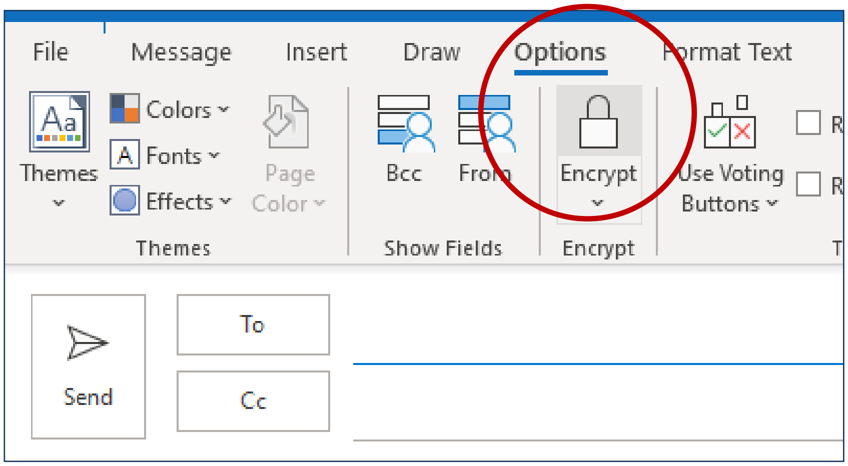
NEWS
CYBER SECURITY
Vol. 8 | Issue 5
May 2023

| Page 2 | Page 3 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

It’s May! Hope you’re able to get outside and enjoy the weather before the Texas sun hits us this summer.

1 big thing: To protect the privacy of an email message, encrypt it.



What to know: Encrypting an email message in Outlook means it's converted from readable plain text into scrambled cipher text to protect it as it travels across the wire to the recipient’s inbox.

Encrypting email can significantly lower the chances of a hacker gaining access to the sensitive data within your emails (for example, Personally Identifiable Information (PII) such as Social Security numbers, driver’s license numbers, bank account numbers, credit card numbers, etc.)

How to encrypt an email: When using Outlook, follow these three quick steps (pictured above).

1. Open a New Email.
2. Click the Options tab.
3. Click the Encrypt button.

And that’s it! Your email is now protected from snoopers.

Note: The process is the same using Outlook’s WebMail (OWA).

Passwords

As we navigate through the digital world, we rely heavily on passwords to protect our sensitive information from cybercriminals. Yet many of us still use weak and easily guessable passwords for the sake of convenience, especially with so many to remember.

Those basic passwords are a hacker's dream come true, as they can be cracked within seconds, leaving us vulnerable to cyberattacks.

With a few simple best practices, you can strengthen your passwords and keep your data safe from prying eyes.

- **Use long and complex passwords.** The longer the password, the harder it is for hackers to crack. Aim for a password that is at least 12 characters long and uses a mix of upper and lowercase letters, numbers, and special characters. Use random words and phrases that are hard for others to guess but easy for you to remember.

- **Avoid using personal information.** Hackers can easily guess your password if it includes personal information such as your name, birthdate or phone number.

- **Use unique passwords for each account.** Using the same password for multiple accounts is a big mistake that can compromise all of your online accounts if one gets hacked. (Password managers can help with this.)

- **Use a password manager.** Consider using a password manager to generate and store complex passwords for each online account. They provide an encrypted vault for your passwords, making it a little easier to use unique, strong passwords without having to remember them all.

- **Enable two-factor authentication.** Two-factor authentication adds an extra layer of security to your accounts, requiring a secondary method of authentication such as a fingerprint or a code sent to your phone, in addition to your password.

- **Keep passwords private.** Don’t share passwords with colleagues, family or friends. Avoid writing them down, especially in plain sight or on your computer (the dreaded sticky note on keyboard!). If you must write them down, store them in a secure location, such as a locked drawer.

For more information on passwords and password managers: https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts

In the News

'Juice Jacking': The Dangers of Public USB Charging Stations

(FTC | Updated: April 11, 2023)

Planning to travel? No doubt you'll have your cell phone or another portable device, and you'll need to re-charge it at some point.

If your battery is running low, be aware that juicing up your electronic device at free USB port charging stations, such as those found in airports and hotel lobbies, might have unfortunate consequences. You could become a victim of "juice jacking," yet another cyber-theft tactic.

Cybersecurity experts warn that bad actors can load malware onto public USB charging stations to maliciously access electronic devices while they are being charged. Malware installed through a corrupted USB port can lock a device or export personal data and passwords directly to the perpetrator. Criminals can then use that information to access online accounts or sell it to other bad actors.

In some cases, criminals may have intentionally left cables plugged in at charging stations. There have even been reports of infected cables being given away as promotional gifts.

Here are some tips to help you avoid becoming a juice jacking victim:

- Avoid using a public USB charging station. Use an AC power outlet instead.
- Bring AC, car chargers, and your own USB cables with you when traveling.
- Carry a portable charger or external battery.
- Consider carrying a charging-only cable, which prevents data from sending or receiving while charging, from a trusted supplier.

If you plug your device into a USB port and a prompt appears asking you to select "share data" or “charge only,” always select “charge only.”

