IN THIS EDITION
NEW BOX WEB EXPERIENCE
STAY SECURE WITH TWO-FACTOR AUTHENTICATION
INBOX BY GMAIL AND G SUITE
LEASE IT - TECHNOLOGY WITHIN REACH

PLUS
• CAMPUS CLOUD PLUS
• UPDATES TO CLASSROOMS AND TECHNOLOGY ENHANCED SPACES
• ISO CORNER
• AND MORE!

SPRING 2017


NEW BOX WEB EXPERIENCE

Box recently announced a new and improved, more personalized web experience. The new experience makes finding, moving, and viewing files much easier with options like:

- a more effective search
- cut and paste of files
- favorites on your home page
- ability to view HD videos and 360 images
- annotate files without opening them (coming soon)

Visit box.cmu.edu/ and click "Try it Out," to begin using the new Box experience. You can switch back to the old interface any time before the final transition in late spring 2017. Stay tuned to Computing News for final transition dates.

Learn More!

Watch the "Introducing the All New Box Experience" video at cloud.app.box.com/v/newboxexperience/ to learn more about the new options.
Passwords are not foolproof and, in today's world, they don't provide the security we need to protect our information and resources. Two-Factor Authentication takes security a step further and makes it that much more difficult for a hacker to steal your information.

The number of phishing campaigns has nearly doubled between 2015 and 2016 (see the numbers from the Email Service Enhancements Change Phish and Malware Processing article on page 4). Newer attacks are often more convincing, making them more difficult to detect. People are also much busier than they have been in the past and frequently use mobile devices with much smaller screens, all of which contributes to making the detection of malicious email more difficult.

Two-Factor Authentication (2fa) is a service that provides a second layer of protection to your digital identity, as well as adding protection to data, systems, and services. To provide this added security, Computing Services recently announced the Two-Factor Authentication service enabled through Duo.

**HOW DOES 2FA WORK?**

You may already be using 2fa through popular social media sites or through your bank. Any time you are providing a secondary token along with your password, you are using 2fa!

If you elect to opt-in to the 2fa service, you will be prompted for two forms of identification when you access Web Login protected services: *something you know* (Andrew UserID and password) and *something you have* (a code on your smartphone).

**HOW DO I REGISTER FOR 2FA?**

Visit the 2fa Self-Service Registration page at [http://2fa.cmu.edu/](http://2fa.cmu.edu/) to register for the service and start using 2fa with your smartphone to protect your identity and university data. Return to the 2fa Self-Service page to register a new device (e.g. iPad, Kindle) or manage an existing device.

For more information, see the Two-Factor Authentication (2fa) pages at [cmu.edu/computing/2fa/](http://cmu.edu/computing/2fa/).

**Most Common Example of 2fa - Automated Teller Machine**

You insert your bank card  
(SOMETHING YOU HAVE)  

Then you provide your PIN  
(SOMETHING YOU KNOW)  

You receive money  
(ACCESS)
Over the last few years, suspicious email messages have been on the rise. These messages are often laden with phishing attacks, attempting to trick users into submitting their credentials to fake websites, or with malware, usually an attachment that will install unwanted and potentially harmful software when it is opened. In addition to there simply being more malicious email messages being sent, they are often much more sophisticated or look more realistic, making it much easier for even a savvy recipient to fall victim.

The number of phishing campaigns has nearly doubled between 2015 and 2016. Newer attacks are often more convincing, making them more difficult to detect. People are also much busier than they have been in the past and are often using mobile devices with much smaller screens, all of which contributes to making the detection of malicious email more difficult.

Recent developments in email systems managed by Computing Services now allow us to sort through the flood of malicious email by removing particularly blatant messages from our mailboxes. By deleting the message before the user gets a chance to see it, we’re hoping to reduce the chance that someone will fall victim.

**How Does It Work?**

The Information Security Office (ISO) will determine which high-priority malicious messages should be deleted. Priority is based on a number of factors, including how dangerous, widespread, and well-crafted the message is. Once the ISO makes the decision to delete the message, it is then examined for criteria that will allow it to be uniquely identified. The ISO uses the criteria to find and delete similar messages from mailboxes on Computing Services Exchange, G Suite, and Cyrus email servers. Email forwarded to non-Computing Services email systems will not be impacted by this process change.

**Privacy Concerns**

Because privacy is important, the ISO has built assurances into the process for deleting malicious email:

1. The identification and deletion of malicious email messages will always be done by automated processes – no individual will read any individual's email as part of this process.
2. Once a message has been identified and deleted, the account holder will be notified, informing them which message was deleted and why.

