Citrus College eMEMO

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

Technology and Computer Services (TeCS) Update

September 2019

Technology Training Classes

TeCS is pleased to present training classes this fall on a variety of topics related to the technology used at Citrus College. Pictured on the right is Felix Perez, IT Support Specialist III, training faculty on the use of the technology in the classroom.

Felix will be offering two additional one hour sessions on this topic: Monday, Sept. 9 at 2 p.m. and Wednesday, Sept.11 at 10 a.m.

Following is a list of additional training classes this month:

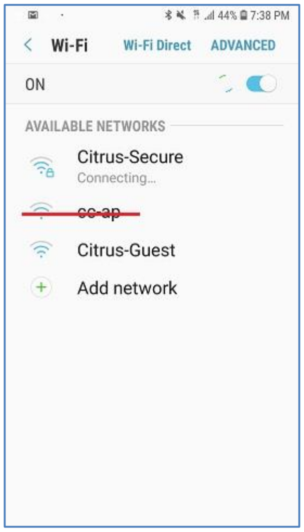
WingSpan 9 Navigation: Friday, Sept.13 at 1:30 p.m.
Argos – Running Reports: Monday, Sept. 16 at 3:00 p.m.
WingSpan Requisitions: Thursday, Sept. 26 at 3:30 p.m.

All classes are held in IS 109 and are scheduled for one hour. To sign up for a training class, log in to the Training Calendar on my.citruscollege.edu.

Citrus-Secure wireless login – stay connected for the term!

Did you know that faculty, staff and students can now connect to the campus wireless network and stay authenticated for the entire term? When you log in to the Citrus-Secure network on your mobile device and enter your network user name and password, you will no longer need to remember to connect and log in each day. Visitors who do not have an account can connect to the Citrus-Guest network and get a one-day pass on our network after registering their e-mail address.

Beginning Friday, September 13 the legacy 'cc-ap' network will be removed. If you need help connecting to the Citrus-Secure wireless network, please visit the Help Desk in IS 103 between 8 a.m. and 5 p.m.



TE 115 Computer Lab Refresh

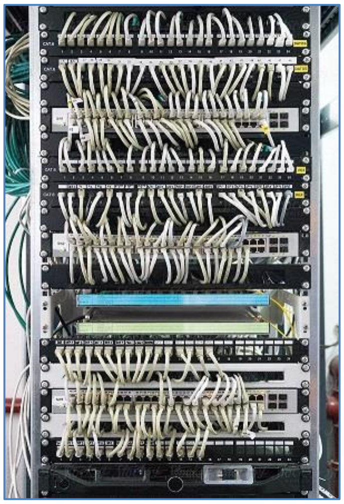
During the summer, TeCS worked to replace 32 desktop computers in TE 115, a lab used primarily for the automotive program.

In 2014, Citrus College established and funded a formal computer equipment replacement cycle to ensure that desktop computers used by students in the classroom reflected the latest technology.

With the completion of the TE 115 computer lab refresh, the five-year cycle has been completed. For the 2019-2020 year, TeCS has identified 159 computers replaced in 2014-2015 and are due for an update, and has submitted plans (pending funding) to start the replacement cycle over again.

Upgrades behind the scenes

Network Switches

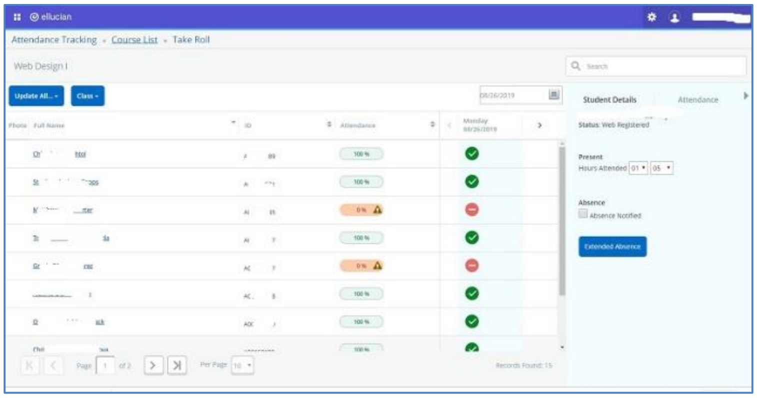


During the past few weeks, TeCS staff have been working early morning hours and weekends to apply some important upgrades to the Citrus College computing infrastructure.

