go to a good home. These puppies are usually sold for at least $3,000. I already have 3 puppies so unfortunately cannot keep this little guy.

Reputable breeder located in Tas, Australia.

You'll need to pay me directly and I'll arrange for the puppy to be vaccinated, insured and transported to your preferred location.

Payment by money order or wire transfer.