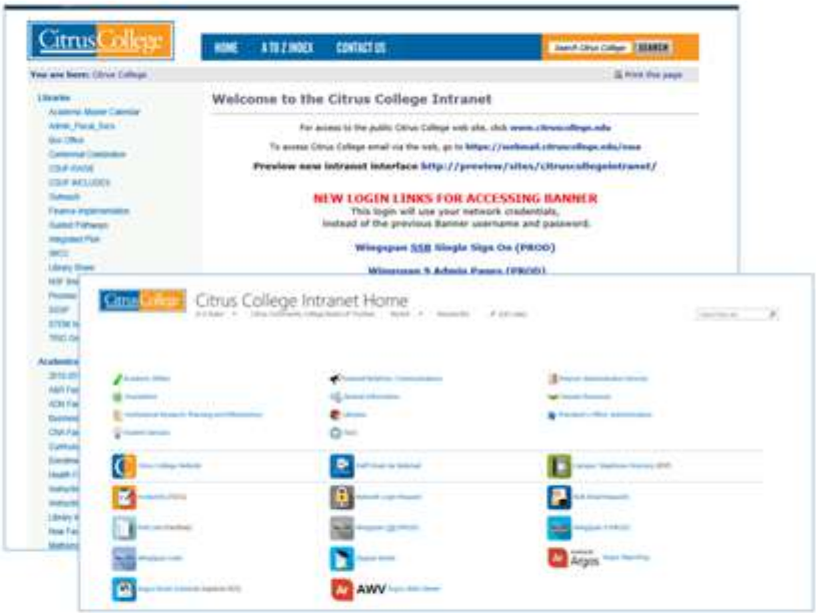
Citrus College eMEMO

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

Technology and Computer Services (TeCS) Update

March 2019

A new Intranet is coming!


Welcome to the Citrus College Intranet

For access to the public Citrus College web site, click www.citruscollege.edu

To access Citrus College email via the web, go to https://webmail.citruscollege.edu/owa

Preview new intranet interface http://preview/sites/citruscollegeintranet/

NEW LOGIN LINKS FOR ACCESSING BANNER

This login will use your network credentials, instead of the previous Banner username and password.

Wingspan SSB Single Sign On (PROD)

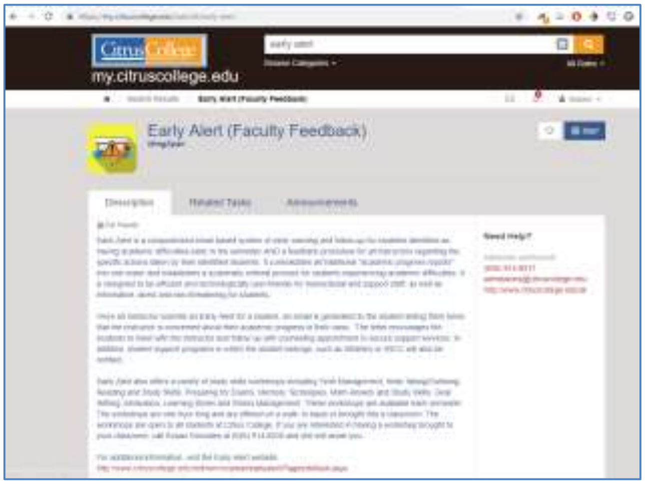
Wingspan 9 Admin Pages (PROD)

Now that we have an updated website and portal, the Citrus College Intranet (https://intranet.citruscollege.edu) is undergoing a facelift.

We've upgraded the Intranet to use newer technology and included graphics similar to the my.citruscollege.edu portal to improve usability.

We've been testing this for several weeks, and you may have already clicked on the 'preview' link on the current Intranet. The new version of the Intranet will not only be more stable and secure, but will provide staff and faculty with more tools for working in teams and collaborating on documents. The new Intranet will be live beginning **Monday, March 18.**

Early Alert in WingSpan



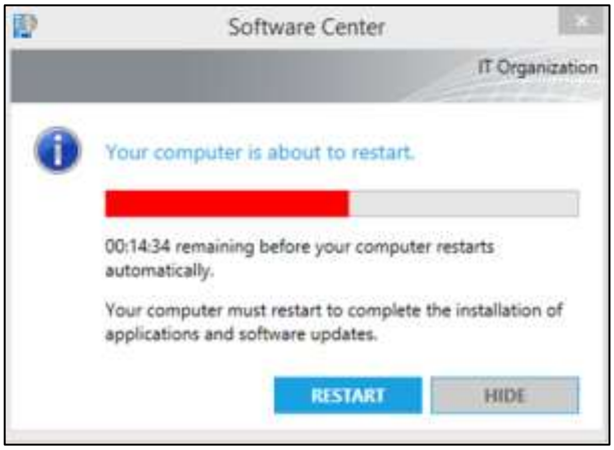
TeCS has partnered with staff and faculty in Counseling, and Admissions and Records to launch a pilot of Faculty Feedback (aka Early Alert) in WingSpan.

Faculty interested in participating in the pilot can log in to Early Alert via the my.citruscollege.edu portal (shown here). After logging in to WingSpan (using your network login), you will be taken to a roster of the classes you are teaching, where you can identify issues that a student may be having and/or recommendations for additional services, such as tutoring or counseling.

This generates automated communications to students via e-mail, and provides reports to service areas for special populations. The goal of this pilot is to make it easier for faculty to provide feedback and improve participation in the Early Alert process, with the ultimate goal of improving student success.

