



October 2008

Volume 3, Issue 3

All the news that's secure to print.

FROM the CISO



By Scott Ksander
Executive Director
IT Networks & Security

The start of the academic year always heralds new activity at Purdue. This year is no different and several exciting things are happening this year as part of the SecurePurdue initiative.

Initially, it is worth mentioning that October is National Cyber Security Awareness Month. We are looking forward to a number of interesting events during the month, focusing on the theme of "Secure Mobility." As the use of "take it anywhere" electronic devices is increasing, we need to remain committed to using those devices in as secure a manner as possible. This protects both our personal information and the University's data. Purdue events for Cyber Security Awareness Month will be held on October 8, 15, 22, 31. Sessions will be from 9:00am to 11:00am in Fowler Hall (located in Stewart Center). The month's events kick off with "Buckle Up! Laptop Security" and end with the much anticipated Cyber Security Halloween Costume Contest on October 31.

One item that we are very excited about this year is the implementation of the Networks Operation and Security Center (NOSC). The NOSC is responsible for monitoring the Purdue network for alarms or certain network and security conditions which may require special attention in order to avoid impact on the performance of the Purdue University network. The Center allows network and security issues to be analyzed before or as they occur, so that Center personnel can correct issues before they have a greater impact on the Purdue network. Many people have worked hard in order to establish the NOSC and ensure its successful start up.

In keeping with our theme of "Secure Mobility," one item that I am really excited about is the coming deployment of 802.11(n) on campus. The deployment of this wireless communication technology

In this issue

CISO message	1, 3
Password Vault	2
Urban Legends	3
October Cybersecurity Events	4
Security Resources	4

is being designed with an eye toward total wireless accessibility on campus. By the end of 2010 we hope to have 6000 802.11(n) wireless access points on campus.

The University's Wireless Network Acceptable Use Standard will be followed for the deployment of the 802.11(n) network in order to ensure seamless communications ability. We will be more aggressive than ever in protecting the services provided by the University and ensuring that those services are not downgraded through the use of non-authorized devices attached to the 802.11(n). Deployment of the 802.11(n) technology really will enhance "Secure Mobility" computing under the SecurePurdue initiative.

One last note at the start of the new semester. Purdue-targeted spam mail is continuing to hit Purdue University e-mail users at an alarming rate. News stories about the various spam variants are posted on the SecurePurdue web page. We continue to remind users to be suspicious of any unsolicited e-mail that requests you to visit a certain URL

Password Vault - Help for Remembering All those passwords

People have a plethora of computer accounts these days; e-mail accounts, online merchants, banks, professional organizations, social networking sites, etc. This leads to an overwhelming number of passwords and PINS that must be remembered. How can you securely keep track of them all? The answer is a Password Vault.

Can't remember all your passwords? Spending more time trying to find where you put the password than getting work done? Use a password vault then!

A Password Vault is a program that provides a central, secure location to store all these account passwords, PINS and other sensitive information and lock it all up with a single master password. With a Vault only the one master password need be remembered and all other passwords are securely encrypted in the Vault rather than being written down or stored insecurely on your computer.

There are many Password Vault programs available. ITaP's Identity and Access Management Office recommends one such program called Password Safe (<http://passwordsafe.sourceforge.net/>) for Windows-based computers.

According to Cherry Delaney of ITaP Networks and Security:

- Password Safe features a simple, intuitive interface that lets users set up their password database in minutes.
- You can copy a password just by double-clicking, and paste it directly into your application.

- Best of all, PasswordSafe is completely free: no license requirements, shareware fees, or other strings attached.

"I set up categories which allowed me to organize my passwords into specific folders: Professional organizations, Online Buying, Health Organizations, Accounts, etc. This tool has a very simple interface and each new entry allows you to store the organization name, your

user id, your password, the web URL to connect to when visiting the organization and even a place for notes to provide needed reminders when visiting the site.

PasswordSafe was created by a noted cryptography and security expert. It has many convenient features, among them; ability to track password expiration and history, generate random passwords, and passwords that comply with a preset password policy. It also integrates nicely with a web browser.

The master password for the password manager must be complex and strong. It should be at least as strong as the most sensitive password stored inside. If the password manager stores any passwords that are subject to the requirements of a password policy, then the same requirements should be observed for the master password.

