Vol. 9 | Issue 4

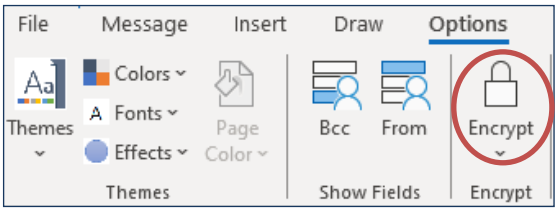
NEWS CYBER SECURITY

April 2024

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Please Encrypt Email When Sharing Sensitive Information Externally



What to know: When emailing sensitive information to outside parties, you should be encrypting those email messages to protect the data within them. Encrypting an email message means readable plain text is scrambled into gibberish that only the intended recipient can unscramble with the right key. Sending them unencrypted leaves them vulnerable to unauthorized access.

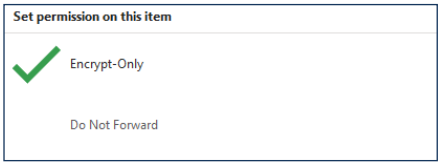
When to encrypt: To help protect against a data breach and protect the privacy of an email message, encrypt every time you send a message containing sensitive information to an external party.

Some examples are:

- Driver license number or state identification card number
- Social Security number
- Credit card/debit card or account numbers
- Health information

How to encrypt:

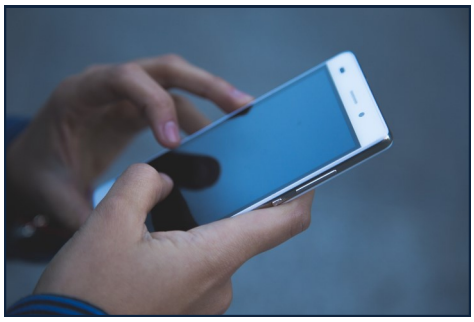
1. With a New Email message open in Outlook, click Options > Encrypt (pictured above).
2. If presented with a drop-down list, select "Encrypt-Only."



3. Look for verification of encryption above To: field

4. Send email as you normally would.

Mobile Device Security



It's not breaking news to say mobile devices have become increasingly more integrated into our everyday lives. We all know this. Our trusty mobile phones are more than just communication tools; they're our pocket-sized command centers. But the convenience they provide does come with a bit of a cost.

Mobile devices will be bigger targets for attackers as they continue to be our preference over desktops for things like browsing the web, checking social media, banking, and other online activity.

So how do we stay safe?

Lock It Down: First things first, make sure your phone is protected with a strong passcode, fingerprint, or facial recognition. This simple step can be your first line of defense against unauthorized access.

Keep It Updated: We all know those pesky update notifications can be annoying, but they're crucial for staying ahead of cyber threats. Regularly updating your phone's operating system and apps patches up vulnerabilities and keeps hackers at bay.

Beware of Wi-Fi Hotspots: Public Wi-Fi networks can be a cyber minefield. Avoid connecting to unsecured networks, as they can leave your device vulnerable to hackers snooping on your data. If you must use public Wi-Fi, consider using a virtual private network (VPN) for an added layer of protection.

Be Smart About Apps: Before downloading that trendy new app, take a moment to check its reviews, permissions, and developer credentials. Stick to reputable app stores like Google Play Store or Apple App Store to minimize the risk of downloading malicious software.

Don't Get Hooked: Cybercriminals love targeting mobile users through phishing emails, texts, QR Codes, and even fake websites. Stay vigilant and never click on suspicious links or provide personal information unless you're absolutely certain of the source's legitimacy.

Lost Phone? Act Fast: If your phone goes missing, act fast to protect your data. Use remote tracking and wiping features to locate your device and erase its contents if necessary.

Trust Your Instincts: Lastly, trust your instincts. If something feels off or too good to be true, it probably is.

Deeper Dive on Mobile Device Security: https://www.proofpoint.com/us/threat-reference/mobile-security

In the News

Hackers are targeting a surprising group of people: young public school students

(Kavitha Cardoza | March 12, 2024)

When Celeste Gravatt first heard about a data breach in her kids' school system in February 2023, it sounded innocuous.

"I didn't really think anything of it at first," Gravatt says.

Officials at Minneapolis Public Schools called it a "system incident," then "technical difficulties," and finally, "an encryption event."

Gravatt has two children who have already graduated from Minneapolis schools, and one who is currently in middle school. She says it was only when she checked social media that she realized the true extent of the attack, and what it could mean for her kids.

Minneapolis Public Schools had been hit by what experts describe as one of the most devastating cyberattacks ever. Hackers stole district data, including files where children were identifiable, and then demanded the district pay a ransom for it. When district officials refused, the hackers released the data online. It included Social Security numbers, school security details and information about sexual assaults and psychiatric holds.

Minneapolis Public Schools did not make any officials available for an interview. In a written statement, the district said it sent written notice of the attack to more than 105,000 people who may have been impacted by it.

"This breach was actually really huge," Gravatt says. "And it wasn't just school records. It was health records, it was all sorts of things that should be privileged information that are now just out there floating around for anybody to buy."

It's an example of a growing nationwide trend in which hackers are targeting a surprising group of people: young public school students.

Full Story: https://www.npr.org/2024/03/12/1237497833/students-schools-cybersecurity-hackers-credit

A Few More Cyber News Stories:

AI-fueled scams target tax refunds
https://www.axios.com/2024/03/20/tax-returns-scam-ai-cybersecurity

Scams are becoming more convincing and costly
https://www.helpnetsecurity.com/2024/03/25/scams-volume-increase

US must establish independent military cyber service to fix 'alarming' problems
https://defensescoop.com/2024/03/25/u-s-must-establish-independent-military-cyber-service-or-risk-catastrophic-condition-report

CYBER CHALLENGE

Insider Threat Detection

This Month's Challenge

For this month's challenge, let's see how well you do in a digital escape room.

We've done Mission 1 of this game from the Center for Development of Security Excellence (CDSE) so give Mission 2 a go. Or if you missed out on Mission 1...feel free to try that one too!

You'll have 25 minutes to search 4 rooms for clues and evidence to aid your investigation.

Send me a screenshot of the last screen once you've completed the mission.
(You'll know it when you see it.)

Good luck!

https://securityawareness.usalearning.gov/cdse/multimedia/games/escape/index.htm