SECUREPURDUE NEWS
www.purdue.edu/securepurdue

October 2010
Volume 5, Issue 3

All the news that's secure to print.

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

October is National Cybersecurity Awareness Month. Our theme for this year is "Be a Cyber Survivor: Predict, Prevent, and Prevail." As always, our focus is on the steps that you can take to protect both Purdue's data and your own information. Information is valuable to the institutions that rely upon it, like Purdue, to provide services. Some personal information, such as account numbers, or Social Security numbers, is just as valuable to criminals as it is to legitimate organizations.

The 2010 Verizon Data Breach Investigations Report was recently released. Verizon conducts this report in cooperation with the United States Secret Service. You can find the report at: http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

The report is worth a read if you are interested in learning about how data breaches happen. The opening paragraph of the report really spoke to me. The report said, "2009 was, in many ways, a transformational year in the trenches. As attackers and defenders vied for advantage, there were numerous developments on many fronts around the world. It's difficult to measure who's winning with any certainty but there are, at least, some measurements available." One notable measurement is that public breach disclosures dropped in 2009.

The Verizon report suggests a number of reasons why this number may be dropping. Even if that number is dropping, we must still be vigilant in how we protect our data. As a Purdue employee, this means knowing how to best handle Purdue data. The University Data Stewards Organization publishes materials that can help you there. In addition, both the Data Stewards, Security Officers Working Group, and IT Networks and Security continue to work together to provide guidance on information security issues. The most recent guidance, a set of guidelines on using cloud computing services, was recently published on the SecurePurdue web page. ITaP's Video and Multimedia Production Services Group and IT Networks and Security have also worked together on a new series of Cybersecurity Training Videos. I hope that you will find these videos as clever and helpful as we have. One of them is even a Telly award winner!

As you think about how you protect data, I hope that you will take a moment to attend our Cybersecurity Awareness Month campus lecture. The presentation will be held on October 27, from 9AM to 11AM at Fowler Hall inside of Stewart Center. Malcolm Harkins, who is the chief information security officer from Intel, will discuss how to calculate information technology risk. We will also discuss the latest computing threats in a University setting. I am looking forward to the lecture and I know you will find it interesting.

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

In this issue

Social Networking Tips

Social Networking Primers
According to US-CERT: "The popularity of social networking sites continues to increase, especially among teenagers and young adults. The nature of these sites introduces security risks, so you should take certain precautions."

OnGuard Online offers some quick facts about social networking sites using games and videos to educate people about safe internet practices. http://www.onguardonline.gov/

The Department of Defense now offers education and training materials, social media guides, policies, and user agreements through their new DoD Social Media Hub. http://socialmedia.defensegov/

Passwords
• Choose strong, complex passwords.
• Choose a unique password for each account.
• Never share your passwords.
• Never use your password on suspicious third party sites.

Safety and Security
Don't reveal too much information about yourself. Depending on the information you reveal, you could become the target of identity or property theft or credit card fraud.

Watch what you click! Don't click on suspicious links or pop-up ads that may infect your device with malware or install spyware. (Recent buzz words for this include clickjacking, likejacking and tabnapping.)

Be wary of scams, such as fake profiles designed to exploit your trust. Scams are no longer limited to e-mails.

Applications that run on social networking sites might send your information to a third party or spread malware.

Check privacy policies (all social networking sites have them.)

Report spam, phishing, or hacking violations.

Ways to protect your identity and data

1. Be selective in giving out personal information. Don't just automatically provide your social security number. Phishing emails ask for passwords, bank account information. They may look real - they are not. Adopt a healthy suspicion of requests for personal data.

2. Don't click on links in emails, they may take you to a fake web site.

3.Be aware of your surroundings and keep an eye on your personal belongings too.

4. Check your credit card and bank statements frequently to quickly alert officials, if need be.

5. Use a password to protect your cell phone or computer from unauthorized viewing of data.

6. To report fraud, call (800) 525-6285

7. To opt out of pre-approved offers of credit, call (888) 567-8688

Check out our videos at: http://www.purdue.edu/securePurdue/training/index.cfm

SPOTLIGHT

Cloud Computing Consumer Guidelines Posted

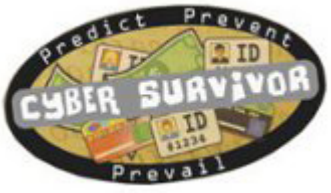
New advances in Internet-based products and services can highlight information security concerns. The use of cloud computing services is one of these new developments. Organizations like Purdue may purchase or use free cloud computing services to lower costs and create efficiencies.

