IT Matters

Protecting your Social Identity
by Scott Finlon, Information Security Engineer

The first thing that you need to know about free online services, if it’s free -- you are the product. They take any information that you give them and sell it to third parties. Have you ever changed your default privacy settings on Facebook? Do you install apps without reading what you are allowing them access to? Have you ever clicked on a link that someone sent you when you weren’t expecting something from them? Do you use the same user name or password on multiple websites? If you answered yes to any of these questions, read on and I’ll explain why these practices aren’t always a good idea.

Continued on page 4

October is CyberSecurity Month
by Jack Williams, IT Training Specialist

Throughout this issue, we’ll feature articles, tips and other information regarding our attempts to promote awareness of computer safety. With identity theft abounding, along with other malicious computer issues, we discuss what steps we can take to protect ourselves.

Our theme is STOP. THINK. CONNECT. We also have a website dedicated to this important topic:

www.scranton.edu/staysafe
CyberSecurity Month Activities
by Jack Williams, IT Training Specialist

October is CyberSecurity Month and the University of Scranton is using this important time to make the entire university community aware of the dangers we face on-line and the measures we can take to protect ourselves.

All month long we'll be highlighting those issues that concern us when we're using our computers in service of the university and at home. ID theft, unauthorized use of information, malicious software, viruses and other unlawful and problematic issues that plague computer users today, will be discussed and practices to combat these, as well.

Posters, table tents, brochures, and website information will be available to all members of our community. A special IT Forum on CyberSecurity, with Social Media as a focus will be presented on October 16th.

CyberSecurity day, October 10th, is geared toward our student population, but everyone can benefit from the activities on that day. We'll have a table setup in DeNaples Center, 1st floor, featuring information on many of these security issues. We'll also have prize giveaways for all interested people.

For more information regarding CyberSecurity Month and CyberSecurity Day, go to our special web page: www.scranton.edu/staysafe, and also our IT Training page at: www.scranton.edu/it_training.

Stop
Stop: Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

Think
Think: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

Connect
Connect: Enjoy the Internet with greater confidence, knowing you’ve taken the right steps to safeguard yourself and your computer.

Spam
Global spam volumes actually declined in 2010, by September: the global spam volume was down to 3.5 trillion spam messages per month.

Stay Safe Online
STOP. THINK. CONNECT.
www.scranton.edu/staysafe

Our Shared Responsibility
staysafeonline.org

National Cyber Security Awareness Month

CyberSecurity Day is Wed., October 10th
Join us at our information table in DeNaples Center
1st Floor from 11:00 am to 2:00 pm
We'll have Prizes, T-shirts, and Hand-outs
Big Data….Big Promise?
by Jerry DeSanto, Ed.D., Vice-President for Planning and CIO

Each year Gartner, an IT research thinktank, produces its Hype Cycle for Education, which basically illustrates graphically the technologies that are currently receiving the most attention in higher education and where they are with respect to their adoption and maturity levels. The concept of Big Data is clearly currently climbing the expectations slope of the Hype Cycle. Big Data is generally described as the massive amounts of data that is collected by an organization over time that is unwieldy to analyze or handle using common database management tools. So, what’s all the fuss about?

Consider the fact that in the higher education industry most universities have collected data about their students, parents, university donors, applicants for admission, and the like for decades. Also, consider the fact that higher education as an industry is becoming increasingly competitive, and decisions that need to be made on many campuses are complex with escalating risks ever-lurking. Also, reflect on how certain companies in the for-profit sector are using information gleaned about you the customer to tailor their offerings to you. Frequent shoppers on Amazon.com are surely familiar with how this extremely successful company uses information about your buying history, your recent searches on their site, and demographics to focus your attention on certain products and services on their site. This use of big data being manipulated by business analytical tools undoubtedly allows Amazon.com to increase their sales. So, if we were to consider how higher education might be able to use our big data in combination with data warehousing and certain analytical techniques to aid in marketing the institution or making business decisions there are numerous possibilities to ponder.

