Technology Information

Tech TALK

Southeast Missouri State University · 1873

CONTENTS

EDITOR'S NOTE

While October is well known as the month of ghosts and goblins, our Information Technology staff want you to recognize the scariest event could involve trickery of a different kind—one that threatens personal or work related information. October is Cybersecurity Awareness month and the Southeast IT department has been busy broadcasting the message, using a variety of means and media. Perhaps you stopped by our Phishing table, in the University Center or Towers Cafeteria, where we challenged students, faculty, and staff to identify phishing content. Using an enlarged, but actual phishing message, technology users learned how to discern the difference between a legitimate or phishing email. Coming soon, our very own Southeast River Campus students will star in our Cybersecurity/Fairy Tale posters. Each poster will help us deliver important security messages and will be rotated across the Southeast campuses. An enormous thank you goes out to Dr. Kenneth Stilson and his great team of stars (staff and students)!

Our Cybersecurity Awareness program will be continued and available, now and in the future, in this edition of TechTalk. Increase your Cybersecurity knowledge on topics such as: Ransomware, Private Browsing, and Browser Cookies. Read about Southeast's successful Cybersecurity degreed program or play a Cybersecurity game. Calculate your online security risk and increase your data security by using the Spring Cleaning Checklist.

While this edition of TechTalk includes an enlarged Cybersecurity section, we strived to include our typical variety of technology related topics. Faculty member, Dr. Michelle Kilburn, contributes an article discussing five ways to establish instructor presence as an online instructor. Education student, Hannah Moss, shares how the Edvolution program helped her with her future career. We identify an app that you may find useful, introduce the latest Banner project, and include an alert that student email is about to make an improved change. And, what about that paperless myth? See the latest printing statistics from the IT student computer labs.

Members of Information Technology consider this third edition of TechTalk as special in two ways. First, we hope to have addressed the Cybersecurity issue that affects each and every one of us, in a way that will bring about awareness and due diligence. Second, we introduce and welcome Information Technology's new leader, Floyd Davenport, by wrapping up this edition with a personal interview. Learn more about the man behind the Associate Vice President title by reading this article.

Martha Henckell

Director, User Services

CYBER SECURITY INTRO

Folks,
October marks National Cyber Security Awareness Month (https://staysafeonline.org/ncsam/). As such, this edition of TechTalk will focus on cyber security; protecting your identity and access to critical resources.

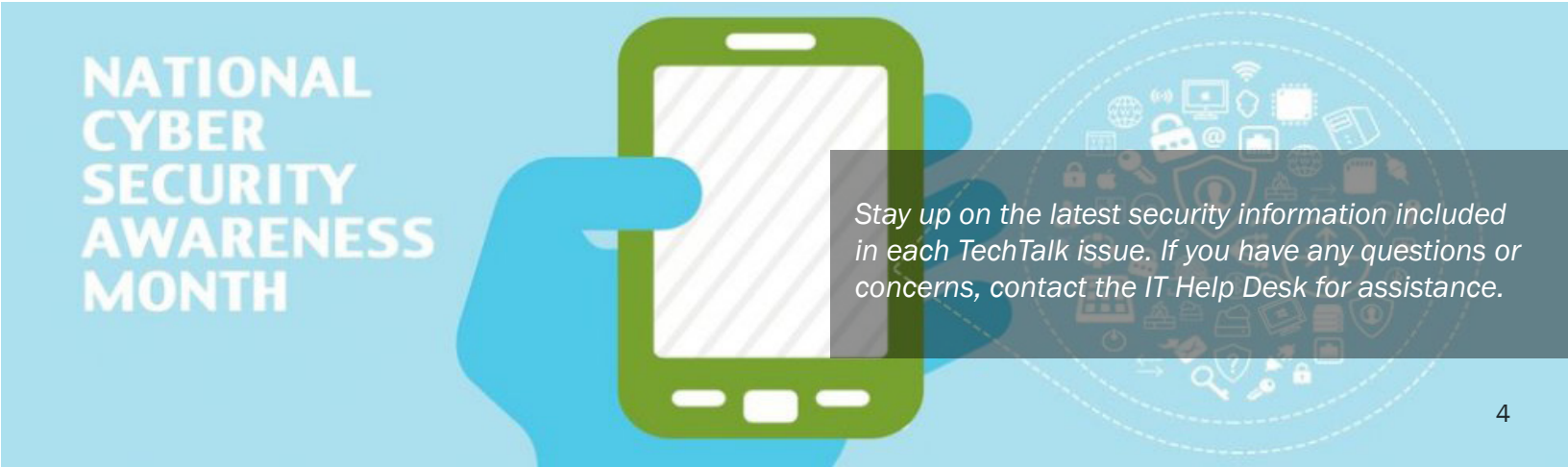
Are you at risk? Absolutely. Phishing schemes, used to steal your personal information, as well as malware, used to take control of your computer, are on the rise. Both are more sophisticated, more targeted, and much more damaging than ever. The Anti-Phishing Working Group (www.apwg.org) reports over 229,000 phishing campaigns in March 2016, along with a significant rise in Ransomware (malware that encrypts your data and holds it for ransom).

Consider how pervasive technology and connectivity are today. I have 67 applications on my iPhone. They are easy to install and allow me to connect with my friends and family, as well as pay my bills and access different online services. Unfortunately, these devices and applications also provide opportunities for malware to take control of my accounts and access information.

While IT has put systems in place to protect campus resources, there is no way to completely shield you from attacks. For example, IT has turned away 67,000,000 attempts to send spam and dubious email to campus in just the last month. Yet, we still have reports of phishing campaigns successfully deceiving faculty, staff and students. You are your last line of defense. Below I've compiled a few best practices that may help keep your identity and personal information safe.

1. Remember, IT will NEVER ask for your username and password.
2. Be cautious and skeptical of any email asking for your personal information or asking you to login to validate your account information. It is better to be safe, even if the message looks legit. Contact the source through other known channels, such as phone, or email directly.
3. Think twice before allowing browsers to store your login information. While it provides for quicker access, it could put you at risk. Even more so if you use the same username and password for multiple sites.
4. Consider using stronger and separate passwords for financial services and sites which manage critical resources. You might consider using a Password Manager application such as Lastpass or Keepass to help track your different passwords.
5. Keep your computer current. Older versions of software will be more vulnerable to cyber-attacks.
6. Know the signs of a phishing message.
   - Demanding immediate action, with dire consequences.
   - Requesting personal or login information.
   - Awkward wording and/or poor grammar.
   - Odd web links (URLs). Phishing sites may rely on similar URLs, such as www.ebay-secure.com or www.upgrade-target.com to fool users. Also, check for the @ symbol in the URL, and don't follow these links.
   - Hover over a link to see where it may really go. Anyone can create a link that says http://www.target.com/ but sends you elsewhere.

- Floyd Davenport, IT AVP



Stay up on the latest security information included in each TechTalk issue. If you have any questions or concerns, contact the IT Help Desk for assistance.

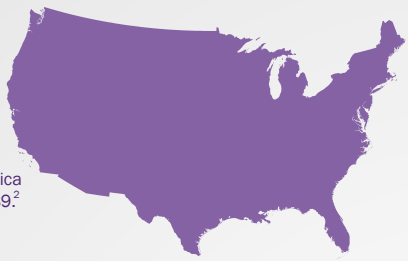
JUST THE FACTS, MA'AM!

Personal:

It's virtually impossible to manage our lives and responsibilities without relying on the internet. It is the basic foundation of so much of what we do – from shopping to monitoring health to turning in homework and keeping in touch with friends and family, we are connected 24/7.[1] Here are some startling statistics:

72%

of Americans believe their accounts are secure with only a username and password, yet the most common passwords in America are 123456 and 123456789.[2]



54%

ComScore's 2015 U.S. Mobile App Report, released last September, revealed that app use accounts for 54 percent of the time people spend with digital media.[3]

Every 2 minutes

there is another victim of identity fraud.[4]

$16,000,000,000

Identity fraud was responsible for $16 billion in losses in 2014.[5]

One of Five

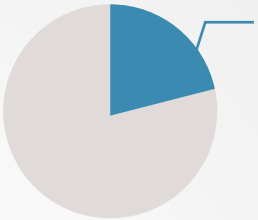
American households have received notification that their information has been lost in a data breach.[6]

63%

of confirmed data breaches involved leveraging weak, default or stolen passwords in 2015.[7]

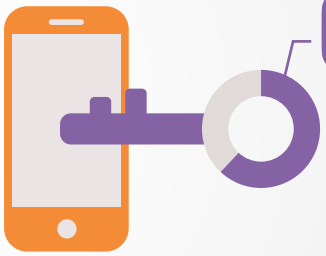
110M

Last year, hackers exposed the personal information of 110 million Americans — roughly half of the nation's adults.[8]



21%

In 2015, 21 percent of internet users (18 years and older) had an online account compromised, such as a social networking account or an email account, and only 23 percent think their accounts are very secure.[9]



62%

Sixty-two percent of Americans fear that their smartphone or computer will be hacked.[10]

53

Theft of personal information and identities

took center stage in 2015, accounting for 53 percent of all data breaches last year.[11]

1,938,383

In 2015 some 1,938,383 data records were stolen or lost every day, 80,766 every hour, 1,346 every minute and 22 every second.[12]

1. 2016 NCSA Strong Authentication Research
2. http://splashdata.com/press/worst-passwords-of-2014.htm
3. https://www.comscore.com/Insights/Presentations-and-Whitepapers/2015/The-2015-US-Mobile-App-Report
4. http://money.cnn.com/2014/02/06/pf/identity-fraud/
5. Javelin Strategy: https://www.javelinstrategy.com/press-release/16-billionsto-len-127-million-identity-fraud-victims-2014-according-javelin-strategy
6. http://staysafeonline.org/download/datasets/15982/BEHIND%20OUR%20DIGITAL%20DOORS%20-%20ESET_NCSA%20Fast%20Facts.pdf
7. https://www.internetretailer.com/2016/08/17/payment-and-personal-data-arewhat-hackers-seek-most
8. http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/
9. http://www.bbb.org/connecticut/news-events/news-releases/2014/08/thinkyou-know-how-to-protect-yourself-online-think-again/
10. http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx
11. http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf
12. Ibid.

