SECUREPURDUE NEWS
www.purdue.edu/securepurdue

October 2009
Volume 4 Issue 4

All the news that's secure to print.

## FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

One of our themes for October Cybersecurity Awareness Month is "Our Shared Responsibility." Nowhere is that fact more evident than in the dramatic increases we are seeing in phishing attempts and; sadly, the equally dramatic increase we are seeing in people falling for those attempts. Wikipedia defines phishing as "the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public."

According to industry sources, the number of phishing URLs reached a record high during the second quarter of 2009. More than 150,000 new phishing URLs were created during this time, surpassing the previous record set during the first quarter of 2007. The techniques used to get these links out in front of unsuspecting users have also become more sophisticated. This appears to be due to new techniques and new "crimeware" available to better disguise phishing attempts. While some experts report the level of broad, undirected phishing is decreasing; it appears that the level of targeted phishing, often called "spear phishing," is on the rise. We are certainly seeing this at Purdue with very targeted phishing attempts referencing our infrastructure, elements of Purdue in the news, and even the Purdue homepage.

## In this issue

CISO message . . . . . 1
October National CyberSecurity Month . . . . . 2
Upcoming SANS Training 2
Purdue Joins InCommon Federation . . . . . 3
A Typical Day in the Network 4
Security Resources . . . . 4

There is significant technology available here at Purdue to intercept phishing attempts before they can reach our community. That technology can and does stop hundreds of thousands of attempts each day, but it will never catch them all. Each time we get smarter with infrastrucure technology, the bad guys are challenged and they get smart too. This is where the shared responsibility must take over. "You" are our best hope to thwart the phishing attempts that technology can't stop. Don't Just Click It! For more information, please see the SecurePurdue web site.

Finally, I hope to see you in Fowler Hall on October 30 for our Cybersecurity Awareness Month campus lecture. We will be discussing cybersecurity from both the industry perspective and the campus perspective. I know you will find it interesting.

As always, thanks for listening and be careful out there.


We may remember the landing on the moon July 20, 1969, but the first test of Arpanet between two computers at UCLA was less publicly noted on September 2, 1969. This was the predecessor to the Internet. With its growth have come significant challenges to the safety of data transfer.
Each year we take time to recognize Cybersecurity Awareness month with presentations.

***ITaP's Networks and Security staff would like to invite you to our fourth annual National Cybersecurity events***

Our live event will be:
October 30: Protecting Data is Not an Impossible Mission

WHEN: October 30, from 9 to 11 a.m.
WHERE: Fowler Hall in Stewart Center

Presenters this year will be:
John McCumber, strategic programs manager in the Public Sector Group of Symantec Corp., who will discuss threats to computer security facing industry. Scott Ksander, Purdue Chief Information Security Officer, will discuss threats to computer security in a university setting. A security–themed Halloween costume contest will conclude the session.

President Barack Obama has endorsed Cybersecurity awareness month, and the U.S. Senate passed a resolution to support it. Governors of 41 states also signed proclamations recognizing the month. The National Cybersecurity Awareness Month has been conducted since 2001 in October to educate individuals about the dangers on the Internet, safe computer behavior and our nation's critical cyber infrastructure.

Purdue is one of a dozen institutions of higher education selected to help target the online computer behavior of 17-25 year olds through National Cybersecurity Awareness Month. For more information and event updates, please visit the SecurePurdue Web site.

## SANS Training Courses for 2010

It is never too early to start planning your professional development. ITNS has scheduled the SANS 557 Virtualization training for January, 2010. Additional proposed training for next year is listed.

**January**
• DEV541 (Secure Coding in Java) 1/5-8/2010
• SEC557 (Virtualization Security & Operations) 1/20-21/2010 (6 seats reserved)
**reduced from $750 - $500**

**Spring 2010 IVC Schedule:**
(http://www.sans.org/training/courses.php)
• SEC546 (IPv6 Essentials)
• DEV422 (Defending Web Applications Security Essentials)

**Summer 2010 IVC Schedule:**
• SEC401 (Security Essentials)
• SEC505 (Securing Windows)
• SEC542 (Web App Penetration Testing and Ethical Hacking)
• Mac OSX (they have updated this course)
Contact Cherry Delaney to register for the training or for further information: cdelaney@purdue.edu

# SPOTLIGHT

## Purdue Joins InCommon Federation

Researchers, faculty, staff, and students who want to use resources available at another university or their sponsored partner may be able to do this more easily. Purdue is now a member of the InCommon Federation, which manages the authentication services needed between higher education institutions and their sponsored partners.

