Vol. 9 | Issue 9

CYBER SECURITY NEWS

September 2024

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: It's Time for Football and Fall Festivals!

What to know: Soon, the unrelenting heat will give way to nice, crisp air and will be the perfect opportunity to gather with friends and family in sports stadiums or concert venues. It's also a prime time for scammers to target unsuspecting event-goers.

Stay Secure While Buying Tickets Online
Fraudulent websites and ticket scams are more common than you might think.

- **Buy from official sources.** Whenever possible, purchase tickets directly from the team's website, the concert venue, or well-known platforms.
- **Avoid public Wi-Fi.** If you must buy tickets while out and about, use your mobile data or wait until you're on a secure home network.

Watch Out for Scams Related to Sports Events and Concerts
Beyond fake tickets, scammers use the excitement of sports events and concerts to trick us.

- **Be mindful of fake messages.** You might receive a message claiming you've won free tickets or asking you to confirm a purchase you didn't make. These are often phishing attempts designed to steal your information.
- **Spot social media scams.** Fraudsters often create fake accounts or posts offering discounted or last-minute tickets for sports events or concerts. Before interacting, check the profile's legitimacy.

Safeguard Your Personal Info at Public Venues
,Your focus should be on enjoying the experience—not worrying about your personal information.

- **Use mobile payments.** Instead of pulling out your credit card at every concession stand, consider using mobile payment options like Apple Pay or Google Wallet.
- **Protect your devices.** Crowded venues, whether for sports or concerts, are prime spots for pickpockets. Keep your phone and wallet secure.

Cybersecurity Culture

"Cybersecurity" not just about having the latest software or the strongest passwords—it's about creating a culture where everyone takes ownership of keeping our digital environment safe. A strong cybersecurity culture means that each of us understands that we play a crucial role in protecting both our personal and agency data.

Why Cybersecurity Matters

Every day, we interact with technology that could be a target for cybercriminals. Whether it's protecting sensitive information at work or keeping your personal details secure at home, strong cybersecurity practices help prevent data breaches, identity theft, and other costly issues. By being mindful of cybersecurity, we can protect not just ourselves, but also our colleagues, the agency, and all the Texas residents we aim to keep safe.

Taking Ownership: Cybersecurity Is Everyone's Responsibility

A good cybersecurity culture is built on the idea that everyone has a part to play. It's not enough to rely on others to keep things secure; each of us needs to take ownership of our actions.

This means:

- **Staying aware** of potential threats like phishing emails or suspicious links.
- **Following best practices** for password management and device security.
- **Keeping informed** about the latest security guidelines and updates.

A Simple Example: Reporting Suspicious Activity

One of the easiest ways you can help strengthen our cybersecurity culture is by reporting suspicious activity. For example, if you receive an unexpected email asking for sensitive information or notice something odd on your computer, don't ignore it; report it.

Also, if you happen to click a link you know you probably shouldn't have or learn later the email was fraudulent, please report it right away. It's natural tendency to stay quiet and hope nothing happened, but that only introduces risk into our agency.

By taking responsibility for our own cybersecurity, we contribute to a safer environment for everyone. This is true for your families at home, as well. Maybe even more so.

Key Takeaways

- Cybersecurity is everyone's responsibility.
- Take ownership by staying aware and following best practices.
- Always report suspicious activity—it could prevent a major breach.

In the News

McDonald's Instagram Hack: Crypto Scammers Claim to Steal $700,000

(Krishna Murthy | August 23, 2024)

Fast-food giant McDonald's Instagram account was hacked on Thursday, which cost fans dearly. The McDonald's Instagram hack was orchestrated on August 22, 2024, when crypto scammers exploited the platform to promote a fraudulent crypto scheme named "GRIMACE", McDonald's iconic purple mascot. The hackers claimed to have netted $700,000 after the hack.

The hackers used the hijacked Instagram account to post deceptive messages claiming the company was distributing free cryptocurrency. This tactic, known as social engineering, preys on unsuspecting users by exploiting brand trust and the allure of a quick financial windfall.

The fraudulent messages included links to malicious websites designed to steal personal and financial information, or trick users into investing in the fictitious GRIMACE coin.

While the full extent of the damage remains unclear, McDonald's has acknowledged the incident and confirmed they have regained control of their Instagram account. In a statement to the New York Post, the company said, "We are aware of an isolated incident that impacted our social media accounts earlier today. We have resolved the issue on those accounts and apologize to our fans for any offensive language posted during that time."

However, the incident raises serious questions about social media security and the vulnerability of even major corporations to cyberattacks.

Full Story: https://thecyberexpress.com/mcdonalds-instagram-hack-crypto-steal-700k

A Few More Cyber News Stories:

PSA: These 'Microsoft Support' ploys may just fool you
https://www.malwarebytes.com/blog/scams/2024/08/psa-these-microsoft-support-ploys-may-just-fool-you

Ecovacs home robots can be hacked to spy on their owners, researchers say
https://techcrunch.com/2024/08/09/ecovacs-home-robots-can-be-hacked-to-spy-on-their-owners-researchers-say

Audit finds notable security gaps in FBI's storage media management
https://www.bleepingcomputer.com/news/security/audit-finds-notable-security-gaps-in-fbis-storage-media-management

CYBER CHALLENGE

Spot the Scam

This Month's Challenge

For this month's challenge, let's see how well you can avoid these common scams we come across while using our smartphones.

There are 7 scenarios presented. You choose whether you think it is a Scam or Not a Scam.

Try to ace this. I think you got it!

(There's also really good info after each correct/incorrect answer so please read up.)

Let me know how you do. Good luck!

https://www.washingtonpost.com/technology/interactive/2023/identify-scam-quiz-zelle-email-text