South Orange County Community College District

Message from District Information Technology (IT)
Welcome to the Spring 2025 Semester!

With the start of the semester, we would like to highlight the growing importance of 'cyber hygiene.' It is something we all need to think about daily to keep our devices, data, and accounts safe and secure. Here are a few helpful things to remember:

1. **Security awareness training:** The district has enrolled all employees for annual security awareness training (with faculty occurring every 2 years) to help educate us with the latest trends in threats and how to protect ourselves at home and within our organization.

   ** Have you had a chance to complete this training yet? If not, or if it has been a while since your last session, we kindly encourage you to take a few minutes to complete it. You will find the training in the **Learning** section of Workday.

2. **AR3720 – Electronic communications:** Our district has guidelines in place to ensure the safe and proper use of electronic communications like email, Teams, and other online tools. These are outlined in Administrative Regulation 3720, which provides clear guidelines for using these tools securely and responsibly.

   ** AR3720 [III. PROHIBITED USES (A)] prohibits communicating any information concerning any password, user account, personal identification number or confidential information protected by law without the permission of its owner or the controlling authority of the computer facility to which it belongs"

3. **Phishing attacks** (scammers sending deceptive emails), Microsoft **Teams messages** (purporting to be from legitimate sources to trick people into divulging sensitive information), **text messaging** (asking for urgency or replies), and **voice calls** (utilizing modern AI techniques to masquerade as real employees or vendors) are on the rise globally. *Never click on links or download attachments from unknown sources.* If a communication is suspected to be a scam or malicious in nature, then please forward the email to report_spam@socccd.edu for further investigation.

4. **Anatomy of a secure password:** Unique strong passwords are essential to the security of accounts. Our Administrative Regulation 3727 requires passwords to be:
    - a **minimum of 8 characters** in length (12 or more characters are highly recommended)
    - have at least **one upper-** and **one lower-**case letter.
    - have at least **one number.**
    - have at least **one special character.**

    Passwords should not be based on your personal information that can be easily guessed or discovered online (such as from social media). For ease of memorization, it preferred to use a **"passphrase"** which promotes longer and more secure passwords. Passphrases are "password phrases" and can tell a story or be a collection of meaningful words. An example can be "Is1PurpleVaseLeft?".

5. **Keep restricted data safe:** When it comes to managing sensitive information like private health data, credit card details, or social security numbers, it is important to use the right tools. These types of data should only be managed through approved applications designed to keep the data secure. **To protect this information, please avoid sharing it through email, Teams messages, or downloading it to your computer.**

    Forwarding emails and personal "cloud storage" can also introduce risks as it often copies the data to non-district protected systems (like GMail, YMail, Box, Google Drive), taking these sensitive items out of our purview and making it harder to support their security. Whenever possible, try to avoid email forwarding and personal cloud storage with **any** work documents or communications.

6. **How to report issues:** Your online safety is our top priority, and we rely on you to help us spot potential issues! If you notice your device acting strangely, think your account might be compromised after replying to an email or visiting a website, or have questions about a recently downloaded file, do not hesitate to let us know.

    Reach out to your local Technology Team right away, we are here to help! You can also report incidents directly through Ivanti, which you will find in our Single Sign-On Apps Portal. Together, we can keep things secure!

Remember, we are all responsible for ensuring the security of our systems and data.
Thank you and we hope you have a good semester.