JUST THE FACTS, MA'AM!

ONLINE SAFETY

When you're in college, your computer and mobile devices are primary tools in your educational and social life. Students use the Internet for homework, research, social networking, online shopping and other activities. The Internet is an amazing tool, but must be used safely and securely.

When you log on to the campus network (or any network), what you do online could impact not only your computer, but other students and the network as well. By combining up-to-date security tools with good judgment, you and your college community are much less likely to encounter a security violation, loss of data, or system problems.

The first step is STOP. THINK. CONNECT.

Keep a Clean Machine

- Keep security software current: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- Automate software updates: Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- Protect all devices that connect to the Internet: Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- Plug & scan: "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

Protect Your Personal Information

- Secure your accounts: Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- Make passwords long and strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals.
- Write it down and keep it safe: Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- Own your online presence: When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit who you share information with.

Connect With Care

- When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
- Get savvy about Wi-Fi hotspots: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- Protect your $$: When banking and shopping, check to be sure the site is security enabled.

Look for web addresses with “https://” or “shttp://”, which means the site takes extra measures to help secure your information. “Http://” is not secure.

Be Web Wise

- Stay current. Keep pace with new ways to stay safe online: Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- •Think before you act: Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- •Back it up: Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

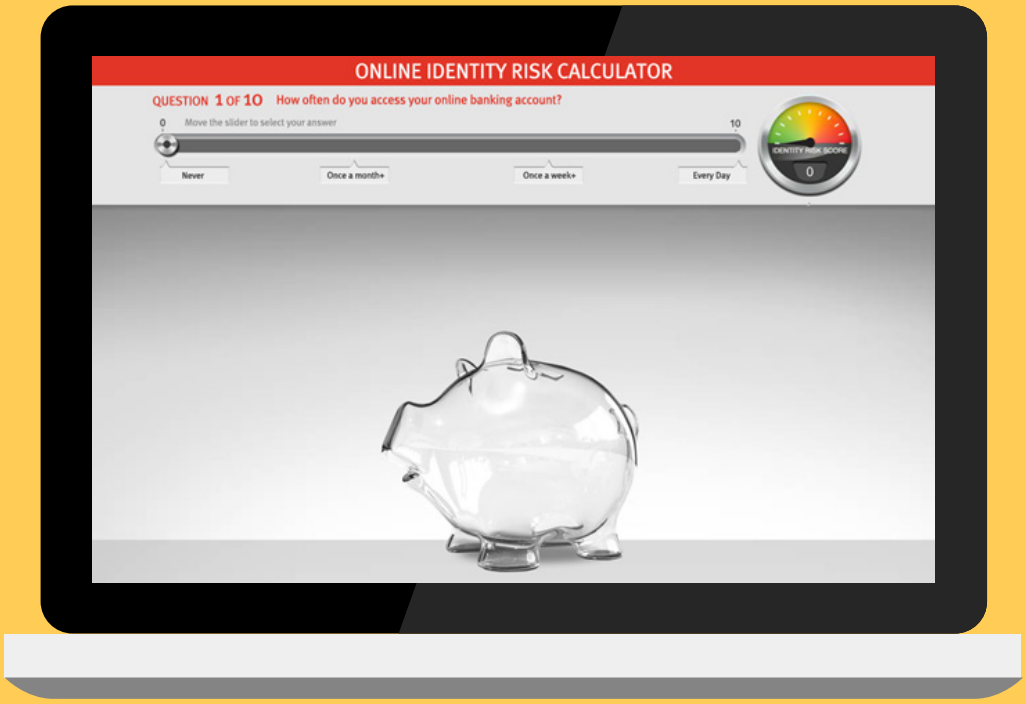
Be a Good Online Citizen

- Safer for me more secure for all: What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- Post only about others as you have them post about you.
- Help the authorities fight cyber crime: Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center and to your local law enforcement, state attorney general and campus police as appropriate.

Note: Adapted from *Basic Tips and Advice*. (2016). Retrieved from http://staysafeonline.org/stay-safe-online/resources/stc-tips-and-advice

- Martha Henckell, User Services

SECURITY TOOLS



Consider it risky business if you are an online user. What you don't know, can hurt you. Visit http://www.emc.com/microsites/fraudgame/flash.htm to see just how much risk you have accepted.

Phishers are looking to lure you with bogus emails and pop-ups that seem safe. Will you take the bait or live to swim another day?

Source: <https://www.consumer.ftc.gov/media/game-0011-phishing-scams>

Now visit the Game On page, located in this issue, to not only test your skill, but maybe also learn something that can save you later.

Should I play security roulette or should I not? If you fail to take steps to protect your identify, your data, etc., you are playing a game of chance with your information. Face it-- the odds are not in your favor!

Try your hand with these fun, but useful, security games.

Protect your village from Vikings with a strong password wall!

Source: <http://www.nsteens.org/Games/Password-Plunder>

Tad wants to keep his gossipy classmates from sharing his personal information. Help him clean up his profile. Put everything into the privacy vault and become a ***Privacy Guru***.

Source: < http://www.nsteens.org/Games/ProfilePanic >

Cyberbully zombies are attacking NSHigh! Don't let them get inside or they will send you mean IMs, post embarrassing pictures of you, try to steal your identity...and eat your brains!

Source: <http://www.nsteens.org/Games/Cyberbully-Zombies>

Now visit the Security Tools page, located in this issue, to test your security risk factor.

Prepare For RANSOMWARE

What is Ransomware?

Computer viruses have been around since before the Internet, even before personal computers were available. In 1990 the term *malware* (or malicious software) was coined, to describe *"any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising."*

Ransomware is a type of malware (malicious software) that infects a user's computer in a way that essentially holds the victim's files hostage until a ransom is paid.

As hardware and software have evolved, so has malware.

Viruses and other forms of malware had primarily been disruptive, annoying and sometimes destructive. Roughly 10 years ago, we saw the rise of another form of malware surface, ransomware. Luring people to activate this type of malware on a computer has become a revenue generator.

The most common method is to encrypt a computer's files, rendering them unusable. In order to decrypt the files, the victim must use a decryption key, and unfortunately, only the malware operator has this pricey solution.

Ransomware typically targets a user's documents, spreadsheets, photographs, videos, and music without affecting the operation of the computer. Generally the user is given a deadline, to heighten the urgency, after which their files will be unrecoverable.

How did I get attacked?

Ransomware is commonly delivered through email messages that include a link to a website or a file attachment. When the user clicks on either the link or attachment, malware is inadvertently downloaded. A less common delivery method for ransomware is referred to as a "drive-by infection." This method can infect your computer by simply visiting a website that contains malicious code or nefarious advertisement.

Once installed, the malware goes to work encrypting every file on the user's computer, every attached device, and potentially on other network connected devices.

Most users are unaware they have been infected until they can no longer access their files or receive an error message requesting that they pay some outrageous fee.

What should I do if I get infected?

- Disconnect your computer from any external storage devices (hard drives, flash drives, etc.) and the network to prevent further infections on other devices

- Contact the IT Help Desk

How to prevent it?

- Don't click on links or attachments you do not recognize or did not expect, until verified by the sender (it is good practice to mention you have attached a file in your email message)

- When prompted, proceed to install updates to Windows, Adobe, and other critical applications

- Back up your information weekly to an external hard drive that you disconnect from your computer once the files are backed up

If you have any questions or need advice, contact the IT Help Desk.

(http://vimeo.com/162117131)

- Todd Williams, Help Desk

COOKIES

: GOOD OR BAD?

Everyone loves a good cookie! When it comes to technology though, cookies can be both good and bad. Here's the good, the bad, and the ugly about cookies and browsers.

What is a technology related cookie?

In this reference, a cookie is information that your web browser saves when visiting various websites. Websites can store a cookie on your computer that allows it to recognize you every time you revisit that site. In this manner, cookies can be helpful. The information that it can and does store, though, can range from shopping cart information, login credentials, and even your browsing habits. This is how you can receive ads

tailored to your interests. Functions for each cookie placed actually will depend on who is responsible for placing it.

So who places cookies?