More info at:

<http://www.purdue.edu/securepurdue/pswdManager.cfm>

SPOTLIGHT

CISO from Page 1

Urban Legends

The world is rapidly changing all the time. With the advancement of electronics, information can be delivered to millions of people in minutes. On the web, e-mail has made communicating with co-workers and friends simpler than ever before. A letter that would have taken a week for the person to receive can now get it the minute the sender finishes writing it. While most of these advancements have improved the way we operate in business, some things can be destructive.

Spam-mail is a term that is universally accepted as an e-mail that is received that is of little to no importance and in most cases was sent to hundreds of others of people. The reason it was sent to these people is they were all on the same mailing list. In a corporation, mailing lists can include everyone from the mail-room clerk to the CEO. When spam is sent in these cases it is typically harmless and usually just to create humor in the workplace. The problem however, is when these e-mails start taking up a large sum of the receiver's in box.

The other problem is that many of these e-mails include stories or rumors that can have no validity to them whatsoever. Even worse, is that some these e-mail are designed to scam the reader out of something of value. These scam e-mail are typically called phishing e-mail. Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as user names, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

When it comes to these rumors and scams, it is important to know the facts. Some of these rumors become chain mail when the story is so amazing that every person that reads it wants to share it with someone else. Before sending these messages out, readers should learn the facts on the issue. In most cases, the spam mail being circulated is multiple years old. Some chain mail is so old it has been done over general mail before there was e-mail.

or provide your Purdue Career Account credentials. IT Networks and Security recommends that users immediately delete the e-mail and do not reply or take the action requested in the e-mail.

Purdue University campus computing users are reminded that IT units at Purdue never ask users to divulge their passwords to University IT resources. Think before you click.

Congratulations on the start of another academic year. I hope to see you during the October events, and now more than ever, be careful out there.

Urban Legends Continued

There are web sites available to the public that are dedicated to informing people about these scams and rumors. These web sites give information to the reader about nearly any story or rumor that has been circulated online.

Listed below, are what corroborators say are the top three sites to gain information about rumors and scams.

1. <http://www.snopes.com/> – This site is the first of all the fact-checking sites. Some of the worst chain spams even quote Snopes with an embedded link to give their e-mail an added level of authenticity. They've also become commercialized and include lots of pop-ups, but it is a very complete site.
2. <http://urbanlegends.about.com/> – This is a site that is hosted by About.com. A team from About works at debunking all those rumors, myths, pranks and odd stories. The information is not much different from Snopes, but there is not as much available.
3. <http://www.truthorfiction.com/> – Check out rumors, inspirational stories, virus warnings, humorous tales, pleas for help, urban legends, prayer requests, and calls to action to see if they are truth or fiction.

MILESTONES



October is National Cyber Security Awareness Month. Now in its third year, Purdue will offer several informational sessions during October centered around the “Security on the Go: Your Ticket to Digital Self Defense” theme.

All events will be held from 9:00AM to 11:00AM in Fowler Hall (located in Stewart Center). The sessions include the following:

October 8 Buckle up! Laptop Security

Scott Ksander, Chief Information Security Officer and Executive Director of Networks and Security of Purdue University will share his enlightening thoughts on mobile security.

October 15 PDA's: “Pretty Darn Accessible” Without Security

Safeguard Your Data & Protect Your Reputation: With PDAs becoming ubiquitous, the same threats that affect desktop users are starting to affect PDAs. Doug Couch and Nathan Heck, Security Analysts, will talk about securing your PDA and external storage devices.

October 22 Phones and Tech Toys: Who Can Hear Me Now?

What new technology will we see next year? What trends will we see? Will these be good or bad? All portable devices incur greater security risks. How can you protect yourself and not live in a cave? Aaron Jarvis, Network Engineer within ITaP will co-present with a representative from Verizon

October 31 Special Security Guest Speaker & Traditional Security Halloween Costume Contest

Chris Kenworthy, McAfee Senior Vice President of Worldwide Enterprise Business will speak. Then find out who wins Purdue’s third annual Security Halloween Contest!

To read more, go to: <http://www.purdue.edu/securepurdue/training/cybersecurity2008.cfm>

SECURITY RESOURCES

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

- SecurePurdue October Cybersecurity events

<http://www.purdue.edu/securepurdue/training/cybersecurity2008.cfm>

- Password Vault Software Download Site

<http://passwordsafe.sourceforge.net/>

- Urban Legends

<http://www.snopes.com/>

<http://urbanlegends.about.com/>

<http://www.truthorfiction.com/>