SECUREPURDUE NEWS
www.purdue.edu/securepurdue

July 2012
Volume 7, Issue 2

All the news that's secure to print.

FROM the CISO

By Greg Hedrick
Interim Executive Director
IT Security & Policy

Things are changing here at Purdue and our new president will arrive soon. Things are changing within ITaP also. This month, IT Security and Policy welcomes our new CISO, David Shaw, who comes from Ohio. He served as State Chief Information Security Officer for the past two years where he fostered a culture of information security across all the state agencies. He lead the development of the state's first enterprise security architecture and established a state standard for information security controls. He has many years of work in the department of education in Ohio that will serve him well in acclimating to his position here at Purdue.

David will assume the leadership of the IT Security and Policy group on July 9th. He has an MBA from Franklin University and is working on his Ph.D. which should be completed in 2015.

Before you know it, we will also be welcoming new students, staff and faculty as we start another academic year. It is wonderful to see their enthusiasm and optimism. We continue to do everything we can to ensure a safe technology environment for them as they plug in to the network.

IT Security and Policy have many new opportunities for the University community. We have great savings possible through the end of July from our collaboration with SANS, a security training vendor. See our article about this to learn more.

McAfee, our anti-virus software that is free to all staff, faculty and students, will soon be rolling out new tools to protect Purdue data and resources. We will keep you posted on new features in the near future.

Doug Couch, and Nathan Heck successfully passed the examination for Information Systems Security Architecture Professional (ISSAP®) administered by $(ISC)^2$. The $(ISC)^2$ Board of Directors has awarded to Doug and Nathan the ISSAP designation. $(ISC)^2$ is a not-for-profit leader in educating and certifying information security professionals. We are very proud ot both of them for attaining this certification.

Greg Hedrick, Director of Information Security Services, has completed the Council of Manager Development two year program and has given presentations on the progress of their project on improving sophomore retention.

Joanna Grama, Information Security Policy and Compliance Director presented with Leah Lang, Senior IT Metrics and Benchmarking Analyst with Educause at the Security Professionals conference held in May in Indianapolis. Their presentation concentrated on Metrics: Benchmarking and Security Metrics at the Educause online-only session. They discussed using a metrics development methodology. The conference was held in Indianapolis, IN.

Cherry Delaney, Security Awareness and Training Coordinator presented with Ben Woelk, Information Secuirty Policy and Awareness Analyst, from Rochester Institute of Technology at the Educause Security Professionals post-conference workshop held in Indianapolis. They presented Engage! Creating a Meaningful Security Awareness Program. Focus was given to integrating social media and other resources to reach a wider audience and various methods to engage University communities to become more security conscious.

In this issue

Digital Profiling and Emergence of Collusion 2
The Gram Scam 2
Android Alert: How To Protect Yourself 3
Internet Search Safety 3
Purdue Salvage: Secure Data and Electronic Recycling 3
Plan Your SANS Training for 2012-2013 4
Nathan Heck Deputized 4
LinkedIn Hack 4

Protect Your Digital Profile

As we roam the Internet researching things, *liking* things or purchasing things, we create a digital profile. It isn't something we intentionally create, but Internet marketers track us and create a data profile of our habits, likes, hobbies, and political leanings. They want to help us find the items or news articles that we have indicated we like by what we visit on the Internet.

When you log into Facebook, you will likely notice advertisements that match your interests. Behavioral tracking is the process of tracking your habits and behaviors online. Online marketers buy information about your online activity to target coupons and campaigns just for you. This can be good but also annoying.

There are some guidelines to follow when entering the Internet each day.

1. Share the least information on websites. Your email site doesn't require more than what is needed to receive emails and send them out. Your friends on Facebook probably already have your address and cell phone number. It is better to limit how much you share.

2. Log out of Facebook, LinkedIn, online banking or whatever sites you have open that contain your personal information before you surf the Internet. Your searches may be easily tied to whatever else you have open.

Beware of "fan pages." Sure, you want to *like* things that your friends post but remember what you post, and *like* online, doesn't go away. Depending on how public you set your profile, many people could see this and maybe that isn't ok.

Think of your digital profile as an audio recording of everything you say and do. It is a digital record of what you said, what pictures you shared, where you went and with whom, and the location the pictures were taken.