Cookies can be broken up into two general groups: First-party cookies and Third-party cookies. First-party cookies are placed by the website that you visit and can create a more efficient experience. These cookies will store information like items in your shopping cart, your log-in name, site preferences (ex. Displaying weather for your hometown), high score for games, and so on. Cookies can also be placed by other sources that the visited website grants permission. These cookies are known as Third-party cookies. The typical uses for these cookies are tracking your browsing habits and creating ads that are targeted toward your interests. Another common use for third-party cookies is for analytic companies to see how you are using certain websites.

Do you need them?

It is recommended to keep First-Party Cookies enabled because they can affect the normal functionality of a website. If Third-Party Cookies tracking your web browsing habits make you uncomfortable, then they can be disabled without affecting First-party cookies. A tutorial on how to disable Third-Party cookies in Google Chrome, Mozilla Firefox, and Microsoft Edge is available on the IT website (Disabling Browser Cookies).

Note: for more information on browser cookies visit the Federal Trade Commission's website, which provides an in-depth explanation of browser cookies.

- Joseph Marks, User Services


PRIVATE
BROWSING
“Secret of Sleuth Searching Simplified”

No you aren't being paranoid. When you use a browser and visit a website, the odds are, you are being tracked. Could be it's your browsing habits and interests being tracked. It could be the collection of data is about the device you are using. Or, it could be that the website is simply counting the number of people visiting their web page. Private browsing, or incognito mode, is a useful feature that can come in handy in a variety of situations. Essentially, private browsing involves a setting on the browser that disables several standard tracking and data collection features that most browsers commonly use.
Did you ever wonder how companies are able to display "Your Recently Viewed Items" or "Others interested in this product also viewed...?" Cookies! Used in this manner, some may consider browser tracking helpful. If you browse in the typical normal mode, cookies can be used by sites to track visitors and save your password for that website. Cookies, though, can also be used to track your search and web history. Beware the functionality of cookies if you are using a shared login in a classroom, on an employee machine, or a friend's computer. Instead, consider browsing in a more private manner. Below are situations where private browsing is suggested.

1) Logging into your accounts on someone else's computer.

If you are using someone else's machine and would like to get on Facebook, Moodle, or the Portal, IT suggests using the private browsing mode because chances are, the owner of the machine uses these sites as well. Private browsing can help prevent the saving of passwords and history, as well as automatically logging you out when the private browsing session is closed. This means that the owner of the machine can't access your accounts because the history or passwords were not saved.

2) Avoiding autofill history on public computers.

Since the classrooms that contain technology packages have a shared login, the possibility of a browser saving and or

populating your passwords or other information automatically is very real.

3) Leave a smaller footprint.

While private browsing will not hide your tracks from the network provider, private browsing can help you by logging out of all your accounts, not saving your passwords, and erasing your history.

Using the private browsing feature is just a simple way you can protect yourself and your information. To activate the private browsing feature on any browser, just right click your browser icon on your task bar at the bottom of the computer screen and select new private or incognito window from the menu.
If you would like to use this feature and need assistance, contact the IT Help Desk via chat, by email (helpdesk@semo.edu), by phone (573-651-4357), or by visiting the Help Desk in Memorial Hall, room 107, or Towers Complex, room 108.

- Alexsis Whitworth, Help Desk

Southeast Missouri State's
Cyber Security Program

Cybersecurity has become an issue that is not only discussed among technical professionals but is now a mainstream issue around the world. Cyber-attacks appear in the headlines of major news stories and have become a common topic among friends and family. This is because cyber-attacks can and have affected many people in the United States. Some of the major attacks that have happened so far this year have leaked data from the FBI, Homeland Security, the Internal Revenue Service, LinkedIn, Myspace, and Verizon. These attacks saw data loss that included information on 2.2 million individuals, 167 million accounts, and 6.5 million passwords! These kind of attacks have created a high demand for cyber security professionals and Southeast's Cybersecurity program has and continues to meet this demand.

Southeast Missouri State University was one of the first universities in Missouri to create a Cybersecurity program. The program launched back in 2011 with fifteen students, under the direction of Dr. Vijay Anand. These students graduated in May of 2014 and a large amount of them were hired into industry positions immediately. Dr. Anand has seen this program grow throughout the years and is now educating over 140 students. He attributes this growth to the public's new found awareness of the topic, the success of the students in competitions like the Collegiate Cyber Defense Competition (CCDC), and the industry's demand almost guaranteeing employment after graduation.

Southeast's program has been successful in educating its students to be industry ready by graduation. The rate at which the students are employed after graduation further attests to the programs quality and viability. Students that have graduated out of the program have been employed by Pricewater House Coopers, Ameren, Emerson, Charter, Dell Secure Works, Enterprise, and more. These companies consistently come back to hire out of Southeast's program year after year.

As other universities begin to implement their own cybersecurity programs, Southeast has plans to be sure that its program continues to stay relevant in this ever changing field. This will be accomplished by obtaining an ABET accreditation and an NSA certification for the program. When asked, Dr. Anand believes that these will be attained by as early as 2018. He said that the accreditation and certification will provide proof of the program's legitimacy and will aid students who are pursuing Master's or PhDs to get into graduate programs all around the country. Dr. Anand also mentioned his plans for the future are adding a Master's program at Southeast and to hire more faculty into the program.

The Cybersecurity program does not just end with the classroom. The program also consists of a Cyber Defense Club and a Collegiate Cyber Defense Competition (CCDC) team. The Cyber Defense Club is run by the students and compliments what is learned in class by diving deeper into the subjects and completing some hands on projects. Students in the Cyber Defense Club can also be selected to join the CCDC team. The CCDC team competes in a competition on an annual basis. The competition tests the student's skills in creating a secure computing environment. This year the team took first in the 2016 Midwest Collegiate Cyber Defense Qualification Competition and second in the 2016 Erich J. Spengler Midwest Regional CCDC. The team's achievements reflect the quality of the students' knowledge as they go through the program.

An interview with Dr. Vijay Anand, Assistant Professor

- Joseph Marks, Student

Between her glass slippers and her phone,
Cinderella is always losing something.
Her identity would be safer with a strong password.

`Glass_slipper`, `prince`, `stepsister`,
and `fairy_godmother` would be
a poor choice in passwords for *Cinderella*.

DIGITAL SPRING CLEANING CHECKLIST

NATIONAL CYBERSECURITY ALLIANCE

BBB

STOP | THINK | CONNECT

WEEK 1: KEEP CLEAN MACHINES

GET STARTED BY MAKING SURE THAT ALL WEB-CONNECTED DEVICES ARE SQUEAKY CLEAN.

- [ ] **Update software on all Internet-connected devices** to reduce risks from malware and infections.
- [ ] **Clean up your mobile life** by deleting unused apps, keeping others current and reviewing app permissions.

WEEK 2: MAKE SURE YOU'RE SECURE

ENHANCING THE SECURITY OF YOUR ONLINE ACCOUNTS IS A MUST AND A FAST, SIMPLE WAY TO BE SAFER ONLINE.

- [ ] **Turn on two-factor authentication on critical accounts** like email, banking and social media. Learn more by visiting stopthinkconnect.org/2stepsahead
- [ ] **Secure your router** by making sure it has a strong password and does not broadcast who you are through its name, such as "the Jones Family" or "123 Elm Street".
- [ ] **Make better passwords** by combining upper and lower case letters with numbers and symbols.
- [ ] **Make unique passwords for important accounts** like email, finance and healthcare.
- [ ] **Write down your new passwords and store them in a safe place away from your computer.**
- [ ] **Check to ensure all devices are password, passcode or fingerprint protected.**

WEEK 3: DIGITAL FILE PURGE AND PROTECTION

TEND TO YOUR DIGITAL RECORDS JUST AS YOU DO FOR PAPER FILES. BE SURE TO PROPERLY DISPOSE OF SENSITIVE MATERIALS - SUCH AS HARD DRIVES, DISKS AND MEMORY CARDS - AT A COMMUNITY SHREDDING EVENT. CHECK BBB.ORG/SECURE-YOUR-ID-DAY TO SEE IF THERE IS A BBB "SECURE YOUR ID DAY" EVENT IN YOUR AREA.

- [ ] **Clean out your old email and empty deleted folders.** If you need to keep old messages, move them to an archive.
- [ ] **Delete or archive older files and outdated financial statements.**
- [ ] **Unsubscribe to newsletters, email alerts and updates you no longer read.**
- [ ] **Update your online photo album** by deleting or backing up old or less flattering photos.
- [ ] **Update online relationships** by reviewing friends on social networks and all contacts lists to make sure everyone still belongs.
- [ ] **Copy important data to a secure cloud site or other drive where it can be safely stored.**
- [ ] **Password protect back-up drives and keep them in a different location off the network.**
- [ ] **Permanently delete all old files.**

WEEK 4: CLEAN UP YOUR ONLINE REPUTATION

PARENTS AND OLDER KIDS WITH SOCIAL MEDIA ACCOUNTS CAN TAKE AN ACTIVE ROLE IN MAKING SURE THEIR ONLINE REPUTATIONS SHINE.

