ITS Battles Webmail Phishing – Please join the fight!

According to OnGuard Online, “Phishing is a scam where Internet fraudsters send spam or pop-up messages to lure personal and financial information from unsuspecting victims.”
www.onguardonline.gov/topics/phishing.aspx

Phishing is the act of casting “electronic bait” with the hopes that a few people will bite. Webmail phishing is a subset of phishing whose objective is to gain login credentials for a user with an email account that can be accessed via a web page from a remote location. The vast majority of webmail phishing attempts are directed against colleges and universities. Surprisingly, numerous students, faculty and staff at all kinds of educational institutions respond to webmail phishing messages just about every day. Webmail phishing emails look official, threaten an unwanted action, such as deleting the email account, and either include a link to a webpage that collects the user’s private information or asks the recipient to reply to the email with personal information, including login id and password.

“We would never ask our users to send a password or any other personal information to us in an email.”
Dr. Frederick Ullman
Director of Computing Services

According to Dr. Frederick Ullman, the Director of Computing Services at SUNY Fredonia, webmail phishing is a serious problem for the campus “We would never ask our users to send a password or any other personal information to us in an email.” We do send emails to alert users of accounts closing or when an email inbox is over its quota, but we would never ask a user to send us any personal information nor would we send a link in a message that brings up a webpage that asks a user to enter a password or any other personal information.

Several thousand webmail phishing messages are sent in a typical week to SUNY Fredonia email accounts. An email filtering process detects and deletes almost all of them before they reach the intended recipient(s). Occasionally a webmail phishing message slips past the detection process, is delivered, and a SUNY Fredonia user subsequently responds with his/her login id and password. The spammer then gains access to the responding user’s SUNY Fredonia email account and uses it to send large quantities of email spam messages. SUNY Fredonia is identified as the source of the spam and our outbound email is blacklisted.

See PHISHING page 5

Win a $10 Gift Card!

If you receive an email that appears to be webmail phishing, and the email subject does not include the text “SCAM WARNING”, it’s almost certainly an undetected new attempt. If you are the first to report a previously undetected webmail phishing message, we’ll send you a $10 FSA gift card. Forward the email to alert@fredonia.edu and if you are the first to report an undetected webmail phishing attempt, you win!

How can you recognize a webmail phishing scam?

- A generic greeting, such as “Dear Fredonia.edu User”
- Asks that you reply with your password
- Contains a link to a site that contains areas to enter your username and password
- Obvious typos or grammatical errors in the message

IN Inside THIS Issue
1 Phishing
2 Houghton Lab Upgrade
3 Meet Alex Moon
3 ITS Highlights 2008—2009
4 Banner Birthday Party!
5 iTunesU Pilot

www.fredonia.edu/its  its@fredonia.edu  716.673.4670
As part of the ITAB Lab 3 year renovation cycle the computer lab in Houghton 122 received new equipment this summer. The project was headed by AIT staff member Christopher Taverna, with assistance provided by AIT Director Colin Plaister and Douglas Johnson, also of AIT. Student employees Max Henstel, Tom Kramer, and Jeff Utter completed the workforce for this project.

The work began during the Spring 2009 semester when the members of the ITAB Lab Subcommittee approved the proposed budget for renovating the lab. The budget proposal included new computers and monitors, upgraded software, new printer, new projector and screen, and new tables for the 25 station lab. Physical work in the lab took place in the two week period from June 29 – July 10. The old computers and monitors were reassigned to the lab located in the Media Center in Thompson Hall.

Dr. Ann Deakin, Geosciences, had this to say regarding the renovated Houghton Lab, “I’m looking forward to showing off the renovated Houghton Lab to our new and returning students. First and foremost, the new computers are much faster and the new monitors and graphics cards vastly improve the visual display. The new tables will provide a more comfortable working environment for the students, while providing me with more room to get around and troubleshoot individual problems. I should be able to more effectively demonstrate lab exercises given the new projector system and the NetSupport application.”

For more information on the ITAB Three Year Computer Renovation Plan please see: http://www.fredonia.edu/its/itabrenovation2008.asp

Identity Management Investigation Begins

ITS is in the early stages of investigating better ways to give new students and employees their accounts, maintain account changes and remove accounts from our systems when students graduate and employees leave their positions. We are researching how we can:

- Give system access and accounts to disparate services in a more timely fashion
- Collect account changes, such as a name change, in a central location and distribute the change effectively across all of our systems
- Give our users easier ways to change passwords, to name a few.

