SECUREPURDUE NEWS
www.purdue.edu/securepurdue

September 2012
Volume 7, Issue 3

All the news that's secure to print.

FROM the CISO

By David Shaw
Chief Information Security Officer
IT Security & Policy

It's the beginning of a new academic school year! Students have returned to campus, football season has started and the campus is literally buzzing with activity. Soon you will be hearing messages about changing your smoke detector batteries and turning your clock back. Yes, fall is right around the corner. One other message that comes with fall is cyber security awareness.

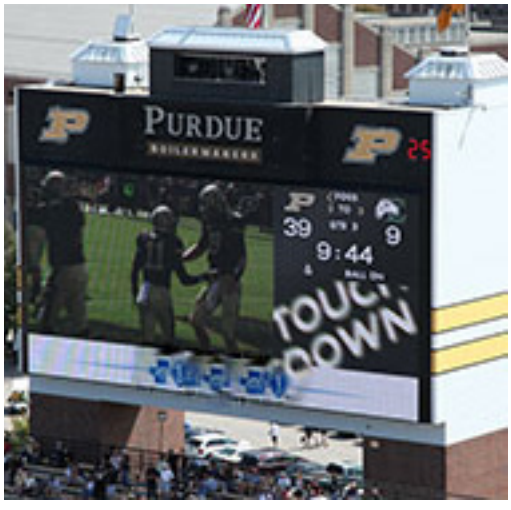
October is cyber security awareness month and several activities are planned around campus and around the nation to remind us of the importance of staying cyber-aware. I want to encourage you to take the opportunity to attend some of these events because they give you a chance to hear about ways you can become or remain a good cyber citizen.

You don't have to wait until October. Cyber security is something you should pay attention to all year long. A good place to start is at SecurePurdue. A number of resources are available at the site to help you understand good security practices. Another great resource I always point people to is the Stop. Think. Connect. campaign This campaign is focused on keeping the web a safe place for everyone to enjoy.

Everyone at the University has a part to play in protecting the resources we use. We all use the same Internet, and network and some of us even share systems. In a 2010 national survey for the National Cyber Security Alliance (NCSA) and the Anti-Phishing Workgroup (APWG), 93 percent of respondents felt their online actions could protect family and friends and also make the web safer for everyone. When asked why they didn't always do the things that they should to stay safer online, 28 percent cited a lack of information or knowledge as the reason.

As Purdue's new Chief Information Security Officer, my role is to help the University community understand the risks associated with cyber activities so we can make informed decisions. I look forward to this opportunity!

The Stop. Think. Connect. campaign is online at www.stopthinkconnect.org.



Be sure to notice the Cybersecurity Public Service Announcements we will air during the two home games in October!

In this issue

Syncing Your Career Account Password with Mobile Devices

Changing your password on a regular basis is something you have to do. While it is often hard to come up with another easy to remember password that is strong, it is a key component in maintaining a secure environment. For tips to create a strong password or passphrase, go to: http://www.purdue.edu/securePurdue/best-practices/passtips.cfm

As described by the current Information Technology Resource Acceptable Use Policy, each Purdue University computer user is responsible for his or her use of technology on campus. The integrity and secrecy of an individual's password is a key element of that responsibility. For more information on this, go to: http://www.purdue.edu/policies/information-technology/viia2.html

Before changing your password:
- log out of Outlook
- turn your smartphone or any other mobile devices off or put them on airplane mode.

These steps will help you avoid being locked out of your account.

Once you have changed your password, you can open your email configuration on your mobile device and enter your new password. My mobile device was already prompting me for a new password when I turned it on.
For more information, go to https://www.itap.purdue.edu/newsroom/detail.cfm?NewsId=2598

SANS has set up a free **Securing The Human** *video for the month of October in support of National Cyber Security Awareness Month.*

The first video is on **Email** *and* **Spear Phishing** *and is available at this link:*

https://www.securingthehuman.org/resources/ncsam

Visit this site throughout October for other videos!

Password Vaults

Password troubles at Linkedin, eHarmony, and Last.fm have been in the news. In most of the articles you will see the following advice:

1) use unique passwords for every site you visit
2) make each password "complex"
3) change them frequently
4) don't write them down.

We, in the security industry, have been recommending this practice for years. However, if you live and work on the Internet, there's a big problem with this advice. There are simply too many passwords to remember because every web site you use wants you to create a new account. It's no wonder that people write passwords down, don't change them frequently, make them easy to remember, and use the same one everywhere.

Until the industry changes its practices on requiring a unique password everywhere, let's try something different. Let's use software to store your passwords safely.

A solution to remembering all the different passwords is to use software designed to store passwords. Tools such as KeePass, and Password Safe encrypt your passwords, create complex passwords for you, and maintain password histories. For a comparison of different software tools, visit our website.

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

Regardless of the tool you use, always create a strong and long master password to protect all of your other passwords. And enjoy using the internet safely again.