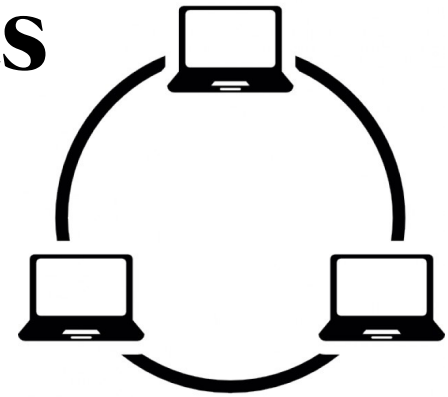
- [ ] **Own your online presence** by reviewing the privacy and security settings on websites you use to be sure they are set at your comfort level for sharing.
- [ ] **Clean up your social media presence** by deleting old photos, etc. that are embarrassing or no longer represent who you are.
- [ ] **Update your "online self"** by reviewing your personal information and updating it where needed.

STAYSAFEONLINE.ORG // STOPTHINKCONNECT.ORG

@STAYSAFEONLINE STAYSAFEONLINE @STOPTHNKCONNECT STOPTHINKCONNECT

STOPTHNKCONNECT

Get Connected with Your Students



With the addition of the Edvolution program, future educators are getting connected to their students' rapidly growing minds, using a variety of technology tools. As a student in the EdVolution program, my teaching methods have now been expanded to include the use of an iPad and other technologies. I have quickly become a fan of the EdVolution program because I have seen, first-hand, the benefits of this program.

All children develop uniquely and at different rates. The use of technology is one way to address these differences. Finding easier levels of games, using different research websites to accommodate the reading level of individual students, or using online organizational tools to help keep a student on task are just a few of the ways technology could be used. The never ending possibilities that technology offers gives teachers the opportunities to create engaging, educational, and interesting lesson plans, all the while incorporating specialized items for every student.

Technology in the classroom has also been identified as a great tool to help stimulate learning. Students tend to become more engaged in the learning experience when it involves technology. Teachers can take advantage of interactive games on the Promethean board or the ever popular iPad. With the students more engaged, teachers now have more time to create even more exciting lesson plans from the newfound free time.

Because students tend to view learning with technology in a positive light, hopefully the learning will continue while at home. There are countless hours of educational videos, from space topics to learning about different animal species, which can carry on the learning experience long after the bell rings. Making sure that your students are prepared for the future and up to date with the ever evolving world of technology is just as important as making sure you yourself are on the cutting edge.

No matter the goal or standard needing to be mastered, technology offers a world of options that will keep your students wanting to learn more and keep them excited to come to school the next morning. Technology advancements will forever shape the way we teach. To me, that means the future looks even brighter.

With my experiences in the Edvolution program, I feel I am more prepared to teach my students. I look forward to expanding their knowledge, as well as mine, as we embrace and incorporate the ever-changing world of technology. Go out and get connected!

-Hannah Moss, student

Getting to Know You:

Establishing Instructor Presence

Dr. Michelle Kilburn,
Associate Professor, Criminal Justice

As an instructor who strives to make a connection with all my students, I remember staring at the blinking cursor on my computer screen and thinking *"How are my students going to know there is someone on the other side of this computer? How will they know I am really here and that I have not just 'flipped a switch" to start my course and am now sitting on a beach somewhere while they spend hours reading and working through the material? By the end of the semester, will they know their computer better than they know me?"* Answering the question of how to interact with students is a challenge for many instructors, both veteran and rookie. This short piece is a conglomeration of literature review, personal experiences, and best practices I have accrued as an online instructor, master quality matters reviewer, interim instructional designer, and former director of Southeast Online.

At the basic level, Moore and Kearley (2005) discuss three primary types of interaction in distance education: student-to-content, student-to-instructor, and student-to-student. There is a discussion as to whether there should be a fourth interaction, student-to-interface (Gunawardena, 1994). Regardless, framing your course from the perspective of making sure your students interact with each other, the content (or course materials) and the instructor is a great way to assure you are incorporating, not only your presence, but also creating a sense of community within your course. To effectively discuss how to establish instructor presence, we are going to focus on student-to-instructor interaction.

{ Five Ways to Establish Instructor Presence }

1 Maintain frequent contact and a regular presence in online class discussions.

An instructor's responsiveness (e.g., answering emails and providing feedback) and message, tone, or style can affect a student's perception of instructor presence (Russo & Campbell, 2004). Students who receive prompt feedback reported positive perceptions of learner-instructor interactions (Thurmond, et al., 2002). The more details and feedback that can be provided for students, the more opportunities they have to experience interaction with the instructor. Simply opening a gradebook and seeing a grade is not authentic interaction.

Instructor presence in discussions can be achieved in a variety of ways. Simply joining the online class discussion is certainly one way of making the instructor's presence known. Another strategy is to provide a summary of the discussions that have taken place and to give feedback on the scope and direction of the discussion. Clarifying and expounding on particular posts, comments or topics also gives the students an awareness that the instructor is involved and active in the discussions.

It is important to note that although instructor interaction is important, presences does not necessarily follow a "more is better" formula. In one study conducted by Mazzolini and Maddison (2003), an increased number of instructor postings resulted in more infrequent and shorter student messages. Faculty should strive to maintain a balance between responding enough to meet the needs of the student and establishing a personal presence in the classroom. However, he/she should strive not to take on such an aggressive role in responding to forum discussions and posts that students are discouraged from interacting with each other.

2 Add personal elements to your course.

It has been suggested that student's like seeing a photo and hearing their instructor's voice. Students report this gives them a feeling of greater connection to the instructor's real-world presence (Russo & Campbell, 2004).

Other elements such as handwritten responses, detailed feedback, video announcements, and instructor introductions of family members may be considered positive interactions from a student's perspective (Kilburn, 2013).

3 Utilize videos and social media when applicable.

Instructor-created audio and video add an important element of individuality and social presence in the online environment (Lane, 2010). One student descriptively summarized the benefits of weekly videos and announcements saying, *"I have taken online courses, and this instructor is the only one that I actually feel like exists. When you take an online course, it often seems like there is an invisible person grading everything and we have no connection. By actually visually seeing this instructor and picking up pieces of her personality, I feel like there was a real teacher in the class"* (Kilburn, 2013, pg. 57).

Self-report studies estimate students use social media an average of 2.7 hours daily. It should be noted this is considered a conservative estimate (Harvard, 2011). Using technology to communicate with students (e.g., Facebook, Twitter, Instagram) outside of the course management system removes a layer of formality and can allow students to increase their feeling of social presence (Kearns & Frey, 2010). According to Baird and

Fisher (2005), today's students are active, wired, "always on" learners who integrate social media technologies as a tool to support learning (pg. 10).

It is also beneficial to make sure your students are engaged and creating content as opposed to just merely consuming content (Seaman & Tinti-Kane, 2013). Other applications that can be useful to meet this objective are blogs/wikis, podcasts, and student streamed videos.

4 Provide clear expectations to learners.

In a face-to-face classroom setting, instructors might hand out an assignment and then spend three to five minutes discussing their expectations for that assignment. It is important not to leave this critical step out of the online environment. Although it is tempting to simply use an assignment or activity from a traditional course, examine the assignment to see if the instructions are clearly laid out for an online student.

Setting expectations in advance helps relieve anxiety for learners. Include details on topics such as: (a) how attendance will be taken, (b) honesty policies, (c) no-tolerance policies for rudeness or incivility, (d) whether homework submitted past the deadline will be accepted, and (e) grading policies. It has been my experience that providing detailed information up front reduces confusion on the students' part- and in turn drastically reduces the number of emails to the instructor.

5 Recognize the importance of instructional design and support.

Keeping up with the most up-to-date trends, apps, and programs can be overwhelming. Instructional designers provide an invaluable service helping faculty develop courses that utilize the most up-to-date technology effectively and in a strong pedagogical foundation. Quality assurance rubrics, such as Quality Matters, provide guidelines and best practices for effectively designing courses from a student perspective. Faculty should not be thrown into the world of online learning, social media, videography, and/or educational gaming without a guide to help them navigate the best way to get to the desired destination: an engaged student who is learning.

Instructor presence is essential in the online environment. Students are coming to us as veteran users of multiple technologies and experience in multiple social media platforms. Students will expect that colleges and the classrooms will support these interactions. Faculty who are cognizant of the need and put forth the effort to establish a presence in their online classroom will help create a community, which can then lead to great student satisfaction, retention and an improved learning environment.

Adapted from Kilburn, M., Henckell, M., & Starrett, D. (2016) Instructor Driven Strategies for Establishing and Sustaining Social Presence. In L. Kyei-Blankson & J. Blankson (Eds.), Handbook of Research on Strategic Management of Interaction, Presence, and Participation in Online Courses (pp. 305-327) Hershey, PA: IGI Global and Kilburn, M.A. (2011). Facilitating Interaction in the Online Environment. In S. Hoffman (Ed.), Teaching the Humanities Online: A Practical Guide to the Virtual Classroom (pp. 71-82). New York: Sharpe.

References

Gunawardena, C. N., & Zittle, F. J. (1997) Social presence as a predictor of satisfaction within a computer-mediated conferencing environment." *The American Journal of Distance Education*, 11(3), 8–26.

Harvard Institute On Politics. (2011). *IOP youth polling: Spring 2011 survey*. Cambridge: Harvard University Kennedy School of Government.

Kearns, L. R., & Frey, I. How do students experiences differ in online LIS programs with and without a residency. *Library Quarterly*, 77(4), 359-363.

