CURSOR

IN THIS EDITION
UNIFIED COMMUNICATIONS UPDATES
MULTI-FACTOR AUTHENTICATION
AVOID SOCIAL ENGINEERING AND PHISHING SCAMS
RANGOS AV UPGRADES

PLUS
• EL CAPITAN, WINDOWS 10 SUPPORT
• OFFICE 2016
• DIGITAL ACCESSIBILITY: TIPS WHEN CREATING CONTENT
• PROTECTING INSTITUTIONAL DATA
Computing Services Vision
Computing Services will meet the changing needs of Carnegie Mellon by combining the best of industry-standard information technology services, innovative solutions and best practices.

Computing Services Mission
Computing Services enables and advances an information technology environment that supports the research and education missions and the associated administrative functions of Carnegie Mellon.

Carnegie Mellon University
Computing Services

XFINITY On Campus

XFINITY On Campus is an IPTV service from Comcast delivered through CMU's network.

XFINITY On Campus is available to the main campus student community. Anytime on campus, whether wired or wireless, XFINITY On Campus delivers what you want to watch, when you want to watch it.

For more information visit cmu.edu/computing/phone-tv/cable-tv/stream.html.
For the past two years, Computing Services has been converting the campus community from the existing Centrex phone system to the Unified Communications (UC) service. This service provides an enhanced suite of features, including:

- Video/non-video calling options
- Multiple simultaneously active calls
- Conferencing directly from the phone
- Location-specific 911 dialing
- Integrated instant messaging
- Voicemail-in-email (for individuals using Outlook clients with the Computing Services Exchange email service)

As of December 2015, the UC team has converted more than half of all campus phone lines and expects to complete the conversion in the next 18 months.

The UC service is licensed-based, meaning that each licensed individual is provided a desk phone with a unique line number, along with the integrated services on their work machine and mobile devices. An individual can place or receive calls on their phone or choose to manage calls on their mobile device through the CMU Jabber Client (along with instant messaging and voicemail).

Since CMU owns and manages its own network, features that were previously itemized in the cost model have been streamlined into the line charge for the UC services (e.g., voicemail).
The monthly fee for a user license now includes:

- Phone Set
- Phone Set maintenance
- All calling features
- All local and domestic long distance calls
- Voicemail-to-email integration
- Jabber client provisioning.
- International calling is available but remains a ‘per call’ charge.

For more information about the UC service visit [cmu.edu/computing/phone-tv/uc/](http://cmu.edu/computing/phone-tv/uc/) or for support, email [tc-help@cmu.edu](mailto:tc-help@cmu.edu).

### PHYSICAL SPACES CONVERTED

<table>
<thead>
<tr>
<th></th>
<th>TOTAL TO DATE</th>
<th>TOTAL IN MOST RECENT PORTING GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUILDINGS</td>
<td>32/58</td>
<td>17</td>
</tr>
<tr>
<td>ORGANIZATIONS</td>
<td>188/311</td>
<td>93</td>
</tr>
<tr>
<td>DEPARTMENTS</td>
<td>71/99</td>
<td>25</td>
</tr>
</tbody>
</table>

**TOTAL TO DATE**: 32/58  
**TOTAL IN MOST RECENT PORTING GROUP**: 17  
**TOTAL TO DATE**: 188/311  
**TOTAL IN MOST RECENT PORTING GROUP**: 93  
**TOTAL TO DATE**: 71/99  
**TOTAL IN MOST RECENT PORTING GROUP**: 25
Computing Services is currently planning to expand and enhance the Multi-Factor Authentication service. This effort will be released in a phased approach by first transitioning to a different vendor (Duo Security) coming in 2016. Once the Duo Security infrastructure is in place individuals currently using One Time Password tokens will be transitioned to the new Multi-Factor service, and finally the service will be extended to other individuals and services across campus.

Multi-factor authentication is a service that provides a second layer of protection to an individual’s digital identity, as well as adding protection to data, systems, and services. Sometimes a password is not enough to protect sensitive and/or restricted data. Because of this, multi-factor authentication may be requested to access certain systems and applications on campus.

The first level (something you know) is the verification of your Andrew userID and password, and the second level (something you have) is generally a smartphone, but other options are available.

