The university is excited to announce that Microsoft Office 365 is now available for all students at Southern Miss! This service provides students with a 50GB mailbox and 1TB file storage on OneDrive. In addition to having access to web versions, students will be able to download the latest Microsoft Office client application on up to five devices (PC, Mac, and/or mobile devices - Android or iOS). Go here for directions on how to install Microsoft Office.

Beginning fall semester 2016, the new student Microsoft 365 (student@usm.edu) email account will become the official university account, and at that time the EagleApps account (@eagles.usm.edu) will be discontinued as the primary contact for university communications. It is strongly recommended that all students begin to use the Office 365 email account (@usm.edu) now by following these directions on forwarding your EagleApps email to your Office 365 account.

To see a full list of available applications and information, go here. Online classes and conferencing, team sites and school video portal are currently disabled.

If you have any questions or need assistance, contact the iTech Help Desk at 601.266.4357(HELP) or by email helpdesk@usm.edu.

**FREQUENTLY ASKED QUESTIONS**

**Will I lose access or will my EagleApps (@eagles.usm.edu) account be deleted?**
No, you will not lose access and your account for EagleApps will not be deleted. However, after August 2016 the primary account for university communications will change to your new Office 365 (@usm.edu) account. Any form of communications from USM will be done through the Office 365 (@usm.edu) account only.

**After graduation will I still have access to my Office 365 account and features?**
Office 365 will be available for Email and Calendar only after you graduate.

**Will I need to notify my professors of my email change?**
All communications are being sent out to faculty, staff, and students. SOAR will update with your new primary account in August 2016.

**If I start using my Office 365 (@usm.edu) account before August 2016, do I need to do anything special to keep from checking two accounts?**
Yes, you will need to follow these directions to migrate your EagleApps account to your Office 365 account.
iTech employees gathered together in fellowship and cake to celebrate the birth of Nehemiah Mark, son of Rico and Nacoshia Mark. Rico has been a Desktop Technician with iTech since September 2015.

Congratulations to the happy parents!

Arthur Rowell, iTech Systems Administrator II, gave a presentation on March 2 at the Microsoft EduDays Conference on USM’s implementation of Microsoft Office 365.

“Today, I put in a work order to check the internet jack in my office. Within hours Marcus [Carter] and his intern Allyson [Ervin] were at my office ready to troubleshoot and fix my problem. Marcus is incredibly knowledgeable about all network issues and talked me through exactly what was needed. He worked hand-in-hand with Allyson making the connections and verifying everything worked perfectly. Both of them are a perfect example of what a great iTech professional is. Great job to Marcus and Allyson and thank you for such quick and accurate service.”

“Kelly [Payton] is extremely helpful. She always asks you if she can help in any way and clearly tells you what resources are available on the iTech website. She repeats information back to you to verify accuracy. She is an absolute professional!”

- Tara Burcham, Marketing & Events Specialist, LEC

EMPLOYEE SPOTLIGHT

iTech is pleased to spotlight Theresa Scardino, Software Integration Analyst. Her job responsibilities are to manage university applications configurations and support the users in their endeavors to use the applications. She works with vendors to coordinate licenses, upgrades, outages, and resolve break-fix issues. She also assists with testing the applications and helps to keep everything up and running for our users. She has been a Software Integration Analyst since November 2015.

“Theresa Scardino is returning to the university and we are happy to have her back in iTech. Her technical skills will be valuable to customers and her knowledge of the university is certainly an asset. Theresa is responsible for supporting quite a few important applications. She is a hard worker and will provide great support to the customers that depend on using these applications. Welcome back, Theresa!”

- Valerie Craig, Manager Technology Applications and Services
Spring is right around the corner, which means flowers, warmer weather, and Spring cleaning! This year, keep your computer in mind when beginning your cleaning checklist. Here are 6 tips to make your computer safer.

1. TIDY UP THAT FILE SYSTEM
It’s easy to scatter files across your computer’s hard drive and external storage devices. Sure, maybe all of the “documents” tend to make it into your “Documents” directory and your downloaded files end up in “Downloads”; but are these files really all that organized? Every so often it’s a good idea to go through your files and delete the ones you don’t need and organize the ones you do. Not only does this make it easier to keep track of your important files, but it helps reduce the complexity and size of backups. Look for files that are older versions of completed documents or downloaded files no longer needed.

2. MAKE SURE ALL YOUR SOFTWARE IS UPDATED
Your computer’s OS and software must be updated. The biggest threat to a computer system on the internet is unpatched software vulnerabilities. These security holes are often used by cyber-criminals to install malware. The best way to protect your computer is to keep the software up to date. Windows users will want to ensure that Windows Update is set to install important updates automatically and that updates are getting installed. Mac users can keep their system updated through (the aptly named) System Update. Some 3rd party applications (Adobe Flash or Firefox, for example) will automatically update themselves, but most 3rd party applications generally need to be updated manually. You can check the websites of developers and publishers for updates to their respective applications.

3. GO DEEP WITH THE VIRUS SCAN
First, if you didn’t do it already, make sure your anti-virus program is updated and it’s getting updated automatically. Once you know it’s up to date, do a full system scan. Ideally, this should happen more than once a year, but let’s be honest: Most people are too busy when they are using a computer to make time for it. Sometime, when you aren’t using your computer, start your anti-virus scanner with the most comprehensive setting possible and walk away. Perhaps on your way to a movie, when it’s dinner time, or when you head off to work or bed.

4. UPDATE YOUR PASSWORDS
Updating your passwords occasionally is a good idea. Why? Because you are undoing any work someone has put into guessing your password or you’ve just protected yourself from a stolen password of which you may not be aware. Also, you aren’t reusing the same password across multiple accounts, are you? Are you? If you find it challenging to remember your passwords, it’s not a bad idea to use a password manager. Do a little research and pick one that has been around a while and has a wide user base. Use a passphrase to lock your password manager.

5. REVIEW YOUR ONLINE SERVICES
Online services, especially social media sites, are constantly updating settings, behavior, look and feel, and policies or agreements. It’s a good idea to occasionally look over your account info, and check to see if privacy or account settings are a good fit for you. You might find changes that are not beneficial to you, or you might find new controls that provide stricter or more flexible security options. For services you’ve abandoned altogether, it’s a good idea to delete or deactivate your account.

6. BACK IT UP!
Now that all those junk files have been deleted and we’re pretty sure that your system is virus free, now’s a great time to backup your files. Things like financial and legal information is (typically) more important and more sensitive than pictures and entertainment libraries. Separate these files when you back them up. It’s best to keep the ‘sensitive’ data separate and backed up on less volatile media and stored in a more secure place. Use that external terabyte drive for your music and family photos. Burn the tax records and other sensitive docs to a CD or DVD and store that somewhere safe (for instance, in an actual safe or, perhaps, a safe deposit box). Sensitive files that are kept for historical reasons and rarely (if ever) accessed should be removed from your computer once they have been backed up and stored securely.

Backups can and do fail. Hard drives are just as susceptible to mechanical failure whether they are internal or external and a scheduled backup task may not include all the files you expect. It’s best to periodically test your backups, so you can identify and fix any deficiencies before it’s too late.