Kilburn, M. (2013). Student perceptions of instructor interaction in the online environment. *International Journal of Research in Social Sciences*, (1)(1), 54-58.

Mazzolini, M., & Maddison, S. (2003). Sage, guide or ghost? The effect of instructor intervention on student participation in online discussion forums. *Computers and Education*, 40(3), 237-253.

Moore, M. & Kearsley (2004). *Distance education: A systems view*. 2nd ed., Belmont, CA: Wadsworth.

Russo, T.C. & Campbell, S.W. (2004). Perceptions of mediated presence in an asynchronous online course: Interplay of communication behaviors and medium. *Distance Education*, 25(2), 215-232.

Seaman, J. & Tinti-Kane, H. *Social media for teaching and learning.* Pearson Learning Solutions and Babson Survey Research Group, Boston, MA.

Thurmond, A., Wambach, K., Connors, H. & Frey, B. (2002). Evaluation of student satisfaction: Determining the impact of web-based environment by controlling for student characteristics. American Journal of Distance Education. (16) 169-189.

SUMMER TECHPACK TESTING

Toward the end of the summer, the IT department started a new annual project of testing each of the tech packs on Southeast campuses. The objective of this project was to ensure instructors would hold their first class with a minimal of technology related issues. This year, the department was able to test almost three quarters of all techpacks on campus. That equates to 196 of about 270 techpacks currently installed!

So what's a TechPack?

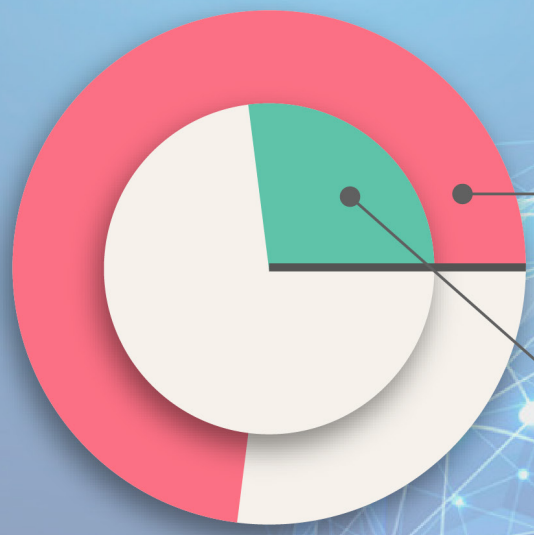
To enrich the learning experience, faculty rely on technology channeled through classroom techpacks. This includes computers, monitors, projectors, microphones, speakers, SmartBoards, and VCR/DVD players. These items were tested to make sure they were in working order. Software updates were also applied for the following programs:

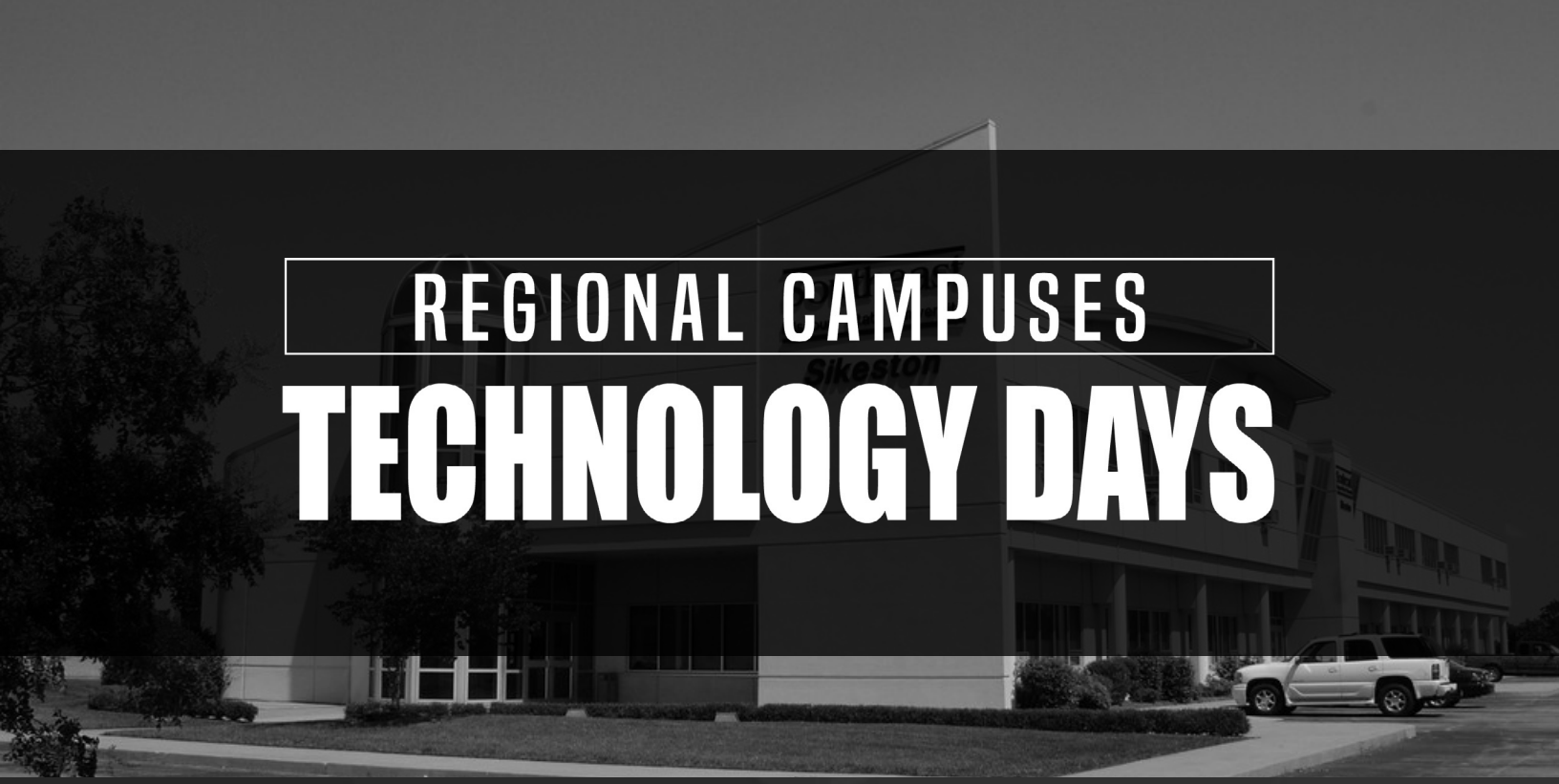
- Windows Updates
- Adobe Flash Player
- Adobe Reader DC
- McAfee
- Java
- Office 2013
- SPSS-24
- Air Server

Access to the updated computer image can only be guaranteed when the faculty log in used is the techpack credentials assigned to that classroom. For this reason, it is recommended that instructors not use their personal login information when using the techpack. This can cause some or all updates to be unavailable for use. Instructors that do not know the generic techpack login credentials can contact the head of their department or the IT Help Desk (573-651-4357). These logins are to be restricted to only official Southeast instructors and are never to be given out to students or taped to the monitors.

Buildings Tested

Academic Hall
Art Building
Brandt Hall
Carnahan Hall
Crisp
Dempster
Grauel
Johnson
Magill
Memorial
Parker
Rhodes
Scully
Serena
Kennett
Malden
Sikeston





REGIONAL CAMPUSES TECHNOLOGY DAYS

The 2016 Regional Campus Technology Day events were successfully held at the Malden, Kennett, and Sikeston campuses on September 14th, 15th, and 16th. The purpose of these events is to give Regional Campus students, faculty, and staff the opportunity to have hands-on technical assistance from Information Technology User Services personnel. This is the second year these events have been offered.

Each day from 11 a.m. to 2:30 p.m., students, faculty and staff received assistance with tasks such as connecting to Wi-Fi, setting up email on their mobile devices and general technology questions regarding basic antivirus procedures, accessing the Portal and Moodle, as well as other technology related topics. While at the regional campuses, scanners were replaced with updated models in the three open computer labs. The new scanners feature sheet feeders and can scan both sides of a document. Free technology related accessories, such as phone kickstands, microfiber cloths, and touchscreen styluses, were also given away to participants.

The next Regional Campus Technology Day events will be held in January or February of the Spring 2017 Semester. For more details regarding these events, check the next issue of the Tech Talk, and/or the Information Technology Event Calendar at http://www.semo.edu/it/events.html.

Travel & Expense Management

The newest University purchase from the Ellucian/Banner portfolio is **Travel and Expense Management (TEM) powered by Chrome River**. As the latest asset in the Banner system, this year-long project has just begun. Our first featured article on this product will address the benefits of this purchase, the team responsible for setting up and launching the software, as well as the timeline.

BENEFITS

Improve efficiency

Automate the entire travel expense submission, approval, and reimbursement process.

Accelerate payment

Submit expenses and receipts from any mobile device for faster reimbursement.

Provide visibility

See trends and spend with real-time analytics and reporting dashboards.

Produce paper

Minimize IT support with an easy-to-use, software as a service solution.

