Vol. 8 | Issue 12

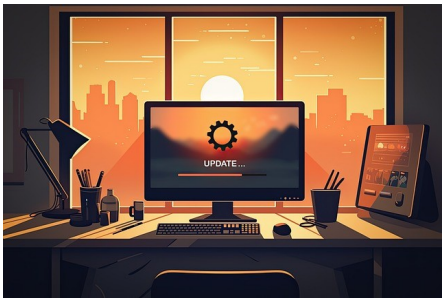
CYBER SECURITY NEWS

December 2023

Welcome to the TXDPS Cyber Security Newsletter

'Tis the season! We hope this newsletter finds you well as Christmas and the New Year approach.

One big thing: safeguard your holiday season by updating your devices!



Software updates are not just about adding new features; they are a frontline defense against cyber threats. Developers continuously identify and patch vulnerabilities in their software to protect users from potential security breaches. Ignoring updates leaves your devices exposed to cybercriminals who exploit these vulnerabilities. And, during the holiday season, cyber threats tend to rise as malicious actors take advantage of increased online activity.

Here are some holiday cyber threats and how regular software updates can help thwart them:

Phishing Scams: Cybercriminals often ramp up phishing attacks during the holidays, using enticing offers or fake charity appeals. Updated software, especially email clients and browsers, can help detect and block phishing attempts.

Online Shopping Risks: With the surge in online shopping, hackers target personal and financial information. Up-to-date antivirus programs and secure browsers can provide an additional layer of protection against malware designed to steal your sensitive data.

Unsecured Wi-Fi Networks: Public Wi-Fi spots are convenient but can be a breeding ground for cyber threats. Ensure your device's operating system and security applications are updated to mitigate the risks associated with connecting to unsecured networks. (Consider avoiding public Wi-Fi.)

Outdated Applications: Apps on your smartphone and computer should be regularly updated, as outdated applications may have unpatched vulnerabilities. These vulnerabilities can be exploited by cybercriminals to gain unauthorized access to your device.

This holiday season, make a cybersecurity checklist a part of your preparations. Ensure that all your devices, including smartphones, tablets, computers, and even smart home devices have the latest software updates installed. Stay safe, stay updated, and enjoy a worry-free holiday season!

In the News

Dallas County IT experts warned of data vulnerabilities months before ransomware attack

(Marina Trahan Martinez | November 21, 2023)

A Dallas County committee that oversees computer safety and the county's IT department sounded alarms months before a recent ransomware attack.

Dallas County was the target of what officials described as a "cybersecurity incident" on Oct. 19. Officials are still working to determine the scope of the attack. Kroll, a cybersecurity firm and longtime county vendor, is investigating the recent data attack.

Among county system security concerns raised at September and October meetings of the IT Executive Governance Committee were password, public network, data and document disposal and reCAPTCHA weaknesses.

The IT department's 2024 budget is over $70 million – up from last year's nearly $58 million. IT maintenance and subscriptions cost more than $14.5 million in the 2023 budget.

The IT department got money for more contract workers to handle employee help requests, fix system problems and safeguard against potential threats – including viruses and virtual attacks.

The county's top IT official told the committee that would help a lot.

"I have the resources I need now, building the muscle we need to deal with any potential incidents that are coming our way," Collins Dibaki, Chief Information Security Officer for Dallas County told the IT committee in September...

Full Story: https://www.keranews.org/news/2023-11-21/dallas-county-it-experts-warned-of-data-vulnerabilities-months-before-ransomware-attack

A Few More Cyber News Stories:

MOVEit victim count latest: 2.6K+ orgs hit, 77M+ people's data stolen
https://www.theregister.com/2023/11/20/moveit_victim_77m_medical

Morgan Stanley Fined $6.5 Million for Exposing Customer Information
https://www.securityweek.com/morgan-stanley-ordered-to-pay-6-5-million-for-exposing-customer-information

Detailed data on employees of U.S. national security lab leak online
https://cyberscoop.com/idaho-national-laboratory-siegedsec

CYBER CHALLENGE

Phishing IQ Test

This Month's Challenge

For this month's challenge, let's see if you can identify what is a real email or a phishing email.

You will be presented with 10 random visual phishing questions. Take a close look at the email you're shown and then select whether you believe it is a "phishing" email or a "legitimate" email.
(5-15 minutes test time)

Let me know how you do! Hoping to see lots of 10/10s … but any result means you're practicing; and that's just as good. You got this!

https://www.phishingbox.com/phishing-iq-test/quiz.php