This project is related to the single sign-on initiative included in The Fredonia Plan SUNY Fredonia’s five-year strategic plan.

Banner 8 Upgrade

Banner will be upgraded (from the current 7.3 version to version 8.1) this coming November. The upgrade requires that the production system, and web links such as Your Connection, be offline and unavailable for 4-5 days. The upgrade has been tentatively planned from the close of business Thursday, November 19th through the close of business Tuesday, November 24th.

Keyboard & Mouse Cleaning Tips

All computer labs and smart rooms will have sanitary wipe dispensers available, and individuals are encouraged to wipe keyboards and mice prior to use, especially during cold and flu season! Individuals in offices are encouraged to do the same.
Thinking of purchasing a “Smart” Phone?

If you are considering purchasing a personal smart phone, and plan to send and receive SUNY Fredonia email and calendaring information, please purchase one that utilizes Windows Mobile OS. Refer to your product manual for setup instructions.

Meet Alex Moon

Alex Moon is the newest addition to the ITS Department holding the position of Help Desk Technician / Consultant. A native of Tampa, FL, Alex moved to Fredonia with his family and graduated from Fredonia High School before moving on to graduate from SUNY Fredonia in 2004. His family has owned and operated Central Station Restaurant in Dunkirk for the past 20 years. Before his employment with SUNY Fredonia, Alex held the positions of IT Specialist and OSP Engineer with DFT Communications. He currently resides in Fredonia with his wife, Allison, and 1-year-old son, Liam.

Information Technology Highlights from 2008-09
by Karen Klose

http://www.fredonia.edu/helpdesk/Policies.asp

A project management office, with the addition of a second project manager, was initiated with the intent to manage large ITS projects and all projects spanning more than one ITS unit. Project managers and project participants concluded thirteen projects, including assisting University Advancement and Student Affairs with completion of various IT-related projects including a scholarship awards and accounting business process.

A multi-layer defense against web phishing attacks was developed and implemented that included 1) Detecting webmail phishing messages and preventing delivery of messages to intended recipients (more than 6,300 known addresses currently and growing daily), 2) Examining all outbound mail for addresses of known ‘reply-to addresses’ used by webmail phishers and filtering these for deletion and, 3) Examining all e-mail outbound to the Internet for patterns that fit the initial password issued to Fredonia AD accounts. Messages are flagged and held for manual examination. In addition to these defenses, it is critical that individuals NEVER share passwords. Even if the request looks legitimate it is NOT!!

Data Communications upgraded the entire wireless network to 802.11n specification, increasing connection speed from 54 to 130 megabit. All academic buildings and many outdoor spaces now provide wireless access for students, faculty, and staff.

A capital funding investment of 2M allowed Data Communications staff to upgrade the network infrastructure with gigabit to the desktop in all academic buildings and in most administrative areas, with 10 gigabit distribution to server switches and core buildings, with network switch upgrades for secure management, and installation of a pair of large scale security appliances to provide increased firewall protection to accommodate increased Internet bandwidth, and to provide automatic failover in the event of hardware failure.

Institutional Internet bandwidth contract increased campus access speed from 120 megabit to 500 megabit with renewal options to 2.5 gigabit.

A redundant fiber connection from our Internet provider was completed as part of our disaster recovery planning and proved effective when the original connection on Central Avenue was inadvertently cut during repair of a water main break. Without this redundant connection academic and business services would have been off-line for an intolerable amount of time and with great cost to the institution from a marketing and service provision perspective.

Academic Information Technology converted the distance learning facility in E335 Thompson Hall to a multi-use facility with the addition of computer and projection equipment and a Tandberg Edge 95 to upgrade video conferencing.

See HIGHLIGHTS page 5
Dear Geek by The Geek

Dear Geek:

I sometimes get email messages that say I will be losing my email privileges or that a bank or company is asking me to verify something on my account. Sometimes a link is provided for me to login. Should I reply to the email or click on the link?

A Fredonia Computer User

Dear Fredonia Computer User:

No, NEVER reply. SUNY Fredonia will NOT send out an email asking you to verify your information via a web link or directly ask you for your login password or PIN.