This mountain of collected data help us spot students who are beginning to show signs of failing? Could we use data to help inform food services or the bookstore about students’ tastes and buying preferences? Could data help us better understand our student customer so that we can provide them with improved customer services perhaps embracing a Customer Relationship Management (CRM) philosophy? Could our data stores help us make pricing decisions regarding tuition and housing? And the list goes on.

Most institutions are currently wrestling with these questions, and examining the tools and methods that would be wise to invest in to leverage the data asset on their respective campuses. However, at this point in time the tools and solution sets are relatively immature and very expensive to successfully deploy. Even though the University has an integrated relational database think about how much data that we as a campus collect annually that resides outside of the central database in auxiliary systems on campus and in the cloud. Consequently, such solutions, if truly comprehensive, will be arduous to architect and implement. The Gartner Hype Cycle currently projects that Big Data will not hit a maturity stage until 5-10 years out. However, it’s not too early to begin our study of what’s possible, how much it will cost, and what the potential return on investment will be. Stay tuned.

IDENTITY THEFT continues to escalate and transform so quickly that the Identity Theft Resource Center says it “can only make educated predictions on the course of identity theft for 2011.”

According to Dataprivacyrights.org, over 512 million personal data records have been reported as breached in the United States. Given there are just over 300 million citizens, the likelihood that your personal information has been stolen multiple times is high.

Need help with a computer problem, or to reset a password or PIN...

Contact:
The Technology Support Center
(570) 941-4357
techsupport@scranton.edu
Facebook Safety Tips

- Pick a strong password: Use a combination of at least six numbers, letters, and punctuation marks (like ! and &)
- Make sure your email account(s) are secure
- Log out of Facebook when you use a computer you share with other people
- Run anti-virus software on your computer: Both Windows and Mac OS
- Add a security question to your account (learn how)
- Use our extra security features (learn more)
- Think before you click or download anything

Learn more - go to: Facebook.com/help/security/tips

Free services like Facebook have privacy settings, but by default are almost completely open and leave your information available to anyone who wants it. You should go in to your account settings and read the personal and privacy settings carefully. If a setting doesn’t make sense to you, it is normally safer to keep them at the most strict level or turned off. Any time that you install an app or take a free quiz or survey, look at what settings the app or quiz is asking to have access to. A lot of the time, they are asking to have full access to all of your personal information. You may be asking “why is this important to me?” The easy answer is that the site may ask you to fill out secret questions to reset your password in case you forget it, and the answers to most of these questions, think mother’s maiden name and street you grew up on, are filled out on a lot of people’s Facebook profile.

Similar to email phishing, which is an attempt to acquire information like usernames or passwords by masquerading as another trustworthy source, there are many different types of Facebook messaging scams. If you get a friend request from someone that you don’t know, they may be trying to get access to your personal information in a different way than the free quizzes try to. If you ever get a link in a message from someone you don’t know, and sometimes from people you do, don’t click on them unless you can verify that they are legitimate. There might be malware on the other side of that link waiting to infect your computer as soon as you click on it. One of the biggest current patterns are videos claiming to be hot-topic current events, but will just try to exploit a vulnerability on your computer and infect you with malware.

Do you use the same username or password on multiple websites or services? Say for example you use your email address and password as your credentials on Facebook, and your Facebook account gets compromised. Now the attackers have your email address and your password, so they can log in to your email and see everything you have in there. They can take it a step further by looking through your email for other website accounts, and even if your password isn’t in your email they can send a password reset email and since they have access to your email and they now have the keys to your identity.

By not protecting yourself in any of these ways, not only is your personal information at risk, but your university account could be at risk too since the answers to your questions, your email addresses, and possibly your password can be found in any of these ways. So next time you go to install something or click on a link, think about your privacy settings and make sure you are protected before you agree to any terms or click on any links.

Facebook Security tips

1. Know how to spot a scam
   If an offer looks too good to be true, it probably is. Think twice before you click on a link for free airline tickets or other common scams.

2. Choose a one-of-a-kind password
   Is your Facebook password different than your email password? If not, please reset your passwords today.

3. Confirm your mobile number
   If you forget your password, Facebook can text you a new one. To make sure Facebook can reach you, confirm your mobile number.
Now is the time for all good men to come to the aid of their party. Now is the time for all good men to come to the aid of their party.

