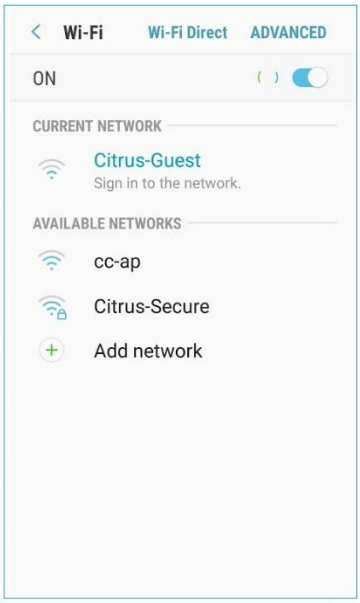
Citrus College eMEMO

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

Technology and Computer Services (TeCS) Update

May 2019

Guest Wireless Access



TeCS is pleased to announce the availability of guest access to our Citrus College wireless network.

There are many occasions when parents, prospective students, job applicants, performing arts and athletic audiences, and other members of the public arrive on campus and need to connect to the Internet.

Thanks to the recent implementation of new network access control software, visitors can select the 'Citrus-Guest' network on their mobile device. If they agree to comply with Citrus College administrative procedures governing network access and provide a valid e-mail address, they will receive a link to a temporary one-day connection to our wireless network.

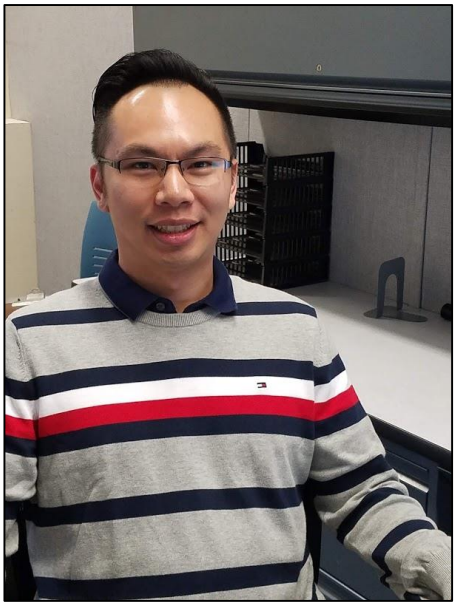
"Meeting Owl" Device for Video Conferencing

Attending a video conference can sometimes be a frustrating experience. TeCS is piloting the Meeting Owl to improve the video conference experience for Citrus College staff and faculty, with the potential for classroom use as well.

The Meeting Owl is a device that sits in the middle of a conference table and contains cameras, microphones and speakers. When connected to a laptop during a typical video conference session, the remote participant can see and hear all of the attendees in the meeting room, and cameras rotate and focus on the individual speaking. A video demo of the device is available at this link.

Contact the TeCS Help Desk at x4357 to reserve the Meeting Owl for your next video conference.

Welcome Ryan Tang – IT Security Analyst



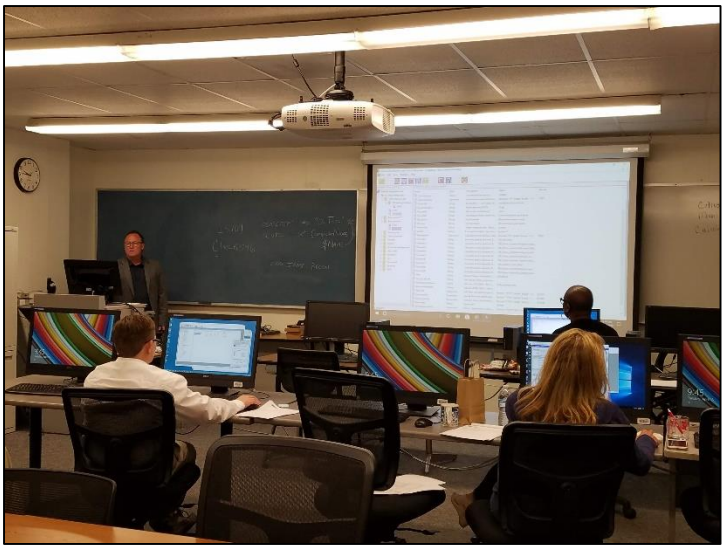
We are pleased to welcome Ryan Tang to our team as the new Information Technology Security Analyst.