Banking institutions, including credit unions, will never ask for this personal information via email. PayPal, eBay, Amazon and other such vendors won’t ask for this either. The Internal Revenue Service will never ask for any personal information directly via email or with an embedded link in a message asking you to login.

Individuals asking for this type of information via email are “Phishing”. Phishing is the practice of requesting confidential information over the Internet under false pretenses in order to fraudulently obtain credit card numbers, passwords, or other personal data. [Dictionary.com]

Stay safe. Don’t respond.

The Geek

Ask The Geek!

"Dear Geek" is written by ITS staff members. If you’d like to ask The Geek a question, please send an email to ITS@fredonia.edu with Dear Geek in the message subject.

2009-2010 ITS Projects

It’s another busy year for ITS. Here are a few of the projects we are working on:

- Upgrade to Banner 8
- Upgrade to ANGEL 7.4
- Online Course Evaluations pilot
- Activity Insight software implementation
- SIRIS (SUNY Institutional Research Informational System) changes in state reporting requirements
- Identity Management investigation
- Workflow Software investigation
- COS system changes
- Student Activities transcripts
- Online textbook information for students
- SUNY HR conversion
- Online Academic Standings letters for students
- Wireless Printing investigation
- Learning Management System investigation

Banner Turns 10!

Remember those jammin’ Banner Babies? Our Banner student information system is 10 years old on September 28th!

Please relay birthday greetings TODAY via http://tinyurl.com/nleapu for inclusion on a ‘birthday banner’, and mark your calendars to celebrate with birthday cake and ice cream on September 28th from 1:00-2:00 in the English Reading Room, 127 Fenton Hall.

Tech Watch

Editor: Janet Mayer
Design: Charlotte Morse
Contributors: Karen Klose, John McCune, Lisa Melohusky, Alex Moon, Colin Plaister, Christopher Taverna, David Torres, Fred Ullman, Gale Verhague, Andrea Wasiura, Cathie Zakrzewski

Tech Watch is published 3 times a year by Information Technology Services. Please send feedback to its@fredonia.edu.
Fall 2009 iTunes U Pilot

iTunesU is a service provided by Apple, Inc. which assists colleges with the management, distribution and access to audio and video content for use by students. A task force investigating streaming media solutions recommended an iTunes U pilot during this academic year to assess ability to meet media-rich course content needs in addition to assessing the cost and requirements to implement and support campus-wide use. SUNY Fredonia implemented an iTunesU site this summer and is piloting the use of this service for six professors courses for the Fall 2009 semester. iTunesU was integrated with our ANGEL learning management system to allow students to access audio and video content from iTunesU through their ANGEL courses. The goal of this pilot is to determine the feasibility of continuing and expanding this service for the faculty and students of SUNY Fredonia. This pilot will run again for the Spring 2010 semester. Pilot applicants must already have audio/visual content ready for posting, be able to attend iTunesU training sessions and provide feedback about the pilot program. Stay tuned for an announcement about applications for the next pilot. If you have questions about the pilot, contact Lisa.Melohusky@Fredonia.edu.

From PHISHING page 1

When we are blacklisted, our users are unable to send email to individuals whose email providers subscribe to the blacklisting services. Getting our systems removed from a blacklist is never easy and not always possible. There are also significant and unpleasant consequences for the user whose email account was compromised.

What YOU can do
Never reply to an email that asks you to provide personal or password information. If you make a mistake and supply your password, once you realize what has happened, immediately change your password and alert the Help Desk via https://fredquest.fredonia.edu/ or by phone 673-3150.

What ITS does
If you report the incident right away, there’s a good chance that our email administrators can review your account to identify and remove any revisions, such as forwarding rules that were made by someone other than you. In some cases, messages deleted by the intruder can be restored. Details of the original message will also be reviewed to identify the other recipients and to help prevent delivery of similar messages. We keep the email filters as updated as possible to catch new phishing scams before they reach you.

