Welcome to the TXDPS Cyber Security Newsletter

One big thing: October is here – and so is Cybersecurity Awareness Month!

What to know: Now is the perfect time to focus on simple ways we can protect ourselves and our personal information from the growing number of cyber threats.

Before you think this is only for the tech gurus, think again! Cybersecurity touches every part of our daily lives, whether we're shopping online, scrolling through social media, or checking emails.

Throughout the month, we'll be sharing tips that show how easy it can be to stay secure online. From spotting phishing emails to creating strong passwords (hint: "password123" won't cut it), you'll learn how to protect your information without turning your life upside down. It's not just about staying safe at work–it's about being mindful of your online habits at home, with your family, and even on your phone.

"Cybersecurity" may sound technical, but it's really about protecting what matters to you most–your identity, your privacy, and your peace of mind.

So stick around this month and keep an eye on our social media for some tips and simple actions that can make a big difference! After all, staying safe online is something we can all do, one step at a time.

More on Cybersecurity Awareness Month:
https://www.cisa.gov/cybersecurity-awareness-month
https://staysafeonline.org/programs/cybersecurity-awareness-month

In the News

One-third of the US population's background info is now public

(Paulina Okunytė | September 25, 2024)

Cybernews exclusive research has revealed that a massive data leak at MC2 Data, a background check firm, affects a staggering amount of US citizens.

MC2 Data and similar companies run public records and background check services. These services gather, compile, and analyze data from a wide range of public sources, including criminal records, employment history, family data, and contact details.

They use this information to create comprehensive profiles that employers, landlords, and others rely on for decision-making and risk management.

Despite dealing with staggering amounts of sensitive data, it is not always kept secure. On August 7th, the Cybernews research team uncovered that the company left a database with 2.2TB of people's data passwordless and easily accessible to anyone on the internet.

What was likely a human error exposed 106,316,633 records containing private information about US citizens, raising serious concerns about privacy and safety. Estimates suggest that at least 100 million individuals were affected by this massive data leak.

People and organizations needing background checks have also been exposed, as the data of 2,319,873 users who subscribed to MC2 Data services was leaked.

Leaked data included: names, emails, partial payment information, home addresses, phone numbers, property records, legal records, relatives/neighbors data, employment history and more.

Full Story: https://cybernews.com/security/us-mc2-background-check-data-leak

A Few More Cyber News Stories:

AT&T pays $13 million FCC settlement over 2023 data breach
https://www.bleepingcomputer.com/news/security/atandt-pays-13-million-fcc-settlement-over-2023-data-breach

Ransomware incidents rose 73% globally in 2023
https://statescoop.com/ransomware-incidents-rose-73-globally-in-2023-report-shows

CISA: Hackers target industrial systems using "unsophisticated methods"
https://www.bleepingcomputer.com/news/security/cisa-hackers-target-industrial-systems-using-unsophisticated-methods

Safe Web Surfing

This Month's Challenge

For this month's challenge, let's practice looking at URLs and learn a little about how a link to a website is broken down.

You can choose your level of difficulty. The questions don't get harder, there's just more of them.

I recommend going "Extreme" and seeing if you can snag all 2000 points!

Good luck! Let me know how you do. (approx. time to complete: 10 min.)

https://training.knowbe4.com/modstore/view/9b18c7c2-88bb-45f3-840e-0973fb598b1d

Safe Web Surfing Game