**BENEFITS**

- Only authorized users can gain access to critical information
- No hardware for system administrators to deploy and manage; the service will be provided by Duo Security a cloud-based two-factor authentication service (partnered with InCommon)

If you currently use One Time Password tokens, you will be contacted with further information and details about transitioning.

If you are an application owner, please contact it-help@cmu.edu if you are interested in the additional access security offered by this service and want more information.
Protecting Institutional Data

Carnegie Mellon University has over 13,200 students and 5,000 faculty and staff. With so many employees and students, it is likely people will shift job responsibilities, leave their position, or graduate. When these changes occur, access to resources no longer required should be removed. This practice is known as deprovisioning and is key to protecting institutional data.

Supervisors should keep a list of resources that employees and students have been authorized to access; and inform system and application managers to deprovision the account or group of affiliated accounts (faculty, staff, students, alumni) when access is no longer authorized.

CONSIDER THE FOLLOWING:

- Shared service or system passwords – change immediately
- Shared mailboxes and calendars
- Mailman or other mailing lists
- Shared server drives (e.g., MyDeptFiles)
- Group membership (e.g., Grouper, LDAP, Windows, Andrew PTS)
- Research databases
- University web site content through the Content Management System (CMS) or Andrew Web Publishing System (AWPS)
- Shared Social Networking accounts (e.g., Twitter, Facebook, etc.)
- Third-party managed applications (e.g., Google Accounts)

There are automated processes that deprovision Andrew accounts upon separation from the University, however, you should not rely on university-driven disabling of the Andrew account alone to remove access to services for which you are responsible.

Unauthorized access could negatively affect the University or cause a disclosure of sensitive institutional data. System and application managers should take the necessary precautions when responsibilities shift or roles change. Another layer of security might be added by considering authorization of individuals or specific populations rather than relying solely on authentication at the broader affiliation level (faculty, staff, student, alumni).

For more information review the Guidelines for Data Protection at cmu.edu/iso/governance/guidelines/data-protection/.
Computing Services cluster reservations are managed by the University Registrar’s Office through SpaceQuest (25Live). Faculty or staff may reserve a cluster for an academic or professional development class; and students for community service projects. Credit-bearing classes receive first priority.

There is an extensive selection of software in cluster locations that should meet most customer needs. Faculty and staff may request software that is not on the cluster software list by emailing it-help@cmu.edu.

To view a detailed software list along with reservation guidelines, visit cmu.edu/computing/clusters/reserve/.

OTHER CLUSTERS

Gates-Hillman clusters and the Margaret Morrison Music Technology Center cannot be reserved through SpaceQuest (25Live). Reservations for these rooms are made through the department see cmu.edu/computing/clusters/reserve/ for a contact list.
Computing Services has updated audio-visual equipment in Rangos Ballroom to reflect current and popular features based on input from various campus groups. If you are looking for a space to host your event, Rangos has a lot of new features to offer – all available for full-service!

WHAT’S NEW?

• On top of a more powerful stage projector, three new projectors have been added and strategically placed for full ballroom or partitioned configurations (Rangos 1, 2, 3).
• The addition of three resident screens along with corresponding projectors strategically placed to support partitioned ballroom configurations.
• Connections to add optional LCD displays throughout.
• Ability to project to individual or multiple screens using one or more inputs. Project from one device to all or specific screens OR use multiple devices to project to individual screens.
• All updated digital connections.
• More speakers and the addition of subwoofers provide better coverage to give a fuller audio experience for a large venue or for individually partitioned spaces.

The placement of updated resident equipment in the ballroom positions Computing Services to offer a self-service option in the future. Stay tuned to Computing News for an update in the coming months (cmu.edu/computing/news/).

Want to schedule your event in Rangos? Reserve it now using SpaceQuest (25Live) at https://25live.collegenet.com/cmu/.
Course Capture Update

Working together with our campus partners: Eberly Center for Teaching and Learning, Heinz, Tepper, Information Networking Institute and Institute for Software Research the course capture pilot was extended through the fall semester. The additional time enabled us to gather more information on the course capture models:

- The active model using Camtasia Studio, where instructors create their own instructional videos through a suite of laptop tools.
- The passive model using Panopto and MediaSite, where existing video conferencing equipment is leveraged to capture a classroom lecture.

Both provide faculty with options for saving and delivering their courses. Stay tuned for a service decision during the Spring 2016 semester.