IT Matters FALL 2012

Upcoming Training

In addition to available instruction in Live@edu, Identity Finder, and SANS Security, IT Services will be offering classes to all staff and faculty in the following:

- Accessing and Using RoyalDrive
- Microsoft WORD
- Windows 7
- Microsoft Excel
- Microsoft Project
- Basic Computer Use
- CMS Training

For information on any of these class offerings, contact Jack Williams, IT Training Specialist, or go to www.scranton.edu/it_training.

Using the FOOTPRINTS Service Catalog

Did you know you can submit your computer problems and service requests via the FootPrints Service Catalog?

Here’s How:
- Log into my.scranton.edu
- Click on the University Links tab
- Scroll down on left to the Administrative Links section and click on FootPrints
- Log into FootPrints using your username and email password

In The Service Catalog:
- **Category 1** allows you to report technology problems with your computer, phone, Royal Card or cable TV as well as audio visual problems and Banner problems.
- **Category 2** allows you to request changes to Banner applications and reports.
- **Category 3** allows you to request services such as multiple PC setups, new VoIP phone requests, port changes, Royal Card reader loans, Royal Drive access, university PC software installations, and web requests.

Please note that you can always call the Technology Support Center at (x4357) for help logging these requests or to have the request logged for you.
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.

Loyal Science Center Update
by Jason Wimmer,
Instructional Services Manager, OIT

After several years of planning and construction, the Loyola Science Center project has come to fruition, with the completion of Phase II and the start of the fall semester. LSC is one of the most technologically advanced buildings on campus, and helped re-establish a new standard of digital technology in our classrooms.

The building has numerous highlights, including a 103” Plasma display that shows scientific related information through various means, including RSS and Twitter feeds. There are also seven smaller displays throughout the building that are integrated with the campus digital signage system. The large lecture hall, LSC 133, is the most advanced room on campus that includes three projection screens, high-definition audio and video, motorized blackboards, an annotative monitor and is one of the two rooms in the building that has Lecture Capture functionality. There are over fifty mediated spaces in the Science Center that include seminar rooms, labs and tiered classrooms. There are several rooms some that have dual projection capabilities and ceiling mounted document cameras. The construction defined various levels of classroom mediation. These definitions have been expanded upon and used for other projects like the Brennan Remediation Project.

Using the lessons learned with this project, the Office of Instructional Technology will build on this experience as we upgrade other facilities and prepare for new construction projects.

Code of Responsible Computing Review
by James Franceschelli
Dir., Information Technology Services, ITS

The Code of Responsible Computing Review Committee was recently formed to review some of the University’s polices regarding the use of IT. The existing policies have been in place for more than a decade and need to be updated to address the changes and use of technology. The group, comprised of faculty, staff and students, will review both the University’s Code of Responsible Computing and the Student Computing Policy with the directive to create a single policy related to responsible use of information technology for all members of the University Community. The group will research current best practices in acceptable use of information and technology policies in higher education as part of their work.

The intended outcome of this group is for a draft policy to be submitted for review to the Vice President for Planning & Chief Information Officer by the end of the academic year. The final policy will be submitted through the University governance system for approvals in 2013-2014. Committee membership was solicited from the University Staff & Student Senates as well as the Faculty Senate Technology Advisory Group (TAG). Members of the Code of Responsible Computing Review Committee include Dave Dzurec (co-chair), Jim Franceschelli (co-chair), Calvin Krzywic, Robert Farrell, Jessica Adler, Clay Nottlemann, Charles Kratz, Xuewu Wesley Wang, Bob Spinelli, Margaret Hynosky, Kyle Gleaves and Jennifer Coco.
Introducing New Tools for Student Mobile Access
by Connie Wisdo, Director of IT Development & Applications

After about a year of research and development, IT Development and Applications (ITDA) is pleased to announce the availability of Blackboard Mobile Learn for ANGEL, and our custom-written Student Services Mobile web app, accessible from any mobile browser, and featuring useful functionality for Scranton students, including access to grades and course schedules.