TEAM

Functional Team Leader: Pam Sander, Controller

Technical Leader: Mark Blaylock, Application Systems Director

TIMELINE

August 1, 2016 – November 10, 2016	Discovery and Design Phase
September 21, 2016 – December 29, 2016	Configuration Phase
November 4, 2016 – February 15, 2017	Validation Phase
December 1, 2016 – January 24, 2017	Training Phase
February 1, 2017 – July 21, 2017	Deployment Phase
July 21, 2017	University-wide Deployment

video URL:
https://www.youtube.com/watch?v=XPNsy-029OeU

You might remember this jingle from the 70's commercials for the fast-food chain Burger King. Wouldn't it be nice, when using the MySoutheast Portal, if you could have it your way? In the Portal, one step toward this goal would be to put the content you most use where it can easily be accessed.

Actually, you can have the MySoutheast Portal your way. The Portal has a feature called Private Pages. Private Pages can be used to arrange Portal content or "portlets" in a customizable fashion, specific to each Portal user.

With Private Pages you can:

- Change the look and feel of the page with different layouts, colors and/or themes
- Add content from different tabs
- Access utilities and tools like a unit converter, password generator and wiki tool
- Change the default language of at least some of the content

For more information on setting up your very own Private Portal Page, checkout the step-by-step tutorial located at http://www.semo.edu/it/tutorials/Lum5CustomPgs.pdf.

- Todd Williams, Help Desk

The What's What On Whats App

WhatsApp! A phenomenal app that allows you to communicate quickly and clearly with anyone around the world! With 450 million users in over 250 countries across the globe, Whatsapp is on the cutting edge of global communication.

What makes it so great? Well, for one thing, WhatsApp is free and operates off Wi-Fi, as opposed to a cell phone carrier, so data rates and messaging fees are currently nonexistent. You can do everything on this app that you could do on a standard messaging program: group messages, send pictures and videos, even call someone thousands of miles away, all presently free of cost! The latest version of the app also offers end-to-end encryption to ensure that only you and your friend will be able to view these messages. This means no third parties prying into your personal details.

The sheer amount of coverage this app provides is equally impressive. You can instantly connect to people right next door or the other side of the world. It doesn't matter if you are in Italy, Japan, Bangladesh, or Norway; chances are that if a location has access to Wi-Fi, they'll have WhatsApp users. Integrating your address book into WhatsApp is done automatically, and will show you all of your contacts that have also downloaded the app!

This is a great app for Southeast students, especially because of the international presence found on campus. With this app, you can maintain those relations even after you or your friends have returned home. It is a fantastic social and networking tool that is continually improving, and should be the next app on your list of things to download!

- Jacob Hill, User Sevices

SOFTWARE DEADLINE

In order to allow sufficient time for software updates to be installed in the Information Technology open computer labs, Academic, and/or Regional Educational Center computer labs/classrooms, deadlines for new software updates have been established. If your department has new software that you would like to have considered for placement in the computer labs or would like to update current software, please deliver or complete the following items by the deadlines listed below:

1. Software
2. Proof of licensing certification
3. A completed online request for installation form from http://www.semo.edu/it/itcomputerlabs/software-request.html.
4. Any additional software documentation

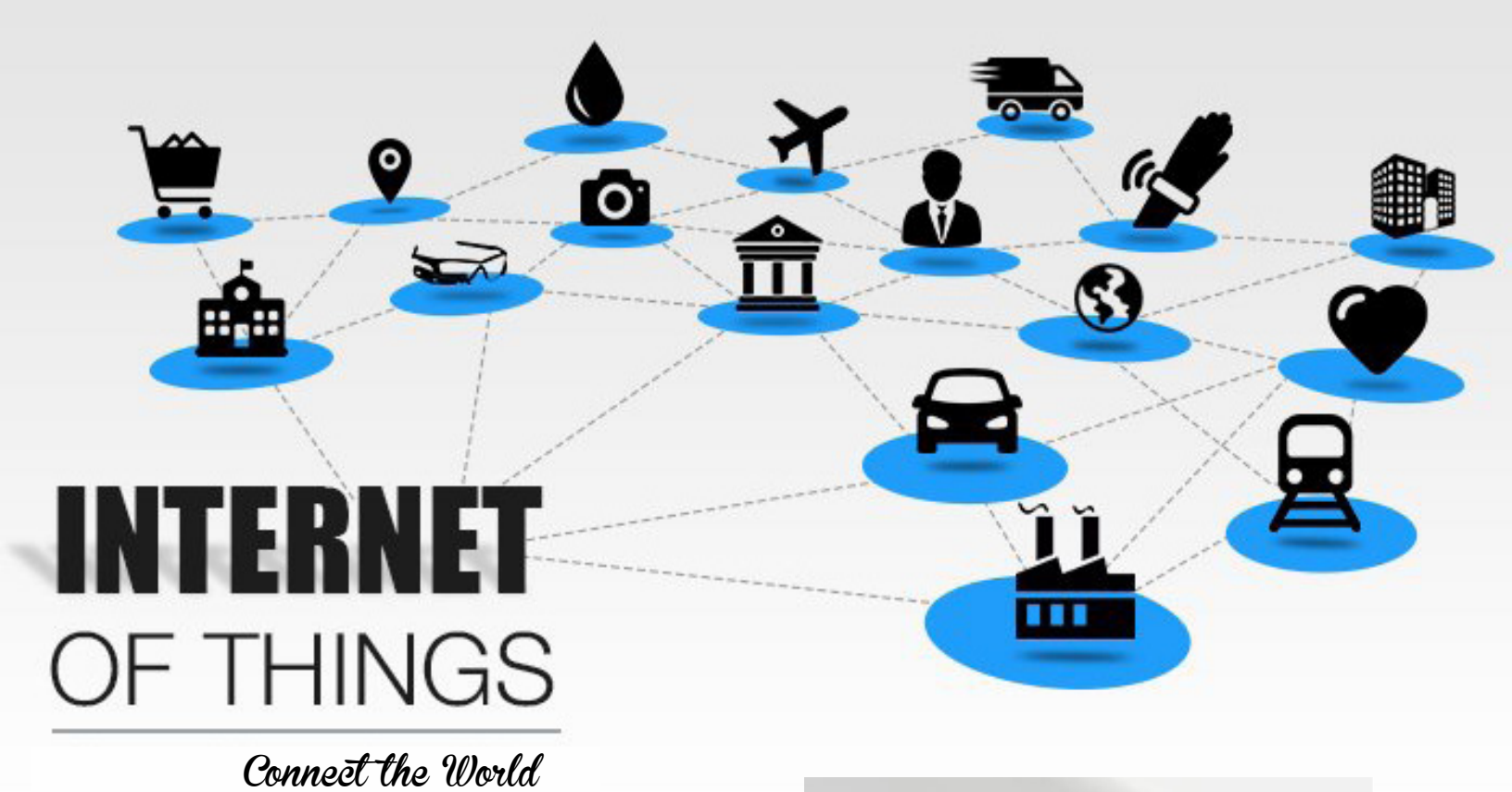
DEADLINES

November 1	**For Spring installation**
April 1	**For Summer installation**
July 1	**For Fall installation**

All software installation decisions are based upon available resources and compatibility with the network and other applications. By instituting these deadlines, Information Technology will have time to create a new desktop image that can be tested prior to the start of semester classes. Due to the length of time required for re-imaging the computer labs, these deadlines are firm!

Special Notices

- The current version for SPSS is 24. If you have a version older than 23 or 24, contact the I.T. Help Desk (x4357 or helpdesk@semo.edu) to request the updated version.
- Please share with your faculty the access and availability of several computer labs, provided by Information Technology, for the occasional use of class teachings. The reservation labs can be reserved by contacting the IT Help Desk at x4357. Details on reservations can be obtained by visiting http://www.semo.edu/it/itcomputerlabs/reservable-labs.html.
- Note: The IT Open Computer Labs are not classified, nor funded, as teaching or academic labs.



Chances are, you know someone with a device that connects, communicates, or controls another product. Within the past five years, a number of home and consumer products are in some way connected to the Internet or connected to a device, such as your smartphone. Welcome to the revolution of the Internet of Things, or IoT, as it is most commonly referred.

IoT devices are classified as any device with an on-off switch that is either connected directly to the Internet or to a device that is connected to the Internet. Common home examples include smart door locks or thermostats. Both can connect to your home WiFi, communicate and be controlled by a computer or cellphone app. Now you can have the functionality to lock or unlock your door and raise and lower your home temperature remotely.

IoT devices can have sensors that send feedback to a cloud based service, provide a second screen to show notifications such as text messages, or be turned on and off according to a schedule. A common example for sensors is your thermostat automatically setting an *Away from Home* status when it senses no one is home.

▲ **Amazon Button**

Some IoT devices allow you to control other gadgets with just your voice. One such device of this type is the Amazon Echo, which connects to your other smart devices, such as Phillips Hue lightbulbs. Did you forget to turn down the lights when watching your movie? All from the ease of your recliner, with your voiced instructions to an Amazon Echo, you can dim, turn on or off your lights.

As with any technology, IoT devices bring not only convenience, but also security issues. Hackers now have a new way to worm in to your life, through IoT devices. New and additional avenues for hacking could provide entrance to aspects of your life that go beyond just accessing your Facebook page or email account. Consider the maliciousness that could be accomplished with access to control your home thermostat. Contemplate what could be overheard from your Amazon Echo, if hackers were to access the always-on microphone.

