SECUREPURDUE NEWS
www.purdue.edu/securepurdue

October 2007
Volume 1, Issue 11

All the news that's secure to print.

October Security Awareness Month

Internet Security: Your Ticket to Ride!

This year's events will focus on using the Internet safely and discuss emerging trends in information technology

WHEN: October 10, 17, 24, and 31, from 9 to 11a.m.
WHERE: Fowler Hall in Stewart Center
HOW: Register online http://www.purdue.edu/securepurdue/training

October 10: Internet Riding Safely
Scott Ksander, Chief Information Security Officer and Executive Director of Networks and Security of Purdue University and Pablo Malevenda, Associate Dean of Students, will discuss ways to safely use the Internet, including appropriate information to share on social networking sites like Facebook. Neil Daswani, an engineer from Google, will talk about security issues.

October 17: Cybercrime and Copyright Infringement
Computers and networks have become a tool and a target for criminal activity. Amber, a Purdue student who was sued by the RIAA for illegally downloading songs, will speak about her experience. Mr. Chris Burgess, CISCO Senior Security Advisor and Chief Scientist, will speak on intellectual property strategies, and Purdue Professor Marcus Rogers will speak on the law and Cyber Forensics.

October 24: Future Destinations: Trends in Technology
What new technology will we see next year? What trends will we see? Will these be good or bad? Come listen to Professor Ed Delp, The Silicon Valley Professor of Electrical and Computer Engineering and professor of biomedical engineering. George Heron, VP and Chief Scientist for McAfee, will share security and technology trends.

October 31: Destination Unknown
In the United States, higher education has had preeminent status since 1936, but is currently experiencing negligible growth, impending enrollment declines, and heightening competition. What might higher education look like in 2020? How will technology impact its changing face? Join Purdue's CIO, Gerry McCartney, and watch a short video, "School of Athens or Mr. Ford's Factory: IT and the Future of Higher Education." Then find out who wins our second annual Security Halloween Contest!

In this issue

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

October is National Cyber Security Awareness Month. We are looking forward to a number of interesting events during the month to promote cyber security awareness. A number of nationally recognized speakers will share their insight and current and future security issues. The sessions are open to everyone and we believe that this opportunity will provide valuable information for all, regardless of your level of technology experience.

Cyber security is not just something we need to practice during October, however. We need to make cyber security a habit in our daily lives.

See CISO, Page 3

Information Security Policies Creation

Creating information security policies is not an exact science; in fact, it is more of an art form. Many factors need to be considered as information security policy is created. Business process needs, technology advancements, and training and education need to be considered each time a new policy is discussed.

Sometimes a policy may be a very good idea from a security standpoint in that it helps protect the University and its data, but when considered with respect to business processes, the policy may be less than ideal. A number of University groups work together in order to develop University-wide IT policies, standards, guidelines, and procedures and make sure that the policy documents work of all areas of the University.

As policies are initially discussed, ITNS works closely with the University Security Officers' Working Group and its various sub-committees to hash out the finer points of the policy and ensure that the policy is both technologically sound and applies to a broad base at the University.

The University Security Officers' Working Group is comprised of one representative from each of Purdue's 34 IT areas, and provides technical input and leadership for the SecurePurdue program.

Joanna Grama, an Information Security Project Manager for ITNS whose main responsibility is creating information security policy is pleased with the working relationship with the University Security Officer's Working Group and its policy sub-committee. "The Security Officers really do a good job of thoroughly going over each policy draft, ensuring that technology objectives are met and described clearly,"

creating information policies is more of an art form.....

Grama said. "I really feel that this type of large-group review creates better policies because many people with varying experience and expertise are looking at and revising a policy prior to the policy ever being presented to higher levels of the University. We know that our policies are technically sound for the University computing environment because of this type of review." Once an information security policy is reviewed and approved by the University Security Officers' Working Group it is presented to the IT Executive Steering Committee for discussion.

IT policies are reviewed, at a minimum, by the University Security Officers' Working Group, the IT Executive Steering Committee, the Vice President for Information Technology, the Executive Vice President and Treasurer, the Provost, the University President, and University Legal Counsel.

Larry Guentert, the Security Officer from the University Development Office, appreciates the new approach to drafting information security policies. "As an IT person who struggled with the Herculean task of writing computer policy at the department level, I was struck with the very pragmatic approach that ITNS and the Security Officers' Working Group has adopted for new information security policies," Guentert said. "By employing a hierarchical structure of 'overarching policy/standards/guidelines/procedures' to separate the underlying details from the overall intent, complex policies are now easy to read and understand, as well as administer and maintain."

More information about the University Security Officers' Working Group can be found at: http://www.purdue.edu/securePurdue/securityofficers/index.cfm

SPOTLIGHT

New End User Security Guidelines Adopted

On September 7, 2007, the University Security Officer's Group and IT Networks and Security (ITNS) issued a new End User Security guideline. This new guideline was developed in order to ensure that every member of the Purdue community who uses a computing device makes Purdue's computing environment more secure. The guideline is actually an extension of the "Security Checklist" that ITNS has used in its educational activities for a number of years.