Last fall, ITDA formed a Mobile Apps working group consisting of 3 faculty, 2 students and more than a dozen staff from several departments across campus. The group was charged by the VP for Planning / CIO to make recommendations for enhancing the functionality of the University’s mobile app, specifically related to teaching and learning, as well as student services. The vendor for the University’s “Scranton app” has been continually updating the app with new or improved modules, such as the recently-added emergency module. However, while the Scranton app contains a lot of functionality, it does not provide the ability for an individual student to “log in” and access data from our ERP system, such as grades or schedules.

The Mobile Apps working group had many good suggestions for additional functionality, but wanted to gain the input of the University community to help narrow down the long list, and determine priorities for development. With input from the working group, a survey was developed by Public Relations for users of the University’s mobile app and another, similar, survey for those who hadn’t yet downloaded it. Over 400 people took the surveys in March, 2012 with students accounting for almost 70% of respondents. The Scranton app received very positive reviews, with 67% of respondents rating the app at either 4 or 5 on a five-point scale on overall impression. With regard to student services, the responding students overwhelmingly asked for mobile access to the ANGEL LMS, followed by class schedules and final exam schedules. So, we set to work.

In late spring, after the LMS Evaluation Working Group made its recommendation for two more years of ANGEL LMS use, ITDA went ahead and negotiated a two-year license for Blackboard Mobile Learn for ANGEL. This app can be downloaded from app stores for free use on iOS, Android, and Blackberry devices.

Around the same time, Joe Casabona began developing the first version of our Student Services Mobile web app, in collaboration with John Culkin and Phil Erb from Systems & Operations. This initial version of Student Services Mobile allows students to: Check Grades, View Full Schedule, View Channel Guide, Visit the Library, and Visit the Aquinas. Near the end of each semester, students can also view the schedule of final exams. Student Services Mobile has been added to the Scranton app, and is also available by going directly to https://m.scranton.edu/studentservices.

The Mobile Apps working group will continue to meet once a semester to provide feedback on the app(s), as well as suggestions for additional functionality. If you would like to nominate a student to the group, please send his/her contact information to constance.wisdo@scranton.edu.

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 cyber criminals.
• Write it down or use KeePass, 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 how and with whom you share information.
Connect with Care

- When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cyber criminals 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 sites you visit are secure 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.

The Top 5 Q&As from the TSC
by Gail Bontrager, Asst. Dir. IR Customer Service

1. Why won’t the library computers let me log into them?
   The way we log into computers in classrooms and labs changed over the summer. IT Services implemented Active Directory in labs and classroom and the username to log into these computers is now the Royal ID #, which can be found on your Royal Card.

2. How do I connect my laptop to the campus network?
   a. Enable the wireless network adapter on your laptop or wireless device.
   b. Connect to the wireless network named ROYALAIR.
   c. Open a browser (IE, Firefox, or Safari).
   d. You will be redirected to a page to download and install Cisco NAC.
   e. Once Cisco NAC is installed, log into it using your myScranton username and password.
   f. If you have not already updated your operating system and/or installed antivirus software, you will be prompted to do so now. We recommend Security Essentials for Windows PCs and Sophos for Macintosh laptops.
   g. Once you have installed all necessary updates, you will get a message that says: You have been successfully logged on the network.
   h. Now you can access internet resources.

3. I can’t remember my password. How can I get into my email?
   If you have your password reset questions set up, you can go to my.scranton.edu and click on the “Forgot your password” link. Once you answer all the questions correctly, you will be given a new password.
   If you do not have password reset questions set up or you cannot answer your questions correctly, you will need to go to the Technology Support Center in Alumni Memorial Hall with your Royal Card and a TSC staff member will give you an unlock code and walk you through the process of setting up your password reset questions and resetting your password.