Source: https://www.fcc.gov/juice-jacking-dangers-public-usb-charging-stations

A Few More Cyber News Stories:

Russian hackers exploit six-year-old Cisco flaw to target US government agencies
https://techcrunch.com/2023/04/19/russian-hackers-exploit-six-year-old-cisco-flaw-to-target-us-government-agencies

AI tools like ChatGPT expected to fuel BEC attacks
https://www.helpnetsecurity.com/2023/04/17/bec-attacks-language-attack-vector

Discarded, not destroyed: Old routers reveal corporate secrets
https://www.welivesecurity.com/2023/04/18/discarded-not-destroyed-old-routers-reveal-corporate-secrets

CYBER
CHALLENGE

Cyber Crossword

This Month's Challenge

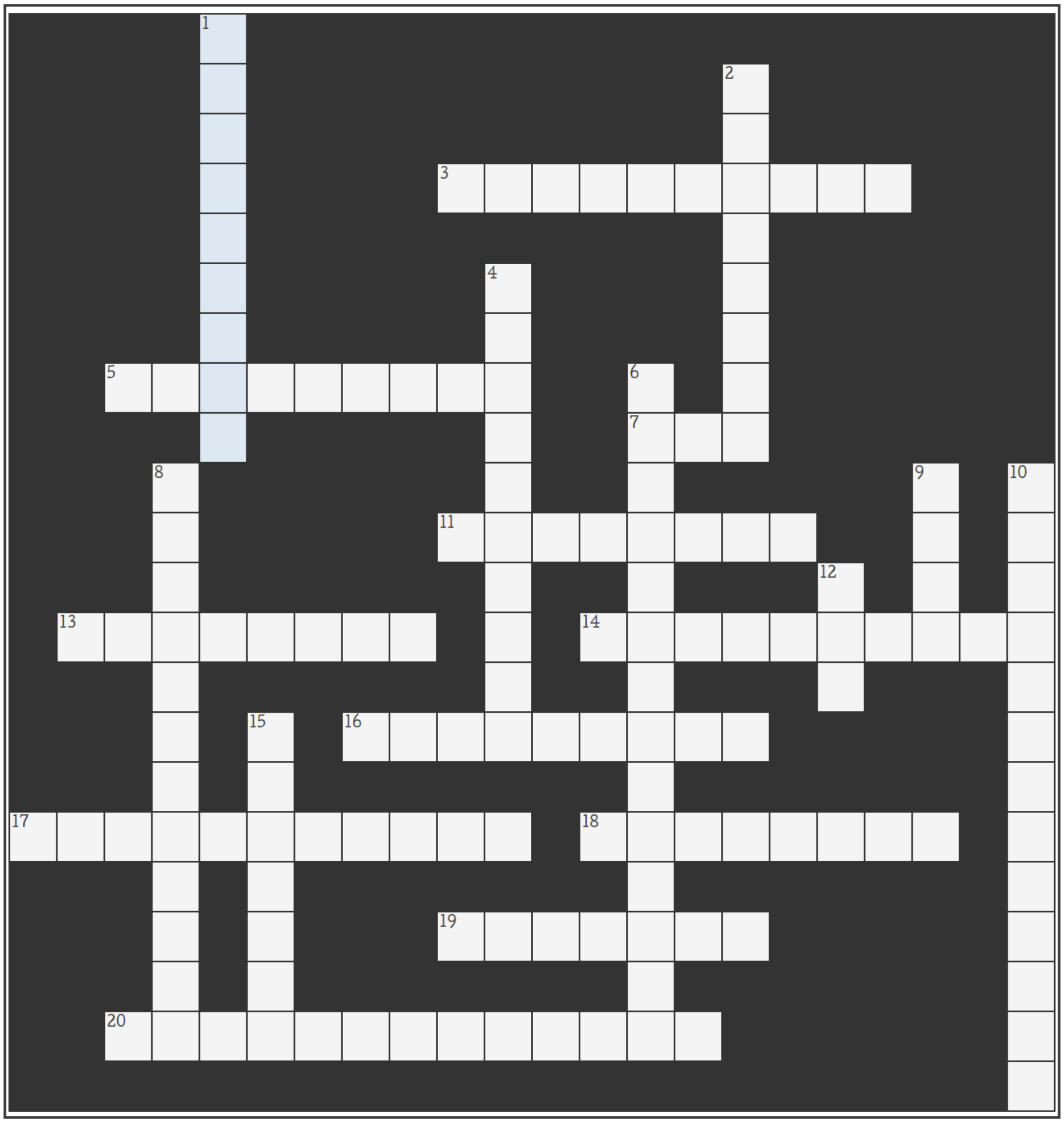
For this month's challenge, let's do a crossword puzzle!

If you've recently taken our annual cyber awareness training, this should be a breeze.

Do me a favor and don't peek at the answers unless you absolutely have to. I'd actually rather you Google the term first so some of what you read sticks!

Send me a screenshot of your completed puzzle. Good luck!

https://securityawareness.usalearning.gov/cdse/multimedia/games/cybersecurity-crossword/index.html


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20