Some items under the guidelines state that end users are expected to apply computing device security software patches and updates regularly; install and use anti-virus and anti-spyware software on computing devices; and regularly verify that system security measures are enabled on your computing device.

The guideline also states that end users are responsible for implementing the guideline's requirements on computing devices under their control which interact with Purdue's computing environment. In the event that a specific computing device lacks a feature specified in the guideline, the guideline directs end users to implement security features appropriate to the underlying computing device.

The guideline also directs Purdue employees and other end users whose computing devices are supported by Purdue central or departmental IT units to check with their respective IT representatives prior to making changes to the security settings of those Purdue provided devices.

Guidelines can be found on the SecurePurdue webpage at http://www.purdue.edu/securepurdue/bestPractices/endUserSecurityGuidelines.cfm

STEAM-CIRT NEWS

STEAM-CIRT is a security team and IT incident response team organized under the ITNS group within ITaP.

For more information about STEAM-CIRT and for security updates throughout the month, visit the STEAM-CIRT Web page at: http://www.purdue.edu/securepurdue/steam/

Top 10 Purdue email viruses

The following list is a 30-day snapshot of the most active email viruses on the Purdue campus.

The maximum occurrences found in one day are listed with the names of each major virus.

(30-day snapshot as of October 11th)

Viruses	Max.	Last
W32/MyDoom-O	1199	305
W32/Dolebot-A	1762	19
W32/Mytob-D	125	46
W32/Netsky-P	177	53
W32/Virut-A	138	3
W32/Sality-AA	141	141
W32/MyDoom-AJ	106	8
W32/Mytob-CN	79	6
W32/Parite-B	86	8
W32/Mytob-HM	62	14

CISO from Page 1

Here are some habits we have suggested in this newsletter and we hope you will incorporate into your "cyber life."

• Protect your personal information and that of others. It is valuable.

• Know who you are dealing with online. The cyber world is full of just as many dangerous people as the physical world.

• Use anti-virus software, a firewall, and anti-spyware software to keep your computer safe and secure.

• Be sure to set up your operating system and web browser software properly, use the most restrictive settings that continue to let you get necessary work completed, and keep your system and applications software updated with current fixes and patches.

• Use a strong password or other authentication technologies to help protect your personal information and information entrusted to you.

•Learn what to do if something goes wrong with your system. Things can happen quickly when your computer is connected to the Internet and ignoring problems is never the right answer.

Think before you click. Some clicks can take you on adventures to "virtual destinations" that you didn't want to visit.

These are good habits that can help keep you safe as you move your way through your "cyber life." I hope to see you during the October events and, as always, be careful out there.

MILESTONES

Authentication and Authorization Policy Signed!

A newly revised Authentication and Authorization Policy (V.1.2) was signed by Purdue University President France Córdova on September 25, 2007.

The revised Authentication and Authorization policy employs a standardized mechanism for identification, authentication, and authorization to access University resources. The revised policy may be found at http://www.purdue.edu/policies/pages/information_technology/v_1_2.html.

Issued simultaneously with the revised policy is a supporting standard called the "User Credentials Standard."

The user credentials standard is intended to explain the different types of credentials that may be issued to a member of the Purdue University community and how they should be used to protect University resources. At this time, the standard primarily addresses the use of passwords; however the standard will be added to in the future to include guidance on token based authentication as well.

The new User Credentials Standard also discusses the password expiration period for University passwords and employs a new process for determining the length of time a password remains valid.

Under the new standard, all University passwords must be changed at least every 120 days unless a staff person's assigned role requires 30 day changes.

Under the new standard, most students will be required to change their passwords every 120 days, rather than every 30 days.

Faculty, staff, student-employees, and other affiliates having access beyond the "Employee Self Service" and "Traveler" roles in the new OnePurdue system will be assigned a 30-day password expiration cycle in the OnePurdue system based upon those roles.

The new User Credentials Standard can be found at http://www.purdue.edu/securepurdue/bestPractices/passStandards.cfm.

SECURITY RESOURCES

Use the following resources to educate yourself about security and privacy issues surrounding computers and data networks.

- **October CyberSecurity Events**
  http://www.purdue.edu/securepurdue/training
- **End User Security Guideline**
  http://www.purdue.edu/securepurdue/bestPractices/endUserSecurityGuidelines.cfm
- **The new User Credentials Standard**
  http://www.purdue.edu/securepurdue/bestPractices/passStandards.cfm.
- **Authentication & Authorization Policy**
  http://www.purdue.edu/policies/pages/information_technology/v_1_2.html
- **How to determine your roles in OnePurdue**
  https://help.itap.purdue.edu/onepurdue/viewarticle.php?articleid=2540