4. My PC has a virus. What should I do?
   If you are a student and your PC is a laptop, please take it to the Technology Support Center during Laptop support hours (listed below) to have the virus removed.
   **Sunday**  Noon – 6 pm
   **Monday through Thursday**  10 am – 8 pm
   **Friday**  10 am – 4 pm
   Students with desktops in a campus residence hall, please contact the Technology Support Center (941-4357 or techsupport@scranton.edu) and we will log a ticket to have a ResCon visit you to remove the virus from your computer.
   Faculty or staff members who have purchased computers through the University ResNet Sales, please take it to the Technology Support Center during Laptop support hours (listed above) to have the virus removed.
   If you are a faculty or staff member and your university owned office PC is infected with a virus, please contact the Technology Support Center and we will log a ticket to have your computer picked up and cleaned of the virus. You can request a loaner desktop if you have no other computer to use.

(Continued on next page)
The Top 5 Q&As from the TSC
(Continued from previous page)

5. How can I get help learning to use the new technology in my classroom?

The Technology Support Center can schedule a student staff member to meet with you 15 minutes before your class to provide technical assistance for the new technology in classrooms. If you would like this service, please complete the OIT Equipment Request Form in the portal on the University Links tab.

Additionally, you may access the Classroom Database from any on-campus computer to acquire information and operating instructions about the technology in various classrooms. Please note, this database is still under construction and the information for some classrooms may not be available yet. You can view the classroom database at www.scranton.edu/techsupport. Click on the Classroom Database link.

IT Services Reminder...
IT Services reminds department representatives to look for Microcomputer Budget Request forms being sent this Fall. Our goal continues to be equipping each office with appropriate hardware for the specific needs of each area.

IT Services Training Calendar
IT Services has greatly expanded classroom training for commonly used software programs on campus. The training is available to all staff and faculty. A training calendar is provided for campus-wide initiatives, such as Live@edu, RoyalDrive, and Windows 7 training. Training is done Monday through Friday, between the hours of 8:30 am and 4:30 pm. Information on specific courses and times/dates is available on the IT Services website:

www.scranton.edu/it_training

If interested in any of the training subjects listed on the website, for individuals or department groups, please contact Jack Williams, jack.williams@scranton.edu.

Software titles not offered can be discussed and programs can be evaluated for potential inclusion in our training offerings.

Training is conducted in the IT Services Computer Lab in Hyland Hall, 4th floor, room #402. Capacity per class is 14 students.

Current campus-wide training courses:

- Using Windows 7
- Live@edu - calendar and email
- RoyalDrive
- Identity Finder
- CMS Training
- Basic Computer Use

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 would have them post about you.
- Help the authorities fight cyber-crime: Report stolen finances or identities and other cyber-crime to the TSC at ext. 4357.
Has your office moved?

Did you know.....
That if your new location information is updated only in BANNER, it will NOT be reflected in the Faculty/Staff Directory. However, when you take a few moments to update your information via the portal, both BANNER and the Faculty/Staff Directory are updated immediately.

Follow the steps on the next page, column on the far right, to update your information.

Desktop Services Updates
by Danielle Morse
Assoc. Dir. Desktop Services, IT Services

Thin Clients now available on campus

IT Services is pleased to announce the availability of a new type of desktop computing in WML and BRN: the Thin Client - also referred to as virtual desktop infrastructure (VDI). These clients function as a regular PC but lack a typical hard drive with software installed directly on them. Instead, the desktop runs from a server located in our data center. In our continuing efforts to lower costs and provide a more secure computing environment, we deployed 190 Wyse P20 clients to WML and BRN that have these benefits:

• Lower cost than a traditional PC
• Takes very little space on the desktop
• New software deployments are much quicker
• Sensitive data is stored in the secure data center reducing security risk
• IT costs are reduced due to fewer technical support issues
• Uses under 7 watts of electrical power, more than 10 times less than a typical desktop computer.
• Silent in operation, no fans, no spinning hard drives
• No moving parts mean a longer expected working life
• Support to the University’s effort to become more sustainable

The Wyse clients have no floppy or optical (CD/DVD) drive. Your documents can be easily copied to a USB flash drive or saved to your RoyalDrive account. IT Services is looking at the feasibility of expanding VDI to other computer labs, classrooms and offices across campus when the equipment is due for replacement.