What will you learn today?

LOG INTO cmu.edu/lynda/

Lynda.com is a continually growing and evolving library of training videos and tutorials covering a wide range of software, technologies and business topics.
UPDATE ON OS SUPPORT

After evaluating our core software and services for compatibility, Computing Services announced support of Windows 10 in October with some exceptions and Mac OS X 10.11 (El Capitan) in December.

WINDOWS 10

Students can download Windows 10 free of charge through DreamSpark (cmu.edu/computing/dreamspark/). Faculty and staff should contact their departmental IT administrator to obtain Windows 10 for university-owned equipment.

You’ll find the support statement, licensing information and exceptions list for Windows 10 at cmu.edu/computing/software/all/windows/.

OS X 10.11 EL CAPITAN

The El Capitan operating system is available as a free upgrade to anyone with compatible hardware through the Mac app store. For information on how to upgrade, visit the Apple site at apple.com/osx/how-to-upgrade/.

With support of El Capitan, support for Mac OS X 10.9 (Mavericks) will end on May 31, 2016.

To review the El Capitan support statement visit cmu.edu/computing/software/all/mac/.

Free training is available for both operating systems through cmu.edu/lynda/ and the FocusU learning management system (cmu.edu/hr/professional-development/).

OFFICE 2016 AVAILABLE TO CAMPUS

Microsoft released Office 2016 for Windows and Mac in September. This was a long anticipated release for the Mac community who has not seen an Office update since 2011.

Since the release, Computing Services has tested our email services for compatibility with Office and is happy to announce support for Outlook 2016. Other office applications are supported on a best effort basis.

With the availability and support of Outlook 2016, we will discontinue support of Outlook 2010 for Windows on June 30, 2016. Those who are running Outlook 2010 are encouraged to upgrade.

• Faculty and staff are licensed to use Microsoft Office 2016 on University owned equipment. Additionally, faculty and staff are eligible to install one copy of Office 2016 on a personal computer via the “Home Rights” clause of our campus agreement. Contact your DSP consultant, IT department administrator or email software@andrew.cmu.edu for more information.

You will find campus licensing details at cmu.edu/computing/software/all/ms-office/.

TRAINING AND DOCUMENTATION

• Steps to setup your Carnegie Mellon email with Outlook 2016 are available at cmu.edu/computing/email/.
• Free training is available to all university affiliates through cmu.edu/lynda/.
• Get started quickly with one of Microsoft’s Quick Start guides at support.office.com/.

BEFORE YOU UPGRADE

As always, Computing Services recommends checking with your departmental IT administrator or DSP consultant before upgrading your operating system.
Keep Accessibility in Mind When Creating New Content

Knowing how to incorporate accessibility with your content at the time of creation will ensure key factors are ingrained in it from the start. Whether you’re building a web page or creating a document in Microsoft Word or Adobe InDesign, be sure to incorporate these basic elements:

- Structure your content using appropriate heading and paragraph tags
- Provide an alternate description for any image that is used to convey meaning
- When providing links, avoid using generic phrases such as “click here”; instead, use relevant keywords relating to the link

Digital accessibility doesn’t stop at the basics. The more accessible you can make your web pages and electronic documents, the better. Further guidance on accessibility can be found at cmu.edu/cms/best-practices/web-accessibility/ including a link to the Web Accessibility Evaluation Tool as well as a playlist of video tutorials on lynda.com.

Remember, accessibility not only benefits those with disabilities, but improves the overall experience for everyone. For information regarding digital accessibility, visit cmu.edu/hr/eos/disability/digital.html.

WANT MORE STORIES LIKE THIS?
SUBSCRIBE TO OUR FEEDS.

The Computing News RSS feeds brings you the latest news and feature stories.

To subscribe, visit cmu.edu/computing/news/getnews/how.html
Identity Finder version 8.1 is now available for both Windows and Mac operating systems. The software manages and protects sensitive data to prevent Identity Theft. Faculty, staff and students can download the software at no cost through the University license.