Cloud computing is a type of computing where both applications and infrastructure capabilities are provided to end users as a service through the Internet. Through cloud computing, entities no longer have to own their own computer hardware, infrastructure, platforms, or applications. By way of an example, software as a service (SaaS) application services are cloud computing services.

While there can be advantages to using cloud computing resources, Purdue units and departments also must be aware of the information security and privacy concerns related to use of such resources. The University Security Officers Working Group, the Data Stewards Organization, and ITaP Networks and Security has created a set of guidelines that identifies the issues that must be considered before purchasing or using cloud computing services at the University.

Information security guidelines are recommended actions and operational guides to users, IT staff, operations staff, and others when a specific Purdue University Information Security policy does not apply. Cross-organizational working groups that include subject matter experts create information security guidelines.

The Cloud Computing Consumer Guidelines document can be found on the SecurePurdue web page at:
http://www.purdue.edu/securePurdue/bestPractices/Cloud%20Consumers.cfm



Predict, prevent, prevail and be a cyber-survivor as ITaP presents Purdue's fifth annual national Cybersecurity Awareness event in October.

This month long focus on secure, safe computer use will culminate with a free presentation in Stewart Center's Fowler Hall.

Malcolm Harkins, chief information security officer and general manager enterprise capabilities, controls and compliance will discuss how to correctly calculate IT risk.

Scott Ksander, Purdue's chief information security officer will discuss the latest computing threats in a University setting.

WHEN: October 27th
9:00 - 11:00 am

WHERE: Stewart Center, Fowler Hall

This event will be live streamed and archived for those not able to attend.
For more information about computer security check out our new website at **http://purdue.edu/securepurdue**

MILESTONES

Own Your Space While Being Social

by Keith Watson and Linda McCarthy

What would our world be like without Facebook, MySpace, or Twitter? Think back, oh say, five years ago. Yep, it would be like that again. For some, that was a better time. For others, not so much. How would we know what was happening with our friends, family, and co-workers? How would we stay in touch with people we haven't seen in years?

While social networking makes it easy to stay connected, it is that connectedness that has some risk. Our personal information, relationship status, friends, likes/dislikes, hobbies, favorite places, employers, passions, charitable causes, compromising photos, and diatribes are all on display for the world to see. Marketers want this information so they can sell us stuff. Employers want to see it to determine if a candidate has the right moral standing for their organization. Mom and Dad want to know what we do outside of class. The boss wants to see what we do outside of the office. Think no one has been fired over something on Facebook, think again.

Some rules to live by:
1. Share the least amount of information. Enter only vague or general information about yourself. Avoid putting contact information online. If the service allows it, share specific information only with people you trust.

2. Only accept friend requests from people you know directly. Don't be too friendly with people you don't know or haven't met.

3. Watch what you post. This information may remain available forever. If your mother wouldn't approve, then don't post it. She may see it some day, so may a future employer...
For more information check out Own Your Space, a book about online safety available for free download at http://www.ownyourspace.net/. In it you will find advice on protecting your computer as well as your information online. Own Your Space has a presence on Facebook, MySpace, and Twitter. Linda McCarthy is the managing editor for the book and online resources. Keith Watson is an information assurance research engineer at the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue and a contributor to Own Your Space. http://www.ownyourspace.net/, http://www.facebook.com/ownyourspace.net/, http://www.myspace.com/ownyourspace/, http://www.twitter.com/ownyourspace/

SECURITY RESOURCES

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

- *Purdue University Best Practices: Cloud Computing Consumer Guidelines*
  http://www.purdue.edu/securePurdue/bestPractices/Cloud%20Consumers.cfm

- *Onguard Online*
  http://www.onguardonline.gov/

- *DoD Social Media Hub*
  http://socialmedia.defensegov/