Summer Lab Updates
by Danielle Morse, Assoc. Dir. Desktop Services, IT Services

Over the summer, most lab and classroom computers were updated to Windows 7 as well as the latest standard software including Microsoft Office 2010, Sharepoint Designer 2007, Internet Explorer, Firefox, Adobe Reader, Flash, Shockwave, Windows Media Player, JRE, Cute PDF, Core FTP Lite, NVU, KompoZer, Open Office, pgina Forefront and Deep Freeze. Lab facilities that did not get converted to Windows 7 yet will be upgraded to Windows 7 during the fall semester.

As part of our continuing efforts to make our campus more secure, we changed the way students, staff, and faculty log into the computers in labs, classrooms, and conference rooms on campus. You can now login to these computers using your Royal ID for Username and your my.scranton Password. Office desktop and laptop computers are not affected.

Lab Stats
IT Services recently purchased a PC lab and application tracking solution from Computer Lab Solutions called LabStats. This software has been installed in lab facilities and will track the amount of use lab machines get as well as the number of times certain applications are launched. The statistics we will gather from this program will help us target which labs should get what software and provide the appropriate number of computers in each facility. Since it can track application usage, expensive applications that are no longer being used can be removed to help decrease software costs.
Information Resources is currently working on the creation of an IT Service Catalog. The Service Catalog will provide a simple, easy to understand, consolidated collection of services that we provide to our user community. In many ways it is a one stop shopping site for our customers to find out how Information Resources can help them. Customers will be able to find information on services including user accounts & access, obtaining classroom support, requesting new workstations, and what types of consultative and application development is available to them. All services that IR offers from the Infrastructure, Application & Development, and IT Services departments will be included in the Service Catalog.

The Service Catalog will include basic information about each service including: an explanation of service; benefits of the service (why would customers need this service); features (what’s included); ways to request the service; service availability; on-line support (tutorials, PDF’s, FAQ’s, self-help); training information; and policies related to Service.

Once completed, the Service Catalog will clarify services and expectations for our customers, as well as, establishing service level expectations among our IR staff. Obtaining help from IR will be easier and customers will know ahead of time what level of service they can expect from IR.

Members of a working group are currently working on the catalog design and collection of information. A draft version will be provided to the Information Resources Advisory Committee later this year.

### Brennan Hall Remediation Project

by Jason Oakey
Instructional Technologist

Phase I of the Brennan Hall remediation project has been completed with great success. All of the first and second floor classrooms have been upgraded with new equipment including all display devices, wiring infrastructure, instructor PC’s and in two of the rooms, Symposion annotative devices were added due to the lack of whiteboard writing space. OIT staff worked closely with JP Lilley (AV integrators), Marooney and Sporer (electrical contractors), the Registrar and our own Network Infrastructure folks to complete these rooms in just over a weeks’ time. This included the removal of the old equipment, the installation of the new equipment and programming the rooms.

The addition of a new flexibly controlled lighting system gives these spaces the added user options of operating the lighting from the touch panels, an interface located near the instructors station and a smaller remote position near the entry of each room eliminating the old malfunctioning system. The new control systems are now networked and connected to Extron Global Viewer, a product that will allow OIT staff and the TSC to remotely support the classrooms. Along with the remote support capability, we will be able to run reports on equipment usage to help plan for future upgrades. The system will also provide OIT staff with notifications on items such as lamp hours, in the hopes that we can replace it before it burns out during a class.

Initial feedback from faculty is promising; several have conveyed their appreciation for the updates as well as for the ease of use of these new classrooms.
Infectious emails

Have you ever gotten an email from a friend telling you to "check this out!" Double-check that it's legitimate before you click. Hackers have become more sophisticated at fraudulent Internet activity, so online interactions aren't always as innocent as they may seem. In a recent survey, some risky behaviors that respondents acknowledged:

- 9 percent of workers have downloaded a virus on their computer at work.
- 18 percent of workers have opened an attachment or clicked on a link from a sender they didn't know.
- 18 percent have looked at a website that they knew wasn’t secure while at work.