Even with IoT devices, as with all electronics connected to the Internet, you can take steps to ensure your protection. Consider all connected devices as part of your whole network and make your security measures holistic. Setup passwords or pin codes on any device that your IoT device is connected. Definitely set up a password protected home WiFi network to prevent connection by unwanted users. Finally, you should always have a current version of anti-virus software on your PC. Remembering to keep all of these devices secure will ensure that your IoT devices will also stay protected.

Images: Apple Watch, sleep tracker, Fitbit, Amazon Echo from top to bottom.

- Robert Hendrix, User Services

DEVICE TUTORIALS

Technology is synonymous with change. Technology brings change to people; often changing behaviors and changing lives. Sometimes it changes too fast for us to catch up. Email, Wi-Fi, cell phone usage, computer maintenance and so much more can make it feel like you're losing your grip on not only your devices, but your life!

We may have a solution for you. The Information Technology department has created, and is constantly updating, online Tutorials (http://semo.edu/it/how-tos/index.html#tutorials) that can be access by anyone. Students, faculty, and staff are encouraged to become familiar with these tutorials that tackle many of the issues that any user may encounter on a daily basis.

Do you have an iPhone? We have several tutorials that will show you how to connect to Wi-Fi, view emails on your phone, stay connected on campus, as well as be more prepared for classes. As technology changes, these tutorials are updated, allowing you to stay up-to-date and well informed.

Do you have an Android? The same goes for this mobile device as well. The IT Help Desk staff, both student and full-time, are willing to walk you through the connection process. We are ready, day or night, to show you how to better utilize your device for campus life.

Do you have a Windows Phone? You guessed it, we have a tutorial for students. More than that, we can help you with all the antiviral and malware protection in regard to your Windows laptop. We can even help get you free Microsoft Office products like Word and Excel for your devices!

Now that your email has been set-up and you are staying up to date with everything coming through, you may wonder, "what else is there available that can help me as a student? What if I bring my Xbox or Playstation on campus and want to get it connected to the internet?" Look no further than the Media Devices section and you will find tutorials on how to connect an Xbox or Playstation to the campus network.
Now that you have had a small sampling of what IT tutorials can offer, visit http://www.semo.edu/it and, chance are, you will find another tutorial that can be of service to you.

- Aaron Alter, User Services

I.T. LABS
UPGRADE HARDWARE

During the summer break, I.T. replaced all computers, located in the Crisp & Magill Open Computer Labs, with dual core 3.7 GHz i3 processors and 22" widescreen LCD monitors.

	Crisp	**Magill**
Locations	Crisp Hall, Rm 215	Magill Hall, Rm 118
Hours of Operation	Monday – Friday: 8am-4pm	Monday – Thursday: 8am-6pm Friday: 8am-4pm
Number of Available PCs	20	22

In addition to the computer replacements, all peripherals, which include: black & white printers, color printers, and scanners, were replaced in all I.T. operated computer labs. These hardware upgrades will help students be more efficient and productive in completing tasks.

	B&W Printers	**Color Printers**	**Scanners**
Crisp	Yes		Yes
Dempster	Yes	Yes	Yes
Kent	Yes	Yes	Yes
Magill	Yes		Yes
Merick	Yes		Yes
River Campus	Yes		Yes
Towers	Yes	Yes	Yes

Check out the latest in scanning technology, available in the I.T. Computer Labs, in this issue!

Another annual Southeast Missouri Open House has just passed, with even more success than the year prior. Students came to view the latest and greatest technology offered on Southeast's campus and beyond.

Many new and old faces were seen at the Open House, unveiling technology to enhance both business and leisure activities. Graduate Assistant Beau Sehau showcased an electric powered car as well as a waterjet milling system used for metalworking, courtesy of the Polytech Department. At Towers, Velocity Electronics co-owner, Ryan Frenz, also made an appearance to demonstrate the new Belkin screen protectors, capable of withstanding impacts as blunt as the strike from a ballpeen hammer! Along with offering technology assistance, two cybersecurity students (Zach Peek and JoLynn Hallmark) were at both the Memorial Hall and Towers Help Desk locations to help students with virus and malware protection and removal, as well as general computer safety tips. An Eachine Racer 250 personal drone, one of the most state-of-the-art drones in the field, was also on display.

Paul Belvin, IT Labs Supervisor, also demonstrated some fantastic new technology available in the world of education and business. The SV600 ScanSnap, now available in IT Labs, will make scanning both faster and easier. This scanner model is noted for its ability to scan books without the book binding issue found with most scanners. It's so fast you could scan a whole textbook in less than an hour! Several other interesting program events included demonstrations of ***Plinkers***, which provides a way to gauge classroom opinions without the use of multiple devices, and ***Nearpod***, an interactive lesson creator for secondary education majors. All of these things are currently free to download and use, so don't be afraid to get your hands on them and explore!

Door prizes were also given out, via a raffle system at both the Memorial Hall and Towers locations, to a few lucky participants. Two grand prizes, a Utopia 360 Virtual Reality Headset, was won by Harrison Backer and Nick Moore. Other notable prizes included a set of Lapgear Deluxe Lapdesks, won by Sultan Alnasser and Logan Surratt, as well as two PNY 32 gigabyte flash drives, won by Taylor Bridges and Swagatam Saha.

- Jacob Hill, User Sevices,
Todd Williams, Help Desk

MIGRATION IS COMING!

In the spirit of advancement and increased efficiency, our email services for Southeast Missouri State University will be moved to the Microsoft Office 365 Email servers! This service will be provided to all of Southeast Missouri State's students by January 2017. Soon, thereafter, employee email will also be moved. Some features to take note of are:

Email	OneDrive	Calendar
50 GB email server space that is fully compatible with touch screen devices and other Microsoft Office software.	A cloud-based storage system that allows you to work on documents from anywhere and gives you 1 Terabyte (equivalent to 212 DVD's!) of document storage.	A planner-type application to keep you organized and on time; can be customized with tasks and flag notifications.

Be on the lookout for future Office 365 announcements by visiting to www.semo.edu/it/Office365.

ENOUGH TO MAKE A GROWN TREE CRY

Fall 2015 B&W Printing Statistics		
Location	**# of Print Jobs**	**# of Pages**
Crisp I.T. Lab	8,169	54,407
Dempster I.T. Lab	24,102	90,286
Kent I.T. Lab	71,064	359,233
Magill I.T. Lab	19,393	96,793
Merick I.T. Lab	12,944	55,563
River I.T. Lab	4,282	19,404
Towers I.T. Lab	44,581	195,114
Total B&W I.T. Lab Printing	**184,535**	**870,800**

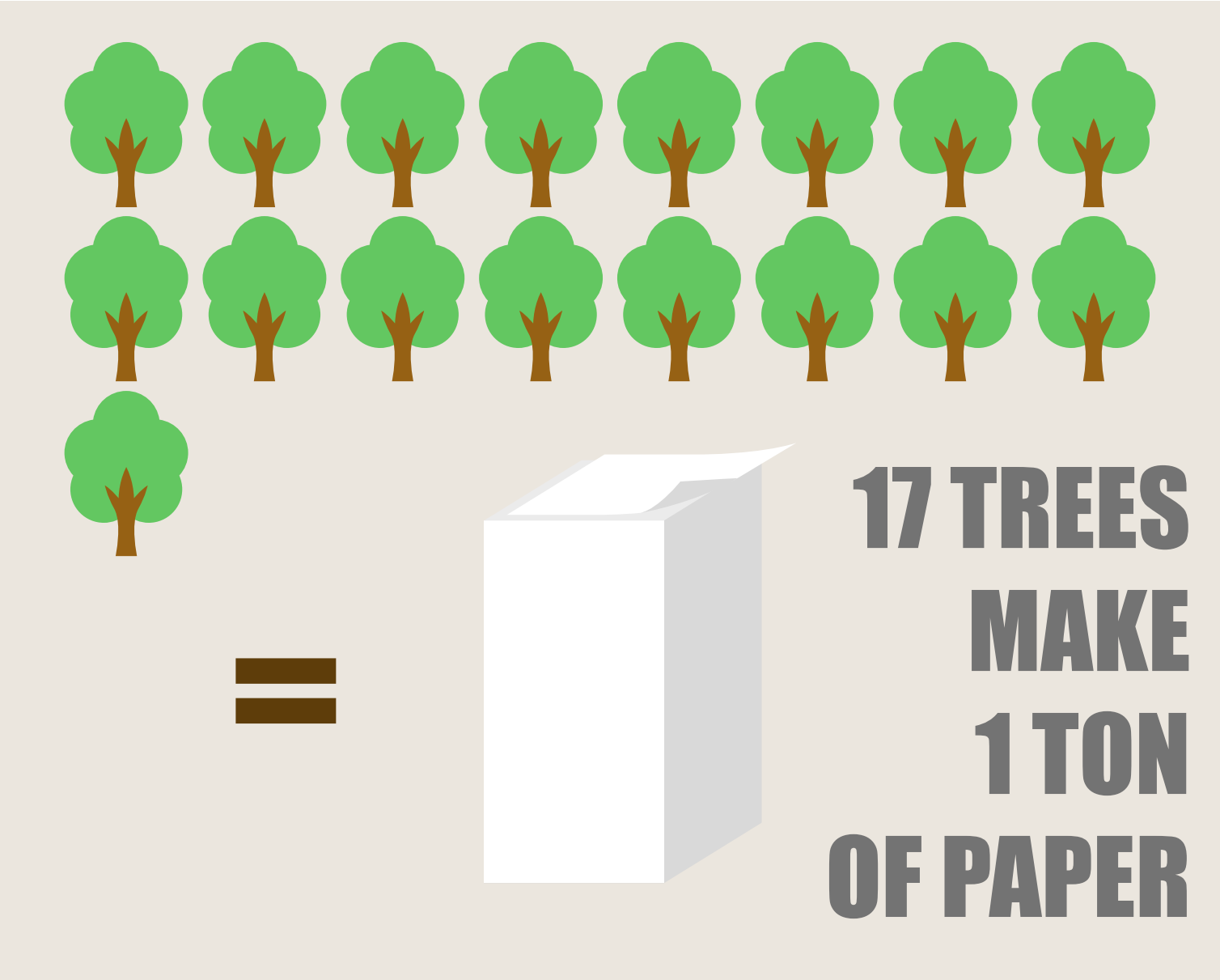
Spring 2016 B&W Printing Statistics		
Location	**# of Print Jobs**	**# of Pages**
Crisp I.T. Lab	8,984	58,450
Dempster I.T. Lab	20,759	96,574
Kent I.T. Lab	63,059	318,100
Magill I.T. Lab	20,861	101,186
Merick I.T. Lab	12,852	55,931
River I.T. Lab	4,033	18,171
Towers I.T. Lab	44,423	200,385
Total B&W I.T. Lab Printing	**174,971**	**848,797**