Each floor of every building on campus has a room filled with network switches that connect phones, desktop computers and other devices to computer servers and to the internet. These network switches have software on them that must be upgraded regularly to ensure security and reliability. Fifteen buildings on campus now have upgraded software on their network switches and have been configured for remote access, enabling staff to respond more quickly to outages. Kudos to Ryan Tang and Manuel Guerrero for their work on this project.

WingSpan

The WingSpan (Banner) ERP System also received a number of upgrades during the summer.



Web Design I

08/26/2019

Photo	Full Name	ID	Attendance	Monday 08/26/2019
	[redacted]	[redacted]	100 %	✓
	[redacted]	[redacted]	100 %	✓
	[redacted]	[redacted]	0 % ⚠	⊖
	[redacted]	[redacted]	100 %	✓
	[redacted]	[redacted]	0 % ⚠	⊖
	[redacted]	[redacted]	100 %	✓
	[redacted]	[redacted]	100 %	✓
	[redacted]	[redacted]	100 %	✓

Status: Web Registered

Present
Hours Attended 01 05

Absence
□ Absence Notified

Mike Maliglig, our Database Administrator, applied patches and upgrades to the general, student, financial aid and accounts receivable modules and applied security-related patches to our WingSpan self-service application.

Mike also installed a test version of Faculty Self Service featuring the new Attendance Tracking module, which Tom Cheng demonstrated at the new faculty orientation.

Security Matters – Understanding the Basics of Online Safety and Security

Shopping, surfing, banking, gaming, and connecting Internet of Things devices such as toasters and refrigerators are some of the many actions performed each minute in cyberspace. These common everyday activities carry the cyber threats of social engineering to gain unauthorized access to data, identity theft, bullying, location tracking, and phishing, to name just a few. How can we decrease our risk from these cyber threats without abandoning our online activities altogether? Here are some basic online tips everyone can follow to help stay secure while online.

- **Set up alerts.** Consider setting up alerts on your financial accounts. Many credit card companies and banks allow you to set up alerts on your accounts via their websites. These alerts range from sending you an email or text each time a transaction happens on your account to alerts when transactions meet or exceed a designated spending limit that you set. These alerts keep you in control of your accounts' activities. These types of alerts are useful because they make you aware of what's going on with your account quicker than waiting for monthly statements. When you receive an alert about a transaction that you did not authorize, you can reach out to the credit card company or bank immediately. Log into your credit card company and banking websites to set up alerts on your accounts.
- **Keep devices and apps up to date.** This familiar tip is useful even if you are just casually surfing the internet. Keeping your devices up to date (including apps and operating systems) ensures you have the latest security fixes.
- **Don't use public Wi-Fi.** In addition to an updated device, the network the device is connected to is also important. Did you have to enter a password to connect to a Wi-Fi network? If you did, that network is more secure than an open one that any device within range can connect to. Whenever possible, use a secure network, especially when banking or shopping online.
- **Consider using a VPN.** VPN stands for virtual private network, and its main purpose is to provide a tunnel for encrypted internet traffic. If you are connected to the internet without using a VPN, your traffic is passed through the internet service provider's servers. The location of your device is known, and if you must connect to a public Wi-Fi network, there is a risk of snooping by other devices on the same network. Connecting to a VPN redirects your internet traffic to a remote server, encrypting the traffic, reducing the snooping risk. There are many options for VPN software today for consumers and businesses. Do your research and decide which one makes sense for your online needs.
- **Create unique passwords.** Here's another familiar tip. Using the same password for many sites is not a best practice. Suppose that one of your accounts suffered a data breach and your password was exposed. If you reused this password on other accounts, it's likely that someone would be able to access those accounts as well (especially if your user name is an email address). Consider using a password manager to manage all your passwords. Not only do these tools manage all your passwords, they can also create strong passwords and can even autofill your username and password as you go to websites on different browsers.
- **Be vigilant.** Be aware, there are fake websites out there waiting to collect your valuable information. Make sure you are on a legitimate site by double-checking the URL website address to make sure it is spelled correctly. Also make sure you see a padlock and https:// in the URL.

Remember that you are in control of your online activities. Following these security tips will give you peace of mind while online.

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