All participants in the federation use a common set of policies and practices to exchange information about their users and resources in order to share access to resources and enable collaboration between participants. Instead of being issued a login and password from another university, Purdue faculty, staff, and students use their Purdue career account to access these remote resources.

The underlying technology used to support federated authentication between participants in the InCommon Federation is the Shibboleth System, with Purdue's Centralized Authentication Service providing the single sign-on protocol for authenticating Purdue faculty, staff, and students using their career account.

One example of student use of InCommon is the use of WebAssign, a web site that lets instructors create assignments online and students work on these assignments online, giving instant feedback on the assignments. The faculty and students use their Purdue career account to access WebAssign.

An example of how staff might use this is with the Committee on Institutional Cooperation (CIC). The CIC is a consortium of the Big Ten universities including Chicago that share expertise, and collaborate on programs. Through InCommon, staff are able to share documents and resources easily by logging on with their Purdue career account but access the materials fellow members may have shared.

Rob Stanfield, Director of Purdue's Identity and Access Management Office, is excited about Purdue's participation with InCommon Federation. "Participation in the InCommon Federation has many benefits for Purdue students, faculty and staff," Stanfield said. "Among those benefits, users no longer have to manage different accounts and passwords in order to access resources

at other institutions, which leads to increased convenience and security."

For additional technical information about this service. https://www.purdue.edu/securepurdue/services/InCommonService.cfm

# MILESTONES

## A Typical Day in the Network

ITaP Networks and Security presents a day in the University's networks.

• There are over 40,000 network connections with fiber optic connectivity to all 255 campus buildings.
• There are 1,800 wireless access points which cover most indoor "common" areas and covers approximately 3.7 million SqFt.
• 24,000 individual users connected on a given day.
• The internet connectivity for research work travels through a 10 Gigabit fiber. We house 568 network equipments "sites."
• We use about 3,030 network devices.

• There are 23,800 ports in the academic and business areas, 13,000 in student rooms, 2,600 in MATH for RCAC research clusters and 1,700 in FREH/HAAS/MATH Data Center.

• The telephone office supports 20,450 active telephone lines.
• There are 614 miles of fiber optic cable and 485 miles of copper cable installed

• Annual Voice service orders – 8,387
• Annual Trouble tickets – 1,247
• Annual Data orders – 15,361
• Annual CS2100 telephone switch calls processed – 27,881,209

• There are 50 managed firewalls
• About 7 million central authentications are processed each month.
• We manage over 8,000 current central ePO users.
• 98 distinct websites have been scanned since October, 2007
• Our intrusion detection systems (IDS) reported 2,196,398 recorded events in the third quarter of 2009
• We blocked 33,000 outbound connections from phishing for "Purdue IT Team."
• We receive an average of 4500 log events per second totaling roughly 264 million new log events received in a 24 hour period from 572 distinct logging sources.
• 775 outbound "leaks" blocked since 4/1/2008
• 463 password or system data leaks thwarted
• 178 e-card malware stopped
• 81 web-based exploits stopped
• 53 worm propagation attempts blocked

ITNS is pursuing a new Wireless Technology Initiative, 802.11n Wireless:
• Higher speeds ( >100mb/s possible)
• Retain support for current 802.11a/b/g
• Pilot Project underway at ARMS, BRK, CL50, DAUC, KNOY, LYNN
• Re-survey buildings for more complete coverage
• Increase number of access points: 1,521 today, around 6,000 projected

## Trends in Telecommunicatons

| | A | B | C | D |
|---|---|---|---|---|
| 1 | Telecommunication's Trends Activit | Column | Column | Column |
| 2 | | 2006 | 2007 | 2008 |
| 3 | Number of Lines | 20,483 | 20,639 | 20,722 |
| 4 | Total Number | | | |
| 5 | of Calls | 26,258,794 | 24,658,106 | 22,672,736 |
| 6 | | | | |
| 7 | Voice Mail | | | |
| 8 | Answered Calls | 5,985,604 | 5,442,601 | 4,786,699 |
| 9 | | | | |
| 10 | Voice Mail Users | 18,816 | 18,965 | 8,514 |

# SECURITY RESOURCES

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

• Identity Access Management office InCommon Federation information
*https://www.purdue.edu/securepurdue/services/InCommonService.cfm*

• SecurePurdue Website
*http://www.purdue.edu/securePurdue/*