**Phishing: A Comparison Between 2015 and 2016**

Note: Data does not include December for either year. Data for those months were not available at the time of the chart’s creation.

<table>
<thead>
<tr>
<th>Year</th>
<th>Total Campaigns</th>
<th>Total Addresses</th>
<th>Total Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>42</td>
<td>15,148</td>
<td>47</td>
</tr>
<tr>
<td>2016</td>
<td>216</td>
<td>68,359</td>
<td>151</td>
</tr>
<tr>
<td>% Increase</td>
<td>Over 400%</td>
<td>Over 350%</td>
<td>Over 200%</td>
</tr>
</tbody>
</table>

Direct questions or comments regarding this change to the Information Security Office (iso-ir@andrew.cmu.edu or 412.268.2044).
The name Google Apps didn’t quite capture the suite of products offered. So, late last year Google Apps was renamed G Suite. Everything is “all together now.”

According to Google, “the new name better reflects our mission to help people everywhere work and innovate together.” G Suite is considered an “all-in-one solution” offering Gmail, Docs, Drive, Calendar and more. For those using Google Apps at CMU, the change to G Suite was seamless.

Inbox is a new Gmail experience that helps you keep your email organized. Promotional, purchase and travel emails are automatically sorted into “bundles.” Or, you can create your own bundles to organize messages. Other features include:

- **Reminders** – add a “to-do” to your inbox
- **Snooze** – hide an email until later
- **Photos at a Glance** – view photos and videos without opening the message

Released to campus in December, those with Google can take advantage of these new features now at inbox.google.com or through the inbox mobile app.

Gmail and Inbox stay in sync, so what you do in one carries over to the other. To return to the old Gmail interface, access your email through email.cmu.edu/. Keep in mind, Inbox works best when you use it consistently.

For more information on the available features and how Inbox works with Gmail, visit google.cmu.edu/.
During the fall 2016 semester, Computing Services worked closely with department volunteers to evaluate interest and value in a standardized laptop service. The feedback from these test participants has been instrumental in improving the overall service design that will be offered campus-wide. We thank the many who participated in this evaluation and we look forward to releasing the new Lease IT service later this year.

The Lease IT service will provide staff, faculty and departments with pre-configured, standardized and secure laptops, including a set of core business applications, features and services.

What are the benefits of Lease IT?

1. Lower equipment costs - yearly subscription model with 3-year warranty and device refresh cycle.
2. Standard and popular software titles including Windows 10 64-bit Enterprise OS.
3. Standardized hardware to enable more effective support through the Computing Services Help Center.
4. Encrypted hard drive for added protection in the event of loss or theft.
5. Up-to-date campus security standards.
6. Backed up system files for added protection and quicker recovery.

...and more!

How do I get Lease IT?

Computing Services will be offering Lease IT starting July, 2017 coinciding with hardware refresh. If your current machine is being refreshed next year, you could qualify to participate in the new Lease IT service. More information along with corresponding rates and terms, will be available in early spring. Any additional questions or interest can be directed to it-help@cmu.edu.
Porter Hall A19D was converted from a standard classroom to a collaborative, bring-your-own-device space. The room features student “pods,” each with a monitor to display student devices wirelessly or through HDMI. An instructor station offers the same presentation choices, as well as a ceiling-mounted document camera. The newly designed graphical user interface (GUI) for the AV equipment makes this space easy to use.

This flexible learning space fosters a collaborative learning environment and accommodates faculty and student interaction and engagement.

The room was made possible by the following donations:

- **Spectrum Furniture** – chairs, tables, pods and instructor station
- **Crestron** – audio visual equipment
- **WolfVision** – ceiling mounted document camera

Reservations can be made through 25Live.

The West Wing collaborative space was given a fresh coat of paint, new carpeting, lighting and furniture. You may notice the computers were rearranged to accommodate the new furnishings.

Additionally, the technology in the Gates Hillman Center classrooms 4101, 4102, 4211, 4215 and 5222 was refreshed over the winter break.

More information about these spaces as well as documentation for using the equipment is available at cmu.edu/computing/tes.
Campus Cloud is the foundation for Campus Cloud Plus. This new service, coming spring 2017, offers virtual servers and disk space with the added benefits of server administration and computer security at a cost-effective price.

Available to department IT staff, faculty and graduate students, the service comes standard with Platform as a Service (PaaS). PaaS includes a virtual server, disk space and server operating system administration for vendor-supported versions of Red Hat Enterprise Linux (RHEL) or Windows OS.

Additionally, customers have the option to utilize Database as a Service (DBaaS). This option supports SQL *Server, MySQL and Oracle relational databases.

