Citrus College eMEMO

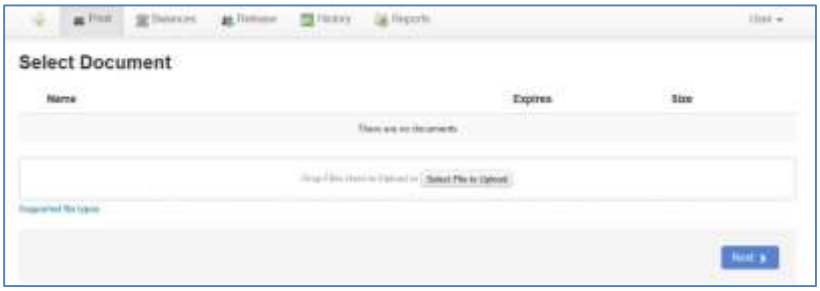
CITRUS COMMUNITY COLLEGE DISTRICT 1000 W. Foothill Blvd., Glendora, CA 91741-1899

Technology and Computer Services (TeCS) Update

July 2018

Wireless Printing in the Library

Students, staff and faculty can now print directly from their mobile devices (phones, tablets and laptops) to select printers in the Haugh Memorial Library. Simply log in to the Citrus College Wireless Network (cc-ap) on your mobile device and go to https://my.citruscollege.edu/task/all/wireless-printing-library to see the step-by-step instructions. Special thanks go to IT Support Specialist Brian Cherry for his work in configuring this feature.



EOP&S Online Application

A new online application form has been created for Extended Opportunity Programs and Services (EOP&S). The online application will streamline the process by eliminating paper; reduces the amount of duplicate information requested of applicants; and eliminates a significant amount of data entry work for EOP&S staff.

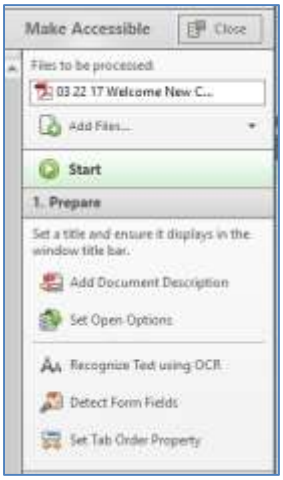
In developing this application, our programmer Bryun Sakaye has created a framework that can be used to more quickly develop additional online applications for use by our students. An online application for the Honors program is coming soon.

Electronic Financial Aid Disbursements

The BankMobile Disbursements project is getting ready for production. Students who are enrolled in classes for Fall 2018 and who have applied for financial aid will be receiving a bright green envelope in the mail beginning July 27. This envelope contains instructions on how students can select their preferred method of receiving an electronic financial aid disbursement – either through a direct deposit to their existing bank account, or to a BankMobile Vibe account.

The BankMobile Vibe account provides the student with a debit MasterCard which can be used to obtain cash without fees at any of 55,000 Allpoint ATM machines. Programmer Robert Coutts has played a key role in this project by developing the automated processes to transfer data from Citrus College to BankMobile.

Creating Accessible PDF documents



Technology and Computer Services has developed a new class to help Citrus College improve our compliance with the California Community College accessibility standard. Content on our website must provide individuals with disabilities "…the opportunity to acquire the same information, engage in the same interactions, and enjoy the same services as a person without a disability in an equally effective and equally integrated manner, with substantially equivalent ease of use."

A significant portion of the content on the Citrus College website is in the form of PDF documents, which often fail to meet standards for accessibility.

Fortunately, Adobe has created an easy to use, step by step wizard that can guide content creators through the process of making their document accessible. Classes on creating Accessible PDF Documents will be held on July 23 and August 6 from 2 pm – 3 pm in IS 109. Additional classes will be held in the future. RSVP at http://tinyurl.com/tecs-training.

Banner Upgrade Sundays

Our Banner Enterprise Resource Planning (ERP) system is in need of some software upgrades. While some of the modules (like Financial Aid) are relatively current with the latest releases, we have other modules that are in some cases several years behind the latest versions. By applying these upgrades, we can avoid encountering known software defects and prepare our system for the significant upgrade to Banner 9, which we hope to begin installing later this year. In order to minimize impact to the college, these upgrades will be installed the mornings of July 22, July 29 and August 5.

Security Matters

What Is Ransomware?
Ransomware is a type of malicious software that encrypts your files. Often, the only way to decrypt and gain access to the files is by paying a "ransom" or fee to the attackers. Ransomware may spread to any shared networks or drives to which your devices are connected.

How Can I Get Infected with Ransomware?
Common vectors for ransomware attacks include e-mails with malicious attachments or links to malicious websites. It's also possible to get an infection through instant messaging or texts with malicious links. Antivirus may or may not detect a malicious attachment, so it's important for you to be vigilant.

How Can I Protect Myself Against Ransomware?
There are two steps to protection against ransomware:

- *Preparation*. Back up your information regularly. Once a ransomware infection occurs, it's often too late to recover the encrypted information. Your research project or other important information may be lost permanently.

- *Identification.* Ransomware typically appears as phishing e-mails, either with links to malicious websites or infected files attached. You might also see a ransomware attack perpetrated through a pop-up telling you that your computer is infected and asking you to click for a free scan. Another possible vector is malvertising, malicious advertising on an otherwise legitimate website.

Probably the Most Important Steps You Can Take to Prepare…

- Ensure that your information is backed up regularly and properly. Because ransomware can encrypt the files on your computer and any connected drives (potentially including connected cloud drives such as Dropbox), it's important to back up your files regularly to a location that you're not continuously connected to.
- Ensure that you're able to restore files from your backups. Again, work with your IT support personnel to discuss how to test restore capabilities.
- Ensure that you're keeping your system (and mobile devices) up to date with patches. If you're prompted by your computer or mobile device to accept updates, accept them at your earliest convenience.
- Don't do day-to-day work using an administrator account. A successful ransomware attack will have the same permissions that you have when working. (If you're not using an account with administrator privileges, the initial attack may be foiled.)

What Do I Do If I Think I'm Infected?

- Report the ransomware attack to your service desk immediately.
- Isolate or shut down the infected computer. (If you're on Wi-Fi, turn off the Wi-Fi. If you're plugged into the network, unplug the computer. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or shared drives.)

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