THINK BEFORE YOU PRINT

Fall 2015 Color Printing Statistics		
Location	**# of Print Jobs**	**# of Pages**
Dempster I.T. Lab	496	1,696
Kent I.T. Lab	2,854	7,757
Towers I.T. Lab	1,225	3,143
Total Color I.T. Lab Printing	**4,575**	**12,596**

Spring 2016 Color Printing Statistics		
Location	**# of Print Jobs**	**# of Pages**
Dempster I.T. Lab	345	1,018
Kent I.T. Lab	2,773	8,505
Towers I.T. Lab	1,823	4,746
Total Color I.T. Lab Printing	**4,941**	**14,269**

DID YOU KNOW?



1. **Print multiple pages per sheet** – Look for the option to print multiple pages on one sheet
2. **Print Only the Text You Need** - Copy only sections needed, then paste into one document and print
3. **Use Print Preview and Shrink to Fit** – Preview print job and make revisions before printing
4. **Print Duplex** – Print double sided to reduce waste
5. **Print in Color only when Necessary** – Color printing costs more and will reduce your print account faster
6. **Scan more and copy less** – Do you really need a hard copy? Email the file to someone instead
7. **Patience Is a Virtue** – Give it time for your document to print. Large PDF and PowerPoint files take longer to process and print

ScanSnap SV600

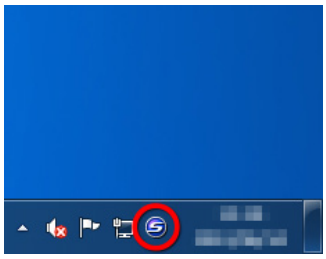
FUJITSU

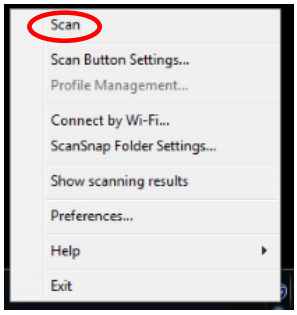
New document scanners have arrived! After year-long testing and receiving positive student feedback, the I.T. department has deployed new document scanners to all I.T. open labs for student use. These new scanners operate more quickly and quietly than traditional scanners. With newer technology, light, during scanning, is no longer a problem. A document cover is no longer required. This new technology allows students to complete their scanning projects more quickly, allowing them more time to study!

Check out the brief operational steps and video below!

1. Press ***Scan*** button to turn on scanner.

2. Right click ***ScanSnap*** icon.





3. Click ***Scan*** button to scan document.

Watch this video for a Live Demonstration of ScanSnap:

AVP Interview

Floyd Davenport

Assistant Vice President of Information Technology, Southeast Missouri State University

After 30+ years, Floyd Davenport has returned to Southeast Missouri State University. This time, it isn't as a student, hailing from Norman, Oklahoma. This time, it isn't as a winning member of the swim team. This time, Floyd returned as Assistant Vice President of Information Technology, and is here to lead the IT team!

Just before college started this fall, Floyd and his wife, Kim (as in fellow Southeast graduate and college sweetheart) Meder, moved to Cape Girardeau and joined the Southeast campus. Having Computer Science degrees from both Southeast and Texas A&M, and 33 years of IT experience in the IT field, Floyd brings a wealth of knowledge and vision to the Information Technology Department. Excerpts of Floyd's vision and philosophy regarding Information Technology and its role in Higher Education are shared below.

Why did you apply for this type of IT position?

I enjoy working with all aspects of information technology... I've been doing it for a long time. I feel strongly about the mission of higher education and I enjoy working with people. This position allows me to work with the campus community while employing technology for advancing higher education. It's a win, win, win.

How does your position serve students?

We serve students primarily by providing access to educational resources. This is accomplished through our campus network, computer labs, software licenses and support services. Some of our labs and our Helpdesk are available 24 hours a day. Of course we support so many other activities that depend on technology, such as general Internet access, email, registering for classes, paying a bill, applying for housing, etc.

How does your position serve faculty?

For faculty, we support technologies employed for teaching. This is a very exciting area as new opportunities for teaching online or using more interactive technologies in the classroom are developed. We want to partner with faculty to effectively capture and deliver instruction and support new teaching models.

How does your position serve staff?

Staff use a multitude of applications which help manage the business of the institution. IT is the caretaker of systems which collect, process and store information on students, courses and finances. From the day a prospective student applies to Southeast to the day the student graduates, staff employ these applications to assist the student along the way.

When I attended Southeast, there were only two computer labs, no personal computers, no Internet, email or social media. Most teaching was accomplished on a blackboard or using overhead

displays. As a service organization, IT has to evolve along with technology and the innovation it fosters to enhance teaching, learning and living.

What originally sparked your interest in an IT field?

I got my first exposure to computer science taking an Assembly class in 1980, while here at Southeast. Assembly is a low level programming language which introduced me to process logic and I was fascinated by the ability to automate and develop applications. I was hooked.

If you did not work in IT, what career do you envision for yourself?

I've always been fascinated by the operations of large manufacturing plants. So, I think I would want to be a plant manager. I guess I enjoy solving problems, working with people and seeing the end product.☺

Describe a typical day for you while working in IT.

A typical day may not seem too exciting. I spend a lot of time visiting with staff, attending meetings, and answering emails. However, underlying those activities is always "what is best for the institution" and "how can we enhance our services".

What do you most often look forward to when you come to work each day?

It will sound corny, but being a part of something that is so important to so many people, where I can add value. Working with people to solve problems and create new opportunities.

What do you love most about working in IT?

It's fun to learn about new technologies and it's even more rewarding when you are able to successfully employ them in the business of teaching and learning.

What are the high points and/or low points of working in an IT department?

As with most highs and lows, they are the opposite sides of a coin. The high is successfully helping someone employ technology. This can be solving a simple problem or implementing a new complex system. The low is when you can't solve that problem or when you find a specific application is not a good fit or consistently fails. The good news is the lows can almost always be turned into highs, it just takes a little time and effort.

What was the craziest or most difficult day you experienced working in the IT department?

I think the craziest and most challenging day was managing the technology of a major conference, which was also streaming multiple sessions across the country. We were so engaged with helping attendees, setting up conference rooms, streaming to hundreds of locations. It was crazy, so many things happening all at once, even with months of preparation... but it was also fun and very rewarding.

Overall, how would you rate your experiences working in IT?

Since it is all I've ever done, I'm going to give it a 10! It's got a good beat and I can dance to it.

What advice would you give to a student pursuing a position in IT?

There are so many aspects of information technology. Explore and find what really excites you. That said, always stay current and explore new opportunities.

List and discuss some of your hobbies.

Well I love to read and watch movies. I guess I like good stories.☺ I've also been swimming all my life. I enjoy it very much; I've just slowed down a little... ok a lot.

List and discuss your immediate family members.

Kim (Meder) and I have been married for over thirty years. We originally met while attending Southeast... Kim received a degree in Geology. We are very proud of both of our grown children, one living in San Diego and one in Illinois.

CREDITS

EDITOR IN CHIEF

Martha Henckell

TECHNICAL EDITORS

Todd Williams

Paul Belvin

CREATIVE DIRECTOR

Michelle Lee

AUTHORS

Aaron Alter

Alexis Whitworth

Floyd Davenport

Hannah Moss

Jacob Hill

Joseph Marks

Michelle Kilburn

Robert Hendrix

Todd Williams

Technology *Information*

Southeast Missouri
State University · 1873

Tech TALK