Vol. 9 | Issue 11

NEWS CYBER SECURITY

November 2024

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Keep Fighting the Phish

We know, we know—phishing is one of those topics that comes up again and again. But here's the thing: phishing is one of the most common, persistent threats out there, and the scammers aren't slowing down.

Every day, we see new and increasingly clever phishing attempts aimed at tricking even the savviest among us. That's why it's crucial to keep revisiting the topic and sharpening our defenses.

Here's a quick refresher on how to *fight the phish*:

1. **Double-check the sender**: Look closely at email addresses, especially if they're asking you to click a link or provide personal info.
2. **Verify unexpected requests**: If you receive an urgent message from a colleague or vendor, take a moment to call them or use a known contact number to confirm it's real.
3. **Stay cautious with links and attachments**: Hover over links before clicking, and be cautious with attachments from unknown sources.

Phishing scams evolve constantly, so it's worth taking a little extra time to double-check even familiar emails. Let's stay vigilant!

In the News

UnitedHealth says data of 100 million stolen in Change Healthcare breach

(Lawrence Abrams | October 24, 2024)

UnitedHealth has confirmed for the first time that over 100 million people had their personal information and healthcare data stolen in the Change Healthcare ransomware attack, marking this as the largest healthcare data breach in recent years.

In May, UnitedHealth CEO Andrew Witty warned during a congressional hearing that "maybe a third" of all American's health data was exposed in the attack.

A month later, Change Healthcare published a data breach notification warning that the February ransomware attack on Change Healthcare exposed a "substantial quantity of data" for a "substantial proportion of people in America."

Today, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) data breach portal updated the total number of impacted people to 100 million, making it the first time UnitedHealth, the parent company of Change Healthcare, put an official number to the breach.

"On October 22, 2024, Change Healthcare notified OCR that approximately 100 million individual notices have been sent regarding this breach," reads an updated FAQ on the OCR website.

Full Story: https://www.bleepingcomputer.com/news/security/unitedhealth-says-data-of-100-million-stolen-in-change-healthcare-breach

A Few More Cyber News Stories:

New Type of Job Scam Targets Financially Vulnerable Populations
https://www.infosecurity-magazine.com/news/job-scam-targets-financially

Fitness App Strava Gives Away Location of Biden, Trump and other Leaders, French Newspaper Says
https://www.securityweek.com/fitness-app-strava-gives-away-location-of-biden-trump-and-other-leaders-french-newspaper-says

Mozilla: ChatGPT Can Be Manipulated Using Hex Code
https://www.darkreading.com/application-security/chatgpt-manipulated-hex-code

CYBER CHALLENGE

Spot the Phish!

This Month's Challenge

For this month's challenge, let's continue to practice spotting phishing emails. The more we practice, the better we'll be when the real deal hits our inboxes!

You'll have 10 emails/text messages to look at and decide whether or not they are legit or a phish.

I actually missed a few...so let's see if you do better than me!

Let me know how you do. Good luck!

https://phishingquiz.withgoogle.com