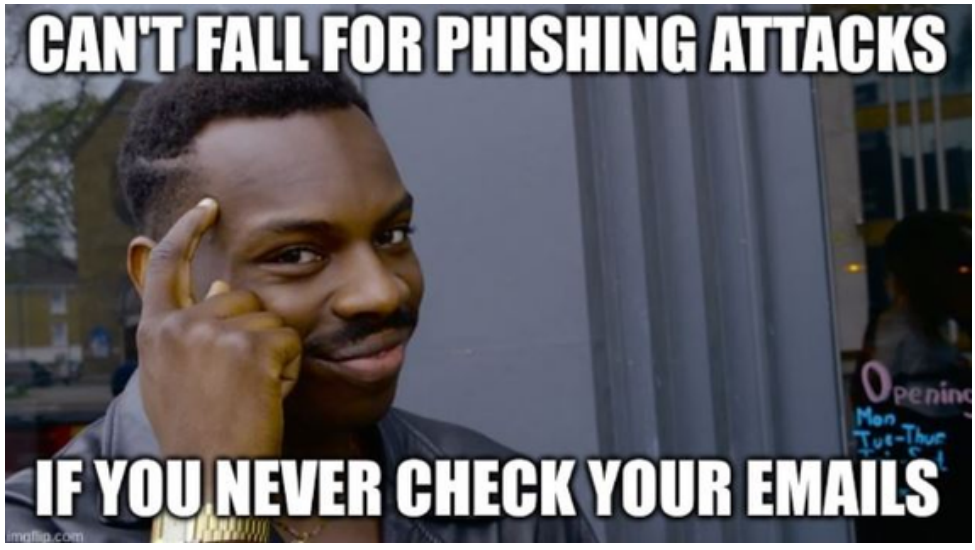
Issue no.21

SY 26-27



October is Cybersecurity Awareness Month



Our constantly connected world has provided massive benefits in terms of data aggregation, analytics and ease at which we can access information.

Unfortunately, all of this convenience comes with a high risk, as year after year Cybersecurity becomes a larger and larger issue. So much so, October has been labeled "**CyberSecurity Awareness Month**"

This issue will contain some Cybersecurity info, tips and tricks to help our users remain safe and secure when online.

common sense

CommonSense.org

Common Sense Media, located at the above URL, offers a great amount of resources for educators regarding CyberSecurity, including definitions, best practices and even how the concepts can be introduced to students.

CommonSense's online curriculum is based on the fact that anyone who uses technology, even just a general smart phone, should be aware of CyberSecurity concepts and practices. The below excerpt is directly from their site:

What are the absolute basics I need to know?
Everyone who uses technology, even just a smartphone, should be familiar with common types of scams and know how to **protect themselves, their data, and their devices**. And when we're aware of the latest kinds of attacks and able to protect ourselves, then we can also help our students and our schools.

What this means for Educators

Online risks do not stop with faculty and staff, but applies to students as well, both inside the classroom and in their daily lives as they use technology to accomplish just about everything they need to do.

It is a shared effort to educate students about online safety, data risks and promoting good Digital Citizenship in the Tech Age.

CyberSecurity tips for educators have even been provided by the US Department of Education and can be viewed here: https://studentprivacy.ed.gov/resources/top-10-cybersecurity-tips-teachers



What's in a Password?

Password guidelines have been in question over the last few years. Most recently, the National Institute of Standards & Technology have released criteria specifically pertaining to Education.

Best practices to keep your passwords safe and secure, both at work and for personal accounts, include:

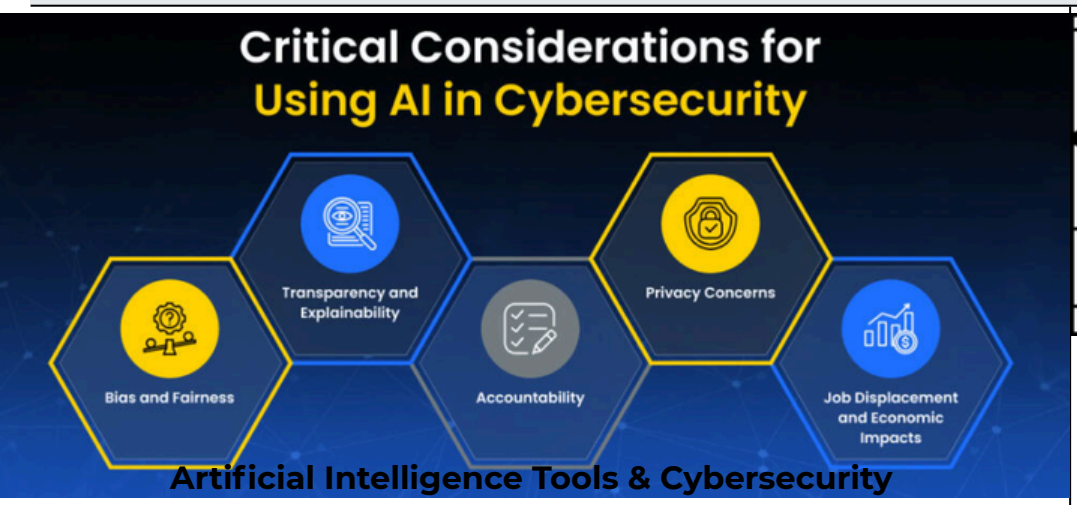
- ***The longer a password is, the stronger it is***
- ***Use pass phrases of 4-7 unrelated words***
- ***Use unique passwords for each account***