Be Safe!
Keep your sensitive information private

ANGEL 7.4 Upgrade

ANGEL Learning released their ANGEL 7.4 in May 2009. SUNY Fredonia will be upgrading to ANGEL 7.4 on December 28, 2009 to December 29, 2009. ANGEL software will not be available for use for these two days. ANGEL 7.4 changes include:

- **Deprecated Quiz Tool** – ANGEL 7.4 does not include the Quiz tool. Assessments replace the quiz functionality. If you use ANGEL Quizzes, your quizzes will migrate to the new assessment tool.
- **Rubrics** – Create assignment rubrics, share them, check inter-grader reliability and associate them with standards and objectives.
- **Gradebook Improvements** – The new gradebook includes single screen access, term-based reporting and improved grading workflow.
- **Lesson Plan Builder** – Create lesson plans associated with standards and objectives and share your plan with other ANGEL faculty.
- **HTML Editor Google Tool** – Search for an embed images and video into courses directly from Google without leaving ANGEL.
- **Much More!** – Improvements were made to surveys, RSS feeds, standards, content exchange, repositories, assessment item analysis, and security roles.

Read more about ANGEL 7.4 here: http://www.fredonia.edu/edtech/angel/docs/7.4.pdf

From HIGHLIGHTS page 3

Five computer labs received new equipment, software, and in some cases furniture this summer! Check the AIT web page to view pictures of 122 Houghton, 2016 and 2017 Mason, 115 Fenton, and 309/310 Rockefeller!

The Programming Team completed the final phase of the VMS to Linux Banner conversion following a considerable investment of staff time over the entire year, with minimal impact to the campus.

SUNY Fredonia received the fourth ANGEL Impact Award (the most awarded to any institution) for the College of Education Enterprise Data Management System.

Academic Information Technology is currently transitioning five traditional classrooms: 175 Fenton, 220 Jewett, E327, E120, and E122 Thompson to ‘smart’ classrooms for use during the fall semester. Additionally, DVD decks have been installed in all smart classrooms.

Data Communications and the Help Desk team assisted with the Maytum Hall move, concluding with minimal network connection inconveniences.
Learning Management System Update

In May, ANGEL announced their merger with Bb. Soon afterwards, SUNY Learning Network announced there would be no significant changes to our ANGEL hosting in the short term. Their long term strategy is “to work with the SUNY Community to evaluate all the options.” Janet Mayer, ITS Project Manager, is a member of the SUNY Learning Network Applications Work Group that will be researching LMS directions for SLN.

Additionally, SUNY Fredonia will commence its own investigation of LMS options. During the 2009-2010 academic year, a small group will gather information on options and test various systems. A task force will be formed for the 2010-2011 academic year to evaluate options and decide which platform best suits our needs. Once this decision is made, migration planning will take place. If you are interested in being a part of LMS investigation, please email Janet.Mayer@Fredonia.edu.

Mark Your Calendars!
Software Security Patch Deployment to Windows Computers Tuesday’s at 12:00 AM

In the ongoing effort to improve all aspects of computer security on campus, Information Technology Services is employing new software that can detect and deploy missing security patches on your Windows computer that fall outside of the regular Microsoft security patches. Due to the fact that the deployment of these patches could cause some slowness and inconvenience to you, the following plan has been developed to minimize the impact these deployments will have.

Deployments will occur to random computers across campus each Tuesday morning at 12:00 AM. In order for the deployments to be successful, your computer must remain powered on but you must be logged off. If you typically shut your computer down at the end of each day we ask that on each Monday you Save All Work and Close All Applications and then Log Off your computer before you leave. Please leave the computer ON. You may turn off your monitor after you log off, but the computer must remain running. The deployment will then take place with no inconvenience to you the next day. Please note that if you Shut Down the computer the deployment will begin when the computer is powered on. This will most likely cause a considerable slowdown of your computer, and once the deployment is complete will require you to restart your computer, causing even more inconvenience.

These patches will be deployed to work-study machines and kiosks as well as faculty and staff computers, so if you are responsible for those machines in your area, please be sure that they are logged off but remain powered on.

If patches are being deployed to a computer that is either not logged off, or if it is powered down, you will see the following message on your screen:

If you see this message on your screen, please log off your computer as soon as possible to complete the deployment. For those of you who regularly power machines off each day as a conscientious sustainability measure, we apologize that Mondays will need to be an exception. Maintaining regular security patches is a critical step in maintaining an accessible and reliable computer environment. Your assistance with improving the security of the campus computer environment is greatly appreciated.

www.fredonia.edu/its  its@fredonia.edu  716.673.4670