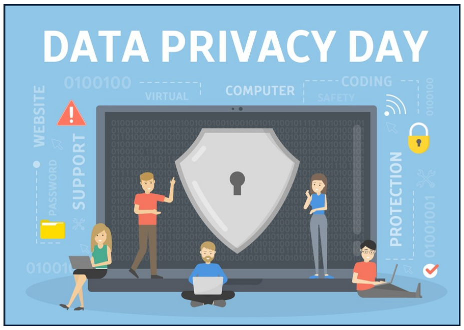
NEWS
CYBER SECURITY
Vol. 9 | Issue 2
February 2024

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Let's celebrate Data Privacy Day!



What to know: Data Privacy Day is on January 28th each year. But, we can still have a belated celebration because it's *that* important! In fact, the National Cybersecurity Alliance dedicates an entire week to data privacy.

Data privacy is focused on the use and governance of personal data to ensure that consumers' personal information is being collected, shared and used in appropriate ways. And, Data Privacy Day serves as an annual call to arms for employers and employees alike to fortify our defenses against potential data breaches and unauthorized access.

A few tips to help us do just that:

1. **Follow Security Procedures.** Adhere to organizational policies and procedures; understand and implement best practices for data protection outlined by the organization.

2. **Secure Password Practices.** Use strong, unique passwords for all accounts and systems. Regularly update passwords and avoid using easily guessable information. Enable two-factor authentication whenever possible.

3. **Limit Access.** Only access data that is necessary for your role. Avoid unnecessary data access and permissions. Be vigilant about sharing sensitive information and grant access only to authorized personnel.

4. **Encrypt Communications.** Ensure emails containing sensitive data to external entities is encrypted.

5. **Use Secure Networks.** Use VPN when accessing bisiness data remotely. Avoid using public Wi-Fi for sensitive work-related tasks.

6. **Physical Security Measures.** Be mindful of physical security. Lock your workstation when not in use, and be aware of your surroundings to prevent unauthorized access to sensitive areas.

7. **Report Security Incidents.** Report any suspicious activity or security incidents promptly. If you notice unusual behavior, unauthorized access, or any potential security threat, inform the IT Service Desk immediately.

Go Deeper: https://www.proofpoint.com/us/threat-reference/data-privacy

Quishing (QR Code Phishing)

Most of us have seen QR codes in the wild. They are those square barcodes we can scan with a smartphone to be directed to a website or other resource provided by the encoded URL. They've become significantly more popular for legitimate use in commercial and public spaces, and the combination of popularity and convenience has led to our general trust in them.

QR code phishing (quishing, for short) is a tactic where cybercriminals create deceptive QR codes to lead us to malicious websites or trick us into sharing sensitive information. It's a form of digital deception that exploits the trust we place in those convenient, black and white squares. And they are difficult to know they are malicious just by looking at them.

Though "quishing" may be a new word to lots of us (just me?), it's been a successful attack method for quite a while.

Malicious actors are likely to increase the use of this phishing method in the upcoming 2024 election cycle. The heightened interest and emotion invoked by the current political landscape, plus the convenience of scanning a QR code, creates the perfect environment for scammers to take advantage of the opportunity.

Stay safe with these tips:

1. **Verify the Source**. Before scanning any QR code, verify its source. Be cautious of codes received in unsolicited messages, emails, or on unfamiliar websites. Stick to trusted sources to minimize risks.

2. **Use Reputable QR Code Scanners**. Choose well-reviewed QR code scanner apps from legitimate app stores. These apps often come with built-in security features to detect and warn against potential phishing threats.

3. **Check the URL**. After scanning a QR code, examine the URL of the website it directs you to. If the URL seems suspicious, doesn't match expectations, or appears out of place, close the site immediately.

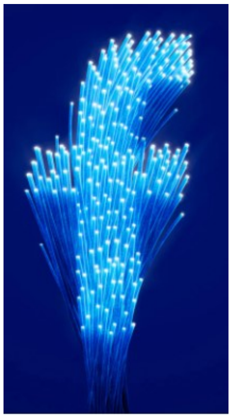
4. **Be Wary of Information Requests**. Legitimate QR codes should never request sensitive information like passwords, credit card details, or personal identifiers. Treat any such request as a potential red flag for phishing.

5. **Report Suspicious QR Codes**. If you come across a QR code that raises suspicions, report it to the relevant authorities or the platform where you found it. Your report could help prevent others from falling victim to the same cyber threats.

Read more: https://www.isaca.org/resources/news-and-trends/industry-news/2023/quishing-the-invisible-threat-in-qr-code-technology

In the News

Watch out for "I can't believe he is gone" Facebook phishing posts



(Lawrence Abrams | January 21, 2024)

A widespread Facebook phishing campaign stating, "I can't believe he is gone. I'm gonna miss him so much," leads unsuspecting users to a website that steals your Facebook credentials.

This phishing attack is ongoing and widely spread on Facebook through friend's hacked accounts, as the threat actors build a massive army of stolen accounts for use in further scams on the social media platform

As the posts come from your friends' hacked accounts, they look more convincing and trustworthy, leading many to fall for the scam.

The phishing campaign started around a year ago, with Facebook having trouble blocking the posts as they continue to this day. However, when new posts are created and reported, Facebook deactivates the Facebook.com redirect link in the post so that they no longer work.

The Facebook phishing posts come in two forms, with one simply stating, "I can't believe he is gone. I'm gonna miss him so much," and containing a Facebook redirect link. The other uses the same text but shows what appears to be a BBC News video of a car accident or other crime scene.