For the past four years, information security has been the most important issue for colleges and universities, as reflected in the annual EDUCAUSE Top 10 IT Issues report. In addition, recent financial aid regulations require that colleges have a designated individual responsible for data security.

Ryan served in the Air Force, and was responsible for launch vehicle systems, user equipment and IT support. While in the Air Force, he was trained in project management and cybersecurity.

Ryan has an AS in Computer Administration and Security from Mt. San Antonio College, a BS in Electrical Engineering from Cal Poly Pomona, and is currently working on his MBA. He has industry certifications in CCNA and Security+, and certificates in CCNP, Windows Administration, Linux and Networking. Ryan will be working on several initiatives this coming year to further protect our data and our networking and computing infrastructure.

Financial Aid Automation



Last month staff from TeCS and the financial aid department worked with consultants to automate and streamline financial aid processing.

Over the course of six days, two consultants worked side by side with college staff to configure our computer job scheduling system to automatically load financial aid applications into our system from the Department of Education, post checklist requirements on applicant records, send e-mails of document requirements and process financial aid awards.

Prior to this process, staff in financial aid were spending up to four hours per day manually running one job in Banner after the other. With the automated process in place, the job sequence is less error-prone, staff can monitor the processes running automatically in the background on their computers, respond to notifications of issues during the process, and the entire process can be completed in less than one hour.

Lab Updates

This spring the VA 210 and LI 120 computer labs received computer replacements. VA 210 received 30 new Mac mini computers and the LI 120 lab received 32 new all-in-one computers, as well as a new instructor computer. During the last 12 months over 400 computers have been replaced throughout campus.

VA 210 Lab

LI 120 Lab

Security Matters – Social Engineering

Social engineering—manipulating people into doing what they want—is the most common way for cybercriminals to steal information and money. According to an article on Wired.com (https://www.wired.com/story/email-scammers-gift-cards-nonprofits/), between November 2017 and February 2019, six hundred and sixty (660) education-related institutions were targeted with a scam in which employees were tricked into purchasing gift cards and sending the codes to someone they wrongly assumed was a trusted authority.

Social engineering is at the heart of all types of phishing attacks—those conducted via email, SMS, and phone calls. Technology makes these sorts of attacks easy and very low risk for the attacker. Make sure you're on the lookout for these variants on the traditional, mass emailed phishing attack:

- **Spear phishing:** This kind of attack involves often very well-crafted messages that come from what looks like a trusted "very important person" (VIP) source. These messages will ask recipients to rush and bypass normal processes. Targets are those who can conduct financial transactions on behalf of the organization (sometimes called "whaling").

- **SMiShing:** Literally, phishing attacks via short message service (SMS) or text messaging. These scams attempt to trick users into supplying content or clicking on links in SMS messages on their mobile devices. Flaws in how caller ID and phone number verification work make this an increasingly popular attack that is hard to stop.

- **Vishing:** Voice phishing are calls from attackers claiming to be government agencies such as the IRS, software vendors like Microsoft, or services offering to help with benefits or credit card rates. Attackers will often appear to be calling from a local number close to yours. As with SMiShing, flaws in how caller ID and phone number verification work make this a dangerous attack vector.

No matter the medium, follow these techniques to help prevent getting tricked by these social engineering attacks:

- **Don't react to scare tactics:** All of these attacks depend on scaring the recipient. Examples include notice that you are being sued; that your computer is full of viruses; or that you might miss out on a chance at a great interest rate. Don't fall for it!

- **Verify contacts independently:** Financial transactions should always follow a defined set of procedures, which includes a way to verify legitimacy outside email or an inbound phone call. Legitimate companies and service providers will give you a real business address and a way for you to contact them back, which you can independently verify on a company website or support line. Don't trust people who contact you out of the blue claiming to represent your bank or an agency.

- **Know the signs:** Does the message or phone call start with a vague information, a generic company name like "card services," an urgent request, and/or an offer that seems impossibly good? Hang up or click that delete button!

To help you more readily identify suspicious e-mails, our mail server will automatically add the following footer to any e-mail that is sent to you from an external source. Take time to reach out to senders via phone or a new e-mail to confirm any unusual action requested of you.

CAUTION: This email originated from outside of the organization. Do not click links, open attachments, or reply unless you recognize the sender and know the content is safe. Contact Helpline at 4357 if you need assistance.

Monthly content for Security Matters is courtesy of the EDUCAUSE Cybersecurity Program.