

IT@UCSF news for January 2012

I am pleased to let you know about a few exciting improvements to the UCSF IT services which will enhance your productivity and make your work life a bit easier.

Single Sign-On for HBS: as of today, you can log in to HBS, our timekeeping system, via MyAccess (<http://myaccess.ucsf.edu/>), the UCSF Single Sign-On service. You will no longer need to use a separate username and password for HBS! Please note: this is not applicable for WebClock users.

MyAccess Favorites: it's easier than ever to log into the applications you access most. When you log into MyAccess, you now see just the applications you have marked as favorites. You can always click on "All Apps" at the top of the MyAccess screen to view the entire application list. With MyAccess you can use all Single Sign-On applications with your Active Directory username and password (often used for workstation or email log in).

UCSF Mobile app version 2.0: a new iPhone and Android version of the UCSF Mobile App is now available. New features include: save most recent trips in Shuttles, faculty research interests, including publications and photo, in Directory, Google Streetview in Maps, SFGH and Mt. Zion added to Maps, Academic events added to Calendars, new Social Media icon, and more. Current iPhone users of this app can get the update directly from the App Store. Current Android users need to uninstall the old version before installing the new one (future upgrades will not require this extra step).

WiFi on shuttle buses: wireless internet access for your laptop or mobile device is now available as a pilot program on three UCSF GREY shuttles that travel non-stop between Parnassus and Mission Bay. Look for the wireless signal labeled "UCSF Transportation FREE WIFI." Transportation Services reminds staff, faculty and students to use discretion when viewing sensitive and confidential content on our shared use shuttles. This project was made possible via a collaboration between ITS and Transportation Services.

Reducing unnecessary email: many of us receive daily email messages sent via a handy mechanism known as "listserv" - we sometimes wonder why we received such messages and wish that we had the option to decline them. The offices of the Executive Vice Chancellor and Provost, Senior Vice Chancellor, and ITS have been working together to facilitate adequate communication with our campus while reducing the amount of unnecessary and repetitive email. We recently completed an inventory of at-will lists and reduced them by 40%. Also, in order to provide you more control, messages sent to members of such lists will soon include an opt-out prompt. Please refer to <http://its.ucsf.edu/main/1901-DSY.html> for guidelines and process information.

Do I need to encrypt my laptop? the short answer is yes. Lost and stolen devices are the leading cause of data and privacy breaches costing, on average, \$2 million per incident. The way to eliminate this risk is to encrypt your computers as required for devices used for UCSF business. Instructions on how to get and install the PGP encryption software (Windows and Mac) are at: [http://its.ucsf.edu/EIS/services\\_products/PGP.html](http://its.ucsf.edu/EIS/services_products/PGP.html)

Mac Lion tip: if you are using the Mac Lion operating system, have you noticed that some applications (e.g., Excel, Word) automatically launch the last document you were working on? If you don't like this feature, you can turn it off: go to System Preferences/General and uncheck the "Restore windows when quitting and re-opening apps" checkbox.

I hope that the above information is useful to you. If you have any questions or experience any problems please contact the UCSF Service Desk at: [ITServiceDesk@ucsf.edu](mailto:ITServiceDesk@ucsf.edu), <http://ucsf.service-now.com/ess/>, or (415) 514-4100. And, as always, feel free to contact me directly at: [elazar.harel@ucsf.edu](mailto:elazar.harel@ucsf.edu) or (415) 476-8434.

Thank you.

Elazar C. Harel, Ph.D.  
Vice Chancellor, Information Technology