For tips on creating a strong password, go to: http://www.purdue.edu/securePurdue/bestpractices/passtips.cfm

SPOTLIGHT

ITaP Cybersecurity Awareness Month 7th Annual Presentation
Purdue University's ITaP Security and Policy unit will observe the annual National Cybersecurity Awareness Month throughout October. We have two tracks of presentations: Security Awareness 2012 and Technical Cybersecurity Tools.
These will be held October 5, from 9:00 AM to 5:00 P.M. in Stewart Center, Rooms 214 A-B, C-D.

KEYNOTE: 9:00 a.m.-10:00 a.m. Gene Spafford, Executive Director of CERIAS will be our keynote speaker for both tracks:

10:15-a.m. 11:15 a.m. Security Perspectives 2012: David Shaw, Chief Information Security Officer will talk about computer security concerns today.
11:25 a.m.-12:25 p.m. The Promise and Peril of Social Networking: Panel of speakers will include Kyle Bowen, Gene Spafford, David Shaw, Lorraine Kisselburgh,
Lunch Break 12:30 – 1:30

Two Presentation Tracks:

Security Awareness

130 - 2:30 **Social Networking Security and Privacy** *Keith Watson*

2:30 - 3:30 **Minimum Security Requirements for Handling Data in Research Projects**

3:30 - 4:30 **Tips on Securing Mobile Devices** *Mike Hill, Preston Wiley*

Technical Cybersecurity Tools

130 - 2:30 **Suricata: Advances in IDS and Why We've Started Over,** *Matt Jonkman*

2:30 - 3:30 **Incident Response Process** *Doug Couch, Nathan Heck*

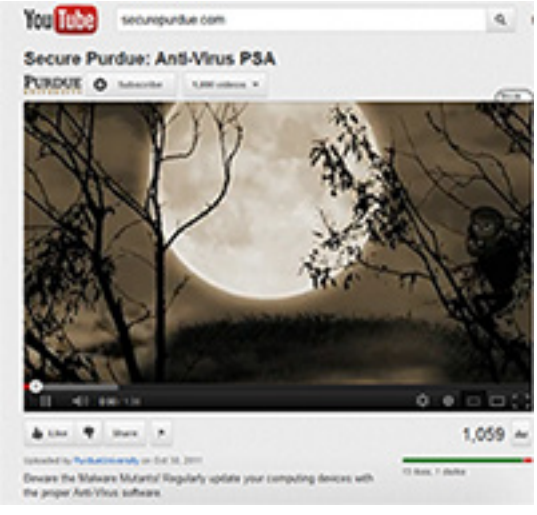
3:30 - 4:30 **System Auditing for System Admin istrators** *George Bailey, Josh Gilliam*

For more information, go to: http://www.purdue.edu/securePurdue

The National Cybersecurity Awareness Month has occurred every October since 2001 to educate computer users about dangers on the Internet, safe behavior online, and the nation's critical cyber infrastructure. We hope you can join us. This free event will be live streamed and later archived to our website at: http://www.purdue.edu/securepurdue/training/Cybersecurity 2012.cfm

Enjoy our Halloween themed video about computer security. This one and others that Rob Hart has created, may be found on YouTube.

Go to YouTube and type securepurdue to enjoy several different themed computer security videos.



IT Resource Acceptable Use Policy

Computer security starts with you. Being aware of campus policies and guidelines can enable you to prevent infecting your work computer or providing unauthorized access to University data and resources. The Acceptable Use Policy states that use of University information technology resources should be for purposes that are consistent with the business and mission of the University. Personal use should be incidental and kept to a minimum and should not incur additional cost to the University, prevent you from attending to and completing work effectively and efficiently, or preclude others with work-related needs from using the resources, including the shared campus and Internet bandwidth. Individual departments or units may place additional restrictions on personal use of the resources by their employees.

Every member of the Purdue community who uses computing devices can make our computing environment more secure by following security guidelines. End users are expected to:

• Apply computing device security software patches and updates regularly.

• Apply computing device operating system patches and updates regularly.

• Apply computing device application software patches and updates regularly (e.g. word processor software, IM clients, and other programs).

• Install and use anti-virus and anti-spyware software on the computing device, keep software definitions up to date, and run regular scans.

• Install and enable a hardware and/or software firewall.

• Use secure methods to securely transfer files (e.g., SecureFX and SecureCRT) to and from the computing device.

• Configure computing device so that it requires authentication (e.g., password, passphrase, token, or biometric authentication), runs in least privilege mode (e.g., user), and times-out after a 15 minute period of inactivity.

• Activate and utilize a lock feature prior to leaving the computing device unattended.

•Use adware removal programs regularly.

•Set the security settings to the highest level on Internet browsers and adjust downward as necessary for your Internet use.

• Regularly verify that system security measures are enabled on your computing device.

• Never share Purdue directories and files without access controls.

SECURITY RESOURCES

• I T Acceptable Use Policy
http://www.purdue.edu/policies/information-technology/viia2.html

• Snyc Mobile Devices with Your Career Account Password
http://www.itap.purdue.edu/newsroom/detail.cfm?NewsID=2598

• SecurePurdue Password Manager Software
http://www.purdue.edu/securepurdue/pswdManager.cfm

• SecurePurdue Website
http://www.purdue.edu/securepurdue/bestPractices/passTips.cfm