Citrus College eMEMO

CITRUS COMMUNITY COLLEGE DISTRICT 1000 W. Foothill Blvd., Glendora, CA 91741-1899

Technology and Computer Services (TeCS) Update

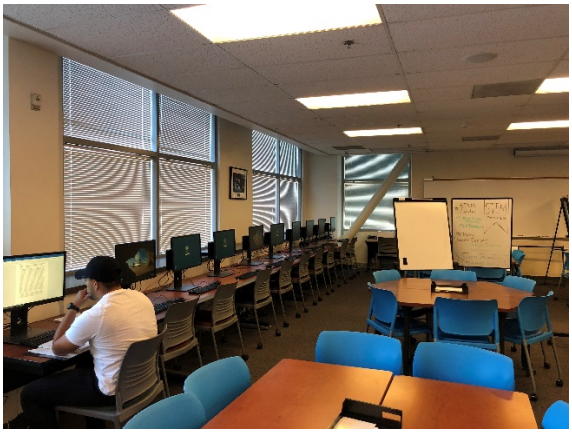
August 2018

Welcome to Fall 2018! Technology and Computer Services has been busy with a number of projects during the summer months.

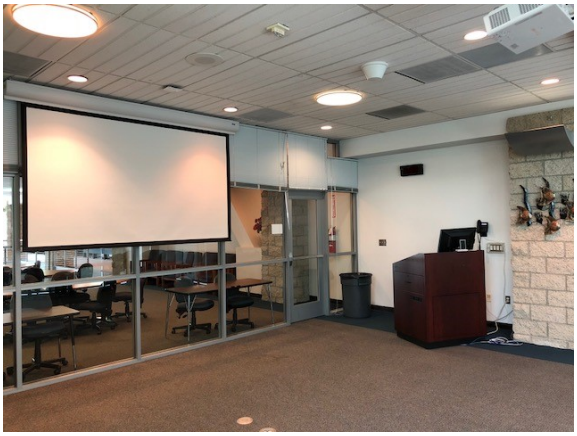
Computer Replacements and Room Conversions

New computers were installed in SS 281 and PC 304. Ten new computers were installed in MA 129 as part of the STEM center relocation, and technology was installed in the Library Fish Bowl (LI 204) to convert that room into a classroom.

SS 281- Career/Transfer Center Lab



MA 129 – STEM Center



Library Fish Bowl (LI 204)

PC 304

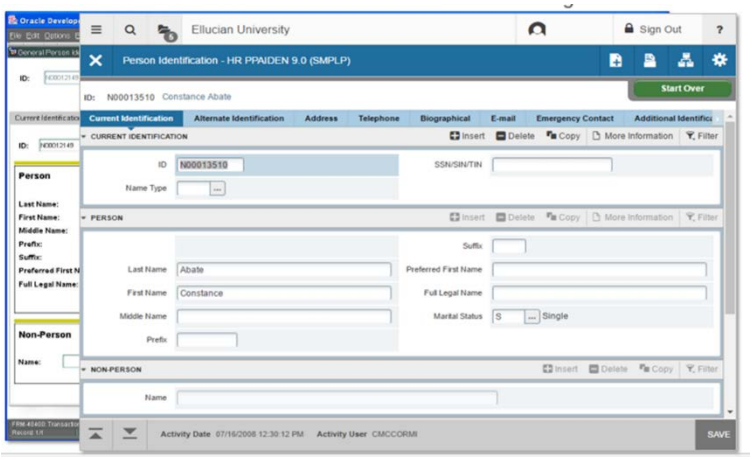
Outdoor Wireless Internet Access

This fall, students, staff and faculty will be able to connect their mobile devices to the Internet at several outdoor locations on campus. The first outdoor wireless access point (shown in the picture on the right) was installed on Friday, August 24.

Outdoor wireless access will be provided near the Visual Arts building, the Hayden Library, the Campus Center, the Mathematics/Science building, the softball fields, the outdoor pool areas and the football stadium.

This project is expected to be completed by mid-September.

Get ready for Banner 9!



Our Banner Student Information System, known as WingSpan, is undergoing a major transformation this year. All of the administrative screens will be converted to web-based forms with a more modern look and feel, and provide better compatibility with the latest web browsers such as Chrome, Firefox, Safari and Edge.

Students will see a significant improvement in their registration experience, as a new 'shopping cart' functionality will be provided and students will be able to register for classes directly from their student educational plans. Training classes for Banner 9 will begin during the fall semester.

Don't Let a Phishing Scam Reel You In!

Citrus College has been the target of several malicious e-mails recently. Some of them have been surprisingly sophisticated, bearing the Citrus College logo and the signature block of the Superintendent/President. TeCS has been proactively deleting these as they appear in our system.

The purpose of these malicious e-mails (referred to as "phishing") is to collect your user name and password so the criminal can use those credentials to send massive amounts of unsolicited commercial e-mails, or "spam", to thousands of other accounts across the world. When this happens to a Citrus College account, large internet service providers such as Google start blocking our legitimate e-mail from reaching its destination, hampering the ability of the college to conduct business.

Security Matters

Social engineering is at the heart of all phishing attacks, especially those conducted via e-mail. Technology makes phishing easy. Setting up and operating a phishing attack is fast, inexpensive, and low risk: any cybercriminal with an e-mail address can launch one.

According to Verizon's 2017 Data Breach Investigations Report, the education sector saw a rise in social engineering–based attacks. Students, staff, and faculty all suffered losses when personal data and research were disclosed to unauthorized parties. Phishing played a part in more than 40% of these breaches. Knowing what you're up against can help you be more secure. Here are a few things you can do to guard against phishing attacks:

- **Limit what you share online.** The less you share about yourself, the smaller the target you are for a phishing attack. Cybercriminals use information you post online to learn how to gain your trust.

- **Protect your credentials.** No legitimate company or organization will ask for your username and password or other personal information via e-mail. Your school definitely won't. Still not sure if the e-mail is a phish? Contact your IT help desk. At Citrus College, you can report these e-mails by forwarding them to badmail@citruscollege.edu.

- **Beware of attachments.** E-mail attachments are the most common vector for malicious software. When you get a message with an attachment, delete it—unless you are expecting it and are absolutely certain it is legitimate.

- **Confirm identities.** Phishing messages can look official. Cybercriminals steal organization and company identities, including logos and URLs that are close to the links they're trying to imitate. There's nothing to stop them from impersonating schools, financial institutions, retailers, and a wide range of other service providers.

- **Trust your instincts.** If you get a suspicious message that claims to be from an agency or service provider, use your browser to manually locate the organization online and contact them via their website, e-mail, or telephone number.

- **Check the sender.** Check the sender's e-mail address. Any correspondence from an organization should come from an organizational e-mail address. A notice from your college or university is unlikely to come from YourIThelpdesk@yahoo.com.

- **Take your time.** If a message states that you must act immediately or lose access, do not comply. Phishing attempts frequently threaten a loss of service unless you do something. Cybercriminals want you to react without thinking; an urgent call to action makes you more likely to cooperate.

- **Don't click links in suspicious messages.** If you don't trust the e-mail (or text message), don't trust the links in it either. Beware of links that are hidden by URL shorteners or text like "Click Here." They may link to a phishing site or a form designed to steal your username and password.

Monthly Content for Security Matters is courtesy of the EDUCAUSE Campus Security Awareness Campaign.