SANS Computer Security Awareness Videos

by Jack Williams, IT Training Specialist

Faculty and staff are reminded that one of the easiest and unique ways to help learn about threats to university and personal data on our computers, is to take our SANS Security video training. Just by viewing these short, 3-4 minute videos, we can learn how we, the computer users, not just the computer itself, can be the prime target of identity thieves and other bad actors trying to access our information, and what steps we can take to prevent unauthorized access to our data.

If you haven’t as yet, taken this important training, you can by going to this website: https://vle.securingthehuman.org/mod/client/auth/login.php.

Login with your former email address, i.e., williamsj4@scranton.edu., for Username; and for Password, use your former password, (prior to Live@ed). If for any reason you have difficulty logging on, contact jack.williams@scranton.edu. Your password will be reset and another sent to you from SANS Security.

Our Shared Responsibility

National Cyber Security Awareness Month

Project Pipeline for Fall 2012

by Lorraine Mancuso, Director Project Management Office

The Project Management Office has released the project portfolio for the Fall 2012 timeframe.

In the Research Pipeline you will find the development of a Campus Virtualization Plan which will also focus on a plan to define any software which can be virtualized. Requirements will be defined for the last phase of implementing Network Access Control for Alumni Memorial Hall. The next Banner upgrade to version 9 is being planned. Requirements are being gathered to automate the employee new hire process which will eliminate various manual efforts.

In the Pilot Pipeline you will find that Lecture Capture is being tested in the Loyola Science Center. Special thanks to Jeremy Sepinsky who is working closely with OIT. Virtual Desktops, which have been placed in Weinberg Memorial Hall and Brennan Hall, will be monitored closely over the Fall semester. The data gleaned from that pilot will set the direction for the future of virtualized environments across campus.

In the Implementation Pipeline, leading the priority list is a much needed upgrade to the 20 year old Royal Card process. The new system is on an aggressive timeline which brings the system on-line late December.

The my.scranton portal will be upgraded to version 5 providing several welcome enhancements and is expected to be released in the Spring. There are many outstanding projects looking to leverage the Footprints product. The desire to complete sub-projects, postponed by last semester’s priorities, gained focus and will be a top priority for the next 8 months. Now that Active directory is fully functional, integration into a variety of processes will commence. The final critical part of the ERP Migration, Documentation, has been defined as a separate project. The campus Wireless project which will address outdoor spaces will be on hold for the Fall pending budget review.

Projects exiting the pipeline are the Email and Calendar Migration to Live@ Edu and the completion of the Loyola Science Center. The creation of a Business Continuity/Disaster Recovery Plan will also be completed this semester.

For more details on any projects within the portfolio please contact the PMO.
Phishing:
Online criminals are often financially motivated to steal your information, whether or not they know who you are. They dress the part, talk the talk, and by pretending to be something or someone they’re not, they try to get your personal details. A phishing website or message tries to trick you into revealing personal information by appearing to be from a legitimate source, such as a bank, social network, or even Google.

Auction fraud:
Scam from sales on Internet auction sites or the non-delivery of products purchased through an Internet auction site. The seller may say he or she lives in the U.S. but tells the victim to send money outside the country for business reasons or a family emergency. The seller may also ask you to wire funds directly to him/her with a bank to bank transfer. That way the money is virtually unrecoverable.

Credit card fraud:
The Internet Crime Complaint Center has received multiple reports alleging foreign subjects are using fraudulent credit cards. The unauthorized use of a credit/debit card, or card number, to fraudulently obtain money or property is considered credit card fraud. Credit/debit card numbers can be stolen from unsecured websites, or can be obtained in an identity theft scheme.

Loyola Science Center Phase II Moves

With the completion of Phase II of the Loyola Science Center, a team was once again assembled to move approximately 50 employees.

History is now housed in St. Thomas Hall. Theology and Philosophy have returned to the 4th and 5th floors of the Harper McGinnis wing which is now part of the Loyola Science Center.

Biology, Chemistry and Math have relocated to the new construction which was completed last year.