When BleepingComputer tested the links in the phishing posts, they brought us to different sites depending on the type of device you are using.

Clicking on the link from the Facebook app on a mobile device will bring visitors to a fake news site called 'NewsAmericaVideos' that prompts them to enter their Facebook credentials to confirm their identity and watch the video.

Full Story: https://www.bleepingcomputer.com/news/security/watch-out-for-i-cant-believe-he-is-gone-facebook-phishing-posts

A Few More Cyber News Stories:

Fake Biden robocall 'tip of the iceberg' for AI election misinformation
https://thehill.com/policy/technology/4424803-fake-biden-robocall-tip-of-the-iceberg-for-ai-election-misinformation

Mother of all breaches reveals 26 billion records: what we know so far
https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches

Jason's Deli says customer data exposed in credential stuffing attack
https://www.bleepingcomputer.com/news/security/jasons-deli-says-customer-data-exposed-in-credential-stuffing-attack

CYBER CHALLENGE

Data Protection IQ Test

This Month's Challenge

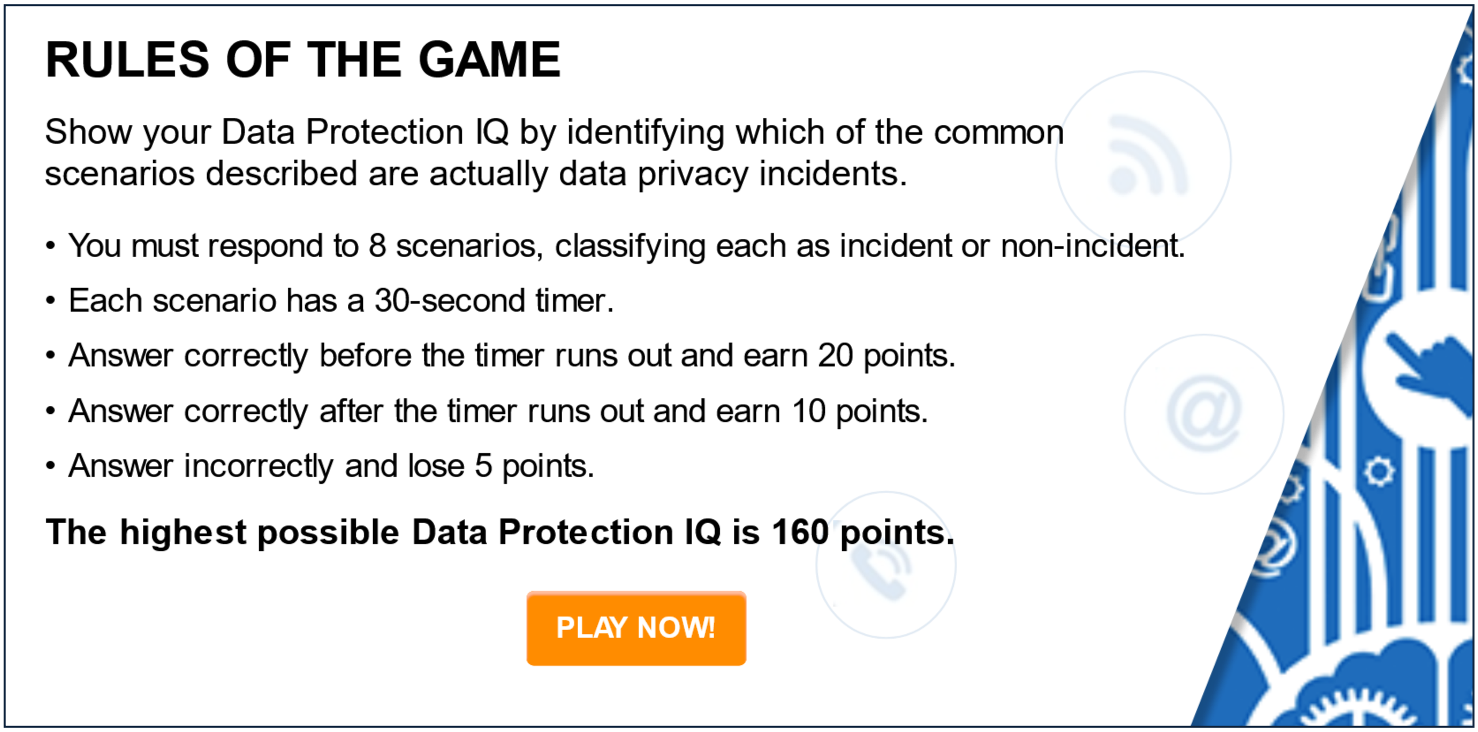
For this month's challenge, let's continue thinking about data privacy.

Here's your chance to see how easily you can identify a privacy incident.

Take a look at the rules of the game (below) and get started when you feel ready.

Let me know how you do by sharing your score!

https://globallearningsystems.com/free-data-privacy-kit/data-protection-iq-game



RULES OF THE GAME

Show your Data Protection IQ by identifying which of the common scenarios described are actually data privacy incidents.

- You must respond to 8 scenarios, classifying each as incident or non-incident.
- Each scenario has a 30-second timer.
- Answer correctly before the timer runs out and earn 20 points.
- Answer correctly after the timer runs out and earn 10 points.
- Answer incorrectly and lose 5 points.

The highest possible Data Protection IQ is 160 points.