What is Cybersecurity?
Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

This edition of the newsletter will offer information in addition to best practices to help you keep your (and the university’s) digital information protected. You play a critical role in protecting university information, so please read and enjoy this latest edition of IT Connect.

Try building a new habit or two based on the tips and tricks listed that will help make our campus a more secure digital workspace. If you would like to learn more or have additional questions, please reach out to Kennesaw State University’s Office of Cybersecurity (https://uits.kennesaw.edu/ocs) at ocs@kennesaw.edu.

If you receive a suspicious email, forward it to abuse@kennesaw.edu without clicking on any of the links or opening any files.
Password Security

Passwords are the first line of defense for most technology accounts. There is a reason why websites and applications need to have strong passwords. Malicious individuals can use their own computers to tirelessly attempt to guess your password. Factors that make a password strong are:
- Not using words found in the dictionary
- Making sure that the password is at least 8 characters long - the longer the better!
- Using special characters such as !@#$%^&*(), mixing upper/lower case, and numbers

It is better to use a "pass phrase" - take your favorite saying, song lyric, mantra, or other phrase and either use part of it as your pass phrase or use the first letter of each word. You are less likely to forget it. For example, if your favorite song is The Rolling Stones "Satisfaction," take the chorus and turn it into a pass phrase "IcantGetnoSatisfaction!" To make it even stronger, and comply with certain applications and websites with password content requirements, try substituting @ for the letter a, the number zero for the letter o, ! for the letter i, and mix the case: “Ic@ntGetnoS@t!sf@ct!0n.”

Never leave your password written down and in plain view and never share your password. Use a password management tool such as LastPass or MiniKeePass to keep track of your important passwords. Lastly, change your passwords frequently, and try never to use the same user ID/password combo on multiple websites.
Phishing is a type of cyber attack used to acquire sensitive and valuable information from individuals through fraudulent means. While this is done in different ways, email is by far the most common method used by attackers. Some phishing emails are designed to put the recipient at ease by appearing to originate from a trustworthy source. Attackers commonly use this tactic to steal login credentials, personal confidential information, or to encourage users to click malicious links. Other phishing emails will impersonate a co-worker or supervisor with a familiar username, urgently asking for confidential or financial data.

Here are some tips to help keep you safe:

- If unsure, check the full email address of the sender and not just the displayed name. Links within these emails can direct the recipient to a fake website, so hovering over the link is a safe way to see if the URL is legitimate.
- Check to see if the URL is misspelled or otherwise altered. Never follow a link if the URL can’t be verified or seen.
- Avoid downloading an attachment or clicking a link in any email that seems suspicious, especially if it’s an unexpected email from someone you don’t recognize or work with. Oftentimes attackers use these links or attachments to install malicious software than can be used to steal confidential information such as passwords or banking information.

Remember that all official University business communication is done through Kennesaw State University email accounts, which will be "@kennesaw.edu" and we never ask for login credentials. If you are still unsure of the legitimacy of an email, contact the sender directly for verification.
Find These 14 words in the word search puzzle:

APPLICATION
AUTHENTICATION
CYBERSECURITY
DEVICE
DUO
EMAIL
HACKER
KENNESAW
MOBILE
PASSWORD
PHISHING
SECURE
SPAM
TECHNOLOGY