Benefits to you:

- **Save money** – only pay for resources you need and leverage Computing Services’ volume pricing
- **Reduce risk** – on-site secure servers, behind the firewall.
- **Peace of mind** – server updates, security patches and maintenance are our responsibility
- **Save time** – reduce purchase, shipping and system administration time
- **Go green** – decrease power inefficiencies of standard hardware

This could be the virtual hosting solution for your next project. Consider Campus Cloud Plus if your department is evaluating options for IT applications, a sponsored graduate student project, web hosting, and other work that traditionally uses physical servers. Email campus-cloud@cmu.edu for additional information or a consultation.

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/
SCS FACILITIES INFRASTRUCTURE TEAM JOINS COMPUTING SERVICES TO STREAMLINE AND IMPROVE SERVICES

The Infrastructure Team from the School of Computer Science Facilities group has partnered with Computing Services to evaluate current technology efforts. This evaluation is being conducted with an eye toward reducing or eliminating duplicate infrastructure services and identifying opportunities for new services that may benefit SCS and the broader university community.

This collaboration seeks innovative solutions to share management of enterprise-level systems and leverage central technology services where it makes sense. When needed, central base services will be augmented with layered, locally targeted services to establish a collaborative service portfolio that serves the business needs of the SCS community.

To achieve these goals, the SCS Infrastructure team officially merged with the Computing Services organization. This integrated team has already identified service areas for consolidation (select email and network services) and new opportunities for joint development. One such opportunity is an SCS-aware implementation of the G Suite for Education service (formerly Google Apps for Education). This service enhancement will support SCS email alias lookup through G Suite and includes investigation of the potential to extend G Suite services to all of campus. Next steps will be the execution of these plans, identification of the next set of services for evaluation and on-going additions to a list of expanding opportunities.

RESIDENT RECORDING SERVICE REFINED THROUGH SCS-COMPUTING SERVICES COLLABORATION

Computing Services’ Media Services group partnered with the School of Computer Science through the fall 2016 semester to pilot a new resident recording service in the Gates Hillman Center Rashid Auditorium (GHC 4401).

Setup time for recorded events is frequently reduced to a 10-minute window due to back-to-back events and room availability. Because recording equipment is now a standard installation in the space, this service allows Media Services staff is able to accommodate more events by reducing setup time while still providing multi-camera live mix recordings and webcasts. The service also provides an expanded option for pre-scheduled recordings when fixed camera production is appropriate passing along additional cost savings because a technician is not required.

Because the implementation in Rashid Auditorium has provided a valuable service at significant cost savings to SCS, they decided to fund the installation of an additional resident recording space during winter break (GHC 6115). The collaboration with SCS has helped Computing Services to demonstrate the value to customers and develop a support model...
for the service. The resident recording service is scheduled for an additional planned pilot in GHC 4307 in spring 2017 as an initial test in registrar-controlled classrooms.

**WORKING WITH CAMPUS PARTNERS IN A COMMON SERVICE MANAGEMENT TOOL**

As Computing Services has gained experience and seen demonstrated value in the use of its ServiceNow service management tool, we’ve extended the service to include a few campus partners who needed a solution for managing their customer issues and requests.

The flexibility of the ServiceNow tool accommodates partner implementation with varying levels of customization. Managing support record work within the same tool eases the process of referring, escalating and sharing work across organizational boundaries. By using the same framework and processes as developed for Computing Services, our partners have a cost-effective option with minimal development time for entry. This model was recently deployed for the SPARCS Help Desk and CMU Qatar Campus Facilities groups. Under this option, there’s still room for customized notifications and limited visibility across organizational records but the interface framework and forms are identical. For situations where our existing frameworks are not appropriate, we can offer customized configurations at a higher cost.

Conversations are underway with a number of campus academic groups to explore the possibility of additional partnerships in the ServiceNow space. If your support center or organization is interested in considering this option, please contact Karen Van Dusen, Sr. Manager and ServiceNow Product Owner, at kvd@cmu.edu.

**NEW TEMPLATE DESIGN FOR CMS SITES**

Marketing & Communications continues its partnership with Computing Services to develop the CMS template version 5 (v5). The new design is flexible and allows for various content types. Its simple and responsive design will provide University web sites with a cohesive, modern look. The colors, design and features have been tested and implemented to encourage ADA and W3C compliance. Content managers will find the standard page template meets most of their needs.

- **Hero** - large image space for a single image, slideshow, silent video or news article.
- **Content** – WYSIWYG area for text, images, media and more with selections for expand/collapse or a sidebar.
- **Grid** – Two, three or four column layouts for photos, news or WYSIWYG.
- **Slideshow** – Images paired with a text area.

Additionally, updated news, RSS and bio templates will be available soon.