Windows Updates

In an effort to keep campus computers secure and up to date, TeCS periodically releases updates to your computer. Once installed your computer may need to be rebooted and a pop up window such as the one illustrated at right may appear. If this message appears, don't be alarmed! Simply save what you are doing, close out all programs and restart your computer at your earliest convenience. Your computer will automatically restart after 2 hours if no action is taken. You may resume normal operations once your computer is restarted.



Your computer is about to restart.

00:14:34 remaining before your computer restarts automatically.

Your computer must restart to complete the installation of applications and software updates.

Citrus Alert and Citrus Guardian

Citrus College will conduct an emergency drill during the evening hours of Thursday, March 21. If you haven't done so already, this would be a good time to sign up for *Citrus Alerts*. Confirm your emergency contact information today at https://my.citruscollege.edu/task/all/citrus-alert-emergency-notifications.

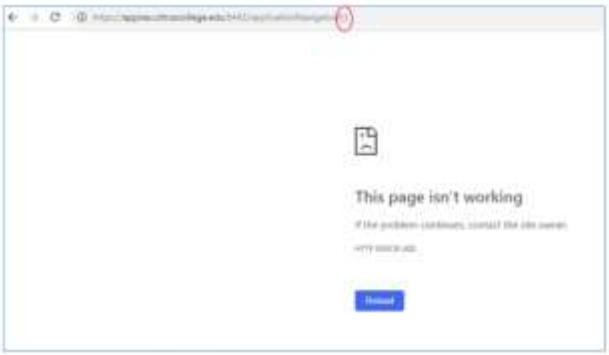
The *Citrus Guardian App* is another important tool that you can use during an emergency to help keep you safe on campus. Some of the features include notifications from Citrus Alert, a phone directory of important numbers, confidential tip submission, and an emergency call button.

Learn more about the *Citrus Guardian App* and how to download it at http://www.citruscollege.edu/campussafety/Documents/GuardianApp.pdf

Banner 9 Troubleshooting and Training

The Citrus College Staff deserve a big "Thank You" for their persistence and patience learning the new Banner 9 interface in WingSpan. The TeCS staff is still troubleshooting some pesky login and timeout issues, and we hope to have them resolved soon.

Tip 1: If you ever experience the screen with the message "This page isn't working" when you try to log in to Banner 9 using the Google Chrome browser, look at the address line. If you see a colon between two brackets **[:]** (circled in the image on the right), put your curser at the end of the address and press delete three times, removing the **[:]** from the address. This will typically launch Banner normally. We're working with our vendor (Ellucian) to figure out why this is happening.



This page isn't working

Tip 2: We're used to clicking on the 'back' button of our web browser when we are surfing the web. But clicking the 'back' button on your browser can cause you to lose your session when you are working in Banner 9. Don't click the 'back' button! Instead, use the controls in Banner 9, such as the *Recently Opened* folder in the toggle menu on the left to return to a previous page.

TeCS is continuing to offer **additional training sessions** on Banner 9 for staff. Training sessions will be available on Friday, March 15 from 9 am – 10 am; Thursday, March 21 from 3:30 pm – 4:30 pm; and Friday, March 29 from 9 am – 10 am. These are open lab sessions where we can cover any topic, such as how to enter a requisition in Banner 9. Sign up at http://tinyurl.com/tecs-training.

Security Matters – Take Control of your Personal Information to Help Prevent Identity Theft

Identity theft has become a fact of life during the past decade. If you are reading this, it is a safe bet that your data has been breached in at least one incident. Does that mean we are all helpless? Thankfully, no. There is a lot we can do to protect ourselves from identity theft and to make recovery from cyber incidents quicker and less painful.

First, take control of your credit reports. Examine your own report at each of the "big three" bureaus. You get one free report from each credit bureau once per year. You can request them by going to **AnnualCreditReport.com**. Make sure there's nothing inaccurate in those reports, and file for correction if needed.

Next, practice good digital hygiene. Just as you lock your front door when you leave home and your car when you park it, make sure your digital world is secured. This means:

1. **Keep your operating system up to date.** When OS updates are released, they correct errors in the code that could let the bad guys in.

2. **Update the application software you use.** Web browsers, plug-ins, email clients, office software, antivirus/antimalware, and every other type of software has flaws. When those flaws are corrected, you are in a race to install that correction before someone uses the flaw against you. The vast majority of hacks leverage vulnerabilities that have a correction already available.

3. **Engage your brain.** Think before you click. Think before you disclose personal information in a web form or over the phone.

4. **Think before you share on social media sites.** Some of those fun-to-share-with-your-friend quizzes and games ask questions that have a disturbing similarity to "security questions" that can be used to recover your account. Do you want the answers to your security questions to be published to the world?

5. **Use a password manager** and keep a strong, unique password for every site or service you use. That way a breach on one site won't open you up to fraud at other sites.

6. **Back it up.** What do you do if you are hit with a ransomware attack? (Or a run-of-the-mill disk failure?) If you have a recent off-line backup, your data are safe, and you can recover without even thinking about paying a ransom.

7. **Full disk encryption is your friend.** If your device is stolen, it will be a lot harder for a thief to access your data, which means you can sleep at night.

8. **Check all your accounts statements regularly.** Paperless statements are convenient in the digital age. But it is easy to forget to check infrequently used accounts such as a health savings account. Make a recurring calendar reminder to check every account for activity that you don't recognize.

9. **Manage those old-style paper statements.** Don't just throw them in the trash or the recycle bin. Shred them with a cross-cut shredder. Or burn them. Or do both. Data stolen from a dumpster are just as useful as data stolen from a website.

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