The updated version (8.1) identifies and highlights sensitive data stored in documents, applications, email and browsers. Once you install and run Identity Finder, the tool will:

- Search documents, files and browser data for possible unprotected Personally Identifiable Information (PII), which includes Social Security Numbers (SSN), credit cards, passwords, driver license number, and state ID or passport number.
- Manage search results by allowing you to determine the most effective and secure way to handle data. Review the identified information and choose to:
  - Shred to securely delete a document
  - Scrub by overwriting sensitive data with zeros or x’s while leaving the rest of the file unchanged
  - Secure by password protecting a document

Protect data by storing documents in a secure location, encrypting or password protecting documents containing sensitive information.

If you are currently running Identity Finder, do not uninstall it prior to installing version 8.1. This will preserve your settings and password vault. Desktop Support Program (DSP) clients should contact DSP to install or upgrade the software.

For more information on installing, running and using Identity Finder visit cmu.edu/computing/software/all/identity/.

Avoid Social Engineering and Phishing Scams

Social engineering and phishing scams are common as we become more dependent on our devices. Last year, social engineering by phone and phishing through email attempted to trick campus affiliates into sharing their credentials or personal information. It is important to recognize these scams to avoid falling victim to these attacks.

Social engineering relies on social skills to trick others into sharing credentials or personal information. In these scams, an attacker impersonates a representative asking questions to piece together the necessary information to gain access to your account or an organization’s network.

Phishing is a form of social engineering where an email, instant message or malicious website appears to be legitimate and from a reputable company. You are urged to take action. Personally identifiable information (PII) is solicited including: username, password, social security number, credit card or banking information.

Many schools continue to experience such scams. Impersonating Human Resources or other university offices, these emails direct unsuspecting recipients to fraudulent log in pages. If the recipient unknowingly logs in through the fraudulent page, the attacker captures their username and password giving them access to Workday and other institutional systems.

To avoid these scams, the Information Security Office (ISO) reminds you to:

- Never send your Andrew userID or password or other confidential information in response to an email. A request to do so is most likely phishing and an attempt to lure you into providing your Andrew credentials.
• Think twice before opening an attachment or clicking a link from an email, instant message or untrusted website. Attachments in unexpected messages or from unknown senders often harbor malware that could infect your computer. Fraudulent websites can lure you into providing your log in credentials. Check the URL before you provide your credentials. For example, “https://login.cmu.edu” is the URL for Web Login at Carnegie Mellon.

• Do not provide sensitive information over the phone. If you receive a phone call asking you to verify a computer or printer IP address or requesting staff member information, simply end the call.

• Run Identity Finder to find and remove personally identifiable information from your university and home computers. For more information about Identity Finder visit cmu.edu/computing/security/idfinder/

• Promptly report security concerns to the ISO (iso-ir@andrew.cmu.edu or 412-268-2044). If you suspect your computer has been compromised, follow the procedure for responding to a compromised computer at cmu.edu/iso/governance/procedures/compromised-computer.html

• Take Security 101 training (cmu.edu/iso/aware/security101/) and learn how to recognize a phishing email.

COPYRIGHT & INTELLECTUAL PROPERTY LAWS

Carnegie Mellon is committed to the protection of intellectual property and copyrights. Illegal copying of creative works such as music, videos, images and text can subject the individual offender to both civil and criminal penalties. The University takes a strong stance against violations of copyright law (e.g., disciplinary action, loss of network connectivity) and also supports fair use of creative works.

For more information, see:

• University’s Copyright Policy - cmu.edu/policies/documents/Copyright.html
• Copyright Violation Guidelines - cmu.edu/iso/governance/guidelines/copyright-memo.html
• Digital Copyright and DMCA - cmu.edu/iso/aware/dmca/

STAY ALERT

The ISO periodically runs phishing campaigns to help community members recognize phishing attempts. Each campaign sends an email that mimics a real world phish and a short training message for individuals who click the email attachment or link.

If you suspect an email is a phishing, forward it to iso-ir@andrew.cmu.edu include any attachments and the message headers. Headers are usually hidden. To view the header information, follow the steps at cmu.edu/iso/aware/email-headers.html.

NEVER SHARE OR REPURPOSE YOUR ANDREW PASSWORD!

The Information Security Office (ISO) reminds you to never share your Andrew password or repurpose it for non-Carnegie Mellon services (e.g., Facebook, LinkedIn, Amazon, etc.). Now is a good time to change your Andrew password…new year, new password! For steps to change your Andrew account password see cmu.edu/computing/accounts/passwords/change.html.