Our current target for existing sites to migrate to the new design is March/April. A more accurate schedule will be shared in the coming weeks. Stay tuned to cmu.edu/computing/news/ for the latest information.

Documentation, training materials and an auto-migration tool are all in development. For a sneak peek of the new design in action as well as a list of new features visit cmu.edu/cms-demo/.

---

Get Microsoft developer tools, applications and Windows operating systems. Find out more cmu.edu/computing/software/all/msimagine/
SECURE BROWSING ON CMU.EDU

In an on-going effort to ensure safe and secure browsing, Computing Services has enhanced the security of several CMU websites. When you visit the following websites, you will notice a padlock and green address (URL) bar in all major browsers, indicating the heightened security:

- 2fa.andrew.cmu.edu
- accounts.cmu.edu
- grouper.andrew.cmu.edu
- identity.andrew.cmu.edu
- login.cmu.edu
- www.cmu.edu

COPYRIGHT VIOLATION PROCESS FOR STUDENTS

When requested, Carnegie Mellon is legally required to stop unauthorized downloading and/or distribution of copyrighted materials. If we receive a Digital Millennium Copyright Act (DMCA) notice and identify your computer as the offender, you will be notified and have 72-hours to resolve the issue with the Student Life Office. If it is not resolved, you will lose your network access and will not be able to register new devices or computers. For more information, see cmu.edu/iso/aware/dmca/.

PROCEDURES FOR COMPROMISED COMPUTERS

If you suspect your computer has been compromised, stop using your computer and report the problem immediately. Students should contact the Computing Services Help Center (412-268-4357 or it-help@cmu.edu).

Faculty and staff should contact the ISO (412-268-2044 or iso@andrew.cmu.edu). For more information visit cmu.edu/iso/governance/procedures/compromised-computer.html.
PASSWORD MANAGERS

Remembering a lot of passwords is difficult, but security experts (including ISO) recommend that you DO NOT reuse passwords. So, how do you manage the hundreds or even thousands of passwords you need to remember in your daily life?

Password Managers: An Overview

Password managers help you generate unique and strong passwords, store them in one safe (encrypted) place, and use them while only remembering one master password.

The ISO recommends three password managers that you can use in your daily life: 1Password, KeePass, and LastPass. While ISO recommends these three tools, this third-party software is not supported by the Computing Services Help Center. If you have questions or support concerns, you will need to contact the software vendor directly.

Each of these three password managers has pros and cons, including cost. The password manager that is best for you may not be best for a co-worker or family member, so select which manager you use based on the features and functionality that fit your needs.

One big decision you will need to make is whether you are comfortable with your encrypted passwords being stored in the cloud. ISO recommends that all of the managers encrypt your passwords on your local device first before storing them in the cloud. Thus, we consider them safe for the majority of users. There is still a possibility that your passwords could become compromised when stored in the cloud, but ISO is comfortable recommending either storage option based on the technology in use.

All password managers share a few pros and cons. The biggest con: if you forget your master/main password, you will lose access to all of your other passwords. No one can retrieve them for you; you will have to reset the passwords on all sites/areas where you used the password manager. The software vendor will not be able to recover your master password, therefore, it is very important to remember your master password!

Selecting a master password (passphrase) for your password manager

**DO**

- Select a long phrase that you will remember, but is not easy to guess.
- Include at least one of each: uppercase letters, lowercase letters, numbers and special characters.
- Because you will be typing this passphrase many times throughout the day/week, select a password that is easy to type on any size keyboard – including a cellphone!

**DON’T**

- Use your Andrew password as the master password for your password vault.
- Select well-known lyrics, or phrases such as “To be or not to be,” as a starting point.

Need more information?

For a comparison of password managers, visit [cmu.edu/iso/governance/guidance/password-managers.html](http://cmu.edu/iso/governance/guidance/password-managers.html).

REPORT CONCERNS

The ISO welcomes any reports of suspicious emails, or concerns about computer, network or data security.

Email [iso-ir@andrew.cmu.edu](mailto:iso-ir@andrew.cmu.edu) or call the ISO Hotline at 412-268-2044.
CYRUS UPDATE

Last fall, Computing Services embarked on a multi-phased project to decommission the Cyrus email service. The initial phase of this work, changing the email option for new Andrew accounts to Google or Exchange based on affiliation, was completed in October. Now in phase two of the project, we are working with administrative departments who use Cyrus to transition them to one of the supported email options in preparation for the decommission.

For more information on this project, visit cmu.edu/computing/email/cyrus/project/.

LOG INTO cmu.edu/lynda/

Lynda.com is an online training library with more than two thousand instructional videos. Log on and learn the latest software skills.