More information and resources on passwords can be found on the cisa.gov site

Cybersecurity Grant Funding

Diman has taken advantage of available grant funding for cybersecurity projects! Over the next 18 months we will be:

- Transitioning to a **new Antivirus Provider** – same software means PCs do not have to be updated directly
- **Internal Penetration Testing** – State resources have asssisted in procuring a vendor that will attempt to break into our internal network to test system resilience



Artificial Intelligence Tools & Cybersecurity

Artificial Intelligence raises several cybersecurity concerns surrounding equity, access and bias. These tools are still actively being developed and are extremely fluid, in that they are changing almost daily. **ONLY AI models covered by a Student Data Privacy Agreement ensure the data input into the system is not retained to continually train the software**.

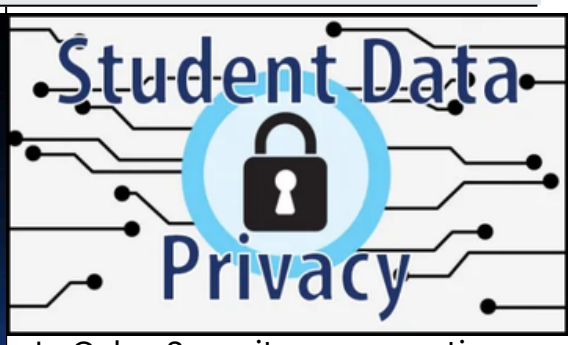
Diman has successfully registered for an extended trial of ChatGPT and Anthropic's Claude AI. These tools are covered by SDPAs as long as you are logging in with your Diman Regional account and working within our specific workspace. *Anyone interested in trying these apps please reach out to helpdesk@dimanregional.org for an invite!*

What in the WiFi?!

Friendly Reminder: Please email helpdesk@dimanregional.org with info on any vendors or visitors that may require Wireless Access to the DimanReg network.

DimanOPEN is available in select areas of the building throughout the day, while DimanPUBLIC broadcasts in the afternoons until the following morning.

Our network vendor will be onsite Thursday and Friday this week to complete a *Wireless Site Survey* – A critical part of any wireless installation where signal strength is measured and coverage gaps identified.



In CyberSecurity conversations we cannot avoid the topic of Student Data Privacy, but what does it mean, exactly? Student Data Privacy refers to a set of guidelines software/technology vendors need to follow in order to ensure student data is not misused.

Why is this important? The most valuable item to nefarious parties in the Information Age is DATA. Raw student data could help companies craft targeted marketing campaigns aimed directly at students, while attackers can use this data to piece together a student profile and potentially ruin a student's credit report before the age of 18. In one of the worst cases seen, private Elementary student data was used to open credit card and other accounts, leading to the students having to now clean this up as they enter the workforce. Talk about a graduation gift!

It is important that any vendor in use by the district complies with and is willing to sign a Data Privacy Agreement. Companies do not care about student privacy, so it is up to us to enforce this protection for our students.

TOP 10 CYBERSECURITY TIPS FOR TEACHERS

From the U.S. Department of Education's Student Privacy Policy Office (SPPO) and its Privacy Technical Assistance Center (PTAC)



1 Be Aware of Social Engineering Techniques

- Be skeptical. Question unexpected or atypical emails or requests for information, especially if they create a sense of urgency or pressure you into immediate action.
- Verify the identity of the person or organization by contacting them independently through official channels.

2 Use Strong Authentication Practices



- Use strong passwords.
- Enable multi-factor authentication.

3 Keep Devices Updated with the Latest Software & Security Patches



- Enable automatic updates.
- Regularly check for updates to your software and apps.

4 Use Anti-Virus Software & Scan Devices Often



- Install and use reputable antivirus software that checks in real-time to spot threats early.
- Ensure the software runs regular system scans.

5 Avoid Public Wi-Fi



- Use your mobile data or personal hotspot instead.
- Avoid accessing or sending sensitive information while connected to public wi-fi.

6 Encrypt Sensitive Information



- Enable full-disk encryption.
- Apply a password to sensitive files & folders.

7 Use Safe Browsing Strategies



- Be cautious when clicking on links or downloading files.
- Regularly clear your web browser cache and cookies.

8 Use Only Approved Software



- Use only school-approved software.
- Always scan downloaded software and data files.

9 Back Up Your Data



- Diversify your backup methods.
- Regularly test your backups.

10 Never Leave Devices Unlocked or Unattended



- Never leave a phone, laptop, or storage media unlocked or unattended.
- Do not attempt to plug in or attach any untrusted media.

Questions or requests for additional information should be directed to SPPO and PTAC at PrivacyTA@ed.gov, or call 1-855-249-3072.