Tips on Preventing Identity Theft
October is CyberSecurity Month

ON-LINE Safeguards
1. Create Strong Passwords and change them often. (Use upper and lowercase letters, numbers, and symbols with a minimum of at least 9 characters.)
2. Don’t use your University password for any on-line log in. Create strong, new passwords for sites that require them.
3. Only navigate to trusted web sites.
4. Avoid downloading files or images from sites you don’t know.
5. If banking on-line, check your balances DAILY to spot irregularities.
6. Don’t give out personal information or transact business over public WiFi networks. Information can be easily intercepted.
7. Don’t share too much personal, financial or location information on social media sites like FaceBook.
8. Avoid sites offering “too good to be true” offers.
9. Never give out your Social Security number to any site. See if you can make other arrangements such as using the US Postal Service.
10. Set your browser(s) to clear your History and your Cookies.
11. Report any problems to TSC at ext. 4357.

Important contacts:
Technology Support Center - techsupport@scranton.edu
Phone (570) 941-4357

IT Services Training - www.scranton.edu/it_training

Stay Safe Online
STOP. THINK. CONNECT.
www.scranton.edu/staysafe
Malware Examples

**Virus:** a computer program that can copy itself and infect a computer.

**Worm:** a self-replicating malware computer program, which uses a computer network to send copies of itself to other computers on the network.

**Spyware:** a malware that collects small pieces of information about users without their knowledge.

**Adware:** any software package which automatically plays, displays, or downloads advertisements to a computer.

**Trojan horse:** a destructive program that masquerades as an application. The software initially appears to perform a desirable function for the user prior to installation, but steals information or harms the system.

Source: Google

---

**GlobalViewer Enterprise**

** Already seeing the benefits**

by Rob Kennedy,
Sr. Instructional Technologist, OIT

During the past ten years, the Office of Instructional Technologies (OIT) has seen a tremendous increase in the number of mediated facilities on campus. The increase in maintenance responsibilities coupled with additional job responsibilities has forced OIT into a predominantly “reactionary” model of support. In an effort to address this issue, OIT implemented Extron’s GlobalViewer Enterprise (GVE) this past summer. We believe this product will help OIT make great strides in balancing the proactive/reactive scales of support and maintenance.

GVE is a classroom management system that monitors the status of audiovisual equipment installed in classrooms. The monitoring and alert capabilities of the product allow for a quicker response to classroom equipment issues. It also allows OIT staff to get a better handle on when preventive maintenance is required. GVE offers a dashboard feature that examines remaining lamp hours, temperatures and other vital statuses of the audiovisual technology. This monitoring platform decreases downtime in classrooms by allowing for proactive responses to potential classroom problems before they arise. The remote control capabilities of the GVE allow OIT staff to support instructors in classrooms from remote locations. These remote features include turning equipment on and off, switching sources, adjusting volumes and in some cases controlling the lights. Remote responses allow OIT staff to assist an instructor experiencing a system malfunction during class without wasting 10 to 15 minutes walking to the class.

Although GVE was installed primarily for its monitoring and remote control capabilities, it has provided great “green” benefits to the University as well. Since all classes on campus are required to take place between 8:00AM and 10:00PM, GVE automatically turns off all of the technology in monitored classrooms at 10:30PM and does not allow it to be turned on prior to 7:00AM. This not only prevents equipment from accidentally being left and thereby conserving energy; it also extends the useful life of audiovisual equipment and consumable items such as lamps and filters. This feature alone is projected to save OIT thousands of dollars each year in projector, lamp and filter expenses.

Currently, GVE is monitoring the status of audiovisual equipment in 23 classrooms across campus. OIT is poised to add another five rooms during winter break and another 20 next summer.

---

**Mobile Phone Security Tips**

- Keep your system updated
- **Get rid of security holes or vulnerabilities by maintaining updated software on both your PC and your smartphone.**
- Install a security application
- A reliable security app safeguards your data, protect against threats and locate your lost or stolen phone.
- Be careful where you click and land
- **Be sure a website starts with “https” before you enter sensitive information.**
- Avoid shopping or banking on a public network
- Keep in mind that public Wi-Fi is mostly not secure.
- Get applications from trusted sources
- Try to avoid 3rd party apps.
- Make it a habit to check each app’s data access on your phone
- A game app doesn’t need access to system files, phoning or messaging data.