A good article and video from TED shares what FireFox is doing to help you be more aware of who is tracking you: in just one day and from sites you never visited.

http://www.ted.com/talks/lang/en/gary_kovacs_tracking_the_trackers.html

Collusion is a new Firefox add-on that Mozilla created to keep track of who is tracking you. Firefox also now offers the option to browse in private mode where no history is cached in your browser. "The memory of the internet is forever," Mozilla CEO Gary Kovacs said. "We are being watched. It's now time for us to watch the watchers."

The Gram Scam

You have probably received notification that your personally identifiable data may have been accessed. But nothing happened. Yet. Or maybe the scammer visited your social media profile to learn the names of your grandchildren and commit what they are calling the grandparent scam. (This would be a good reason not to leave your Facebook visibility to public.)

Whichever way, scammers have now gained access to your personal information. They use this information to set up the scam. You receive a phone call or an email from someone claiming to be your grandchild who is traveling and is in need of emergency funds. The phone is quickly transferred to someone claiming to be from law enforcement, an emergency medical professional or an attorney. They explain the situation and the necessity of you to wire them money. The caller pushes for immediate action. They present the situation as one of extreme urgency and impress upon you that there is no time to contact the police or other family members.

Resist the pressure to act quickly. Instead, ask the "grandchild" supposedly calling some questions that only your grandchild would know. A pet's name, a nick name or what color car you drive. If they can't answer it correctly, just hang up and directly contact your family member who claims to be in trouble to confirm an emergency exists.

Hackers may also use your contact list to send a mass email to everyone that you need help. It will appear as though it is coming from you and the message will always be that you are in need of a money wire transfer.

If you think you have been a victim of a scam, contact the wire service immediately to report the incident. You may yet be able to retrieve your money. If they have already picked up the money, it is almost impossible to trace. The money is gone.

For further information about this scam, go to: http://www.fbi.gov/news/stories/2012/april/grandparent_040212

SPOTLIGHT

Android Alert: How To Protect Yourself

Android malware samples increased greatly: from hundreds of Android threats in 2011 to thousands in 2012. Hackers are targeting the Android system.

Cybercriminals exploit the Android system when unsecured apps are downloaded to your smartphone. There are some ways to protect yourself.

1. Don't download applications from unofficial sites. Think Angry Birds.

2. Only download applications from the Official Android Market.

Be careful downloading or viewing something sent from a friend. Don't be too curious to see something. Make sure to keep your OS updated to the latest vulnerabilities.

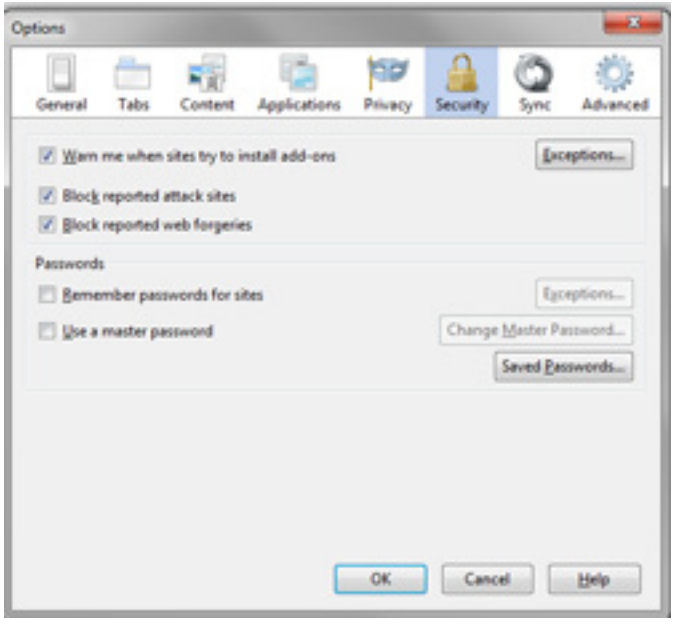
Internet Search Safety

There are 2.5 billion people searching the Internet, daily. It would not be surprising then that hackers/cybercriminals would find a way to use this to their advantage. Not all web sites are legitimate. Some act like a phishing email attempting to get information from you. Other dangerous sites contain malware that could be downloaded or installed on your computer without your consent. Searching on the Internet can be as dangerous as clicking on links in emails. The most dangerous searches used to be to celebrity websites or major news events but the cybercriminals tactics have changed to include obscure electronic parts or craft sites. These are places where there may be fewer search results and the hackers website will show up at the top of the search results. Be selective in which search result you click on.

Pay attention to the details of the sites you are visiting. Awareness is the key in protecting yourself online. Does the site have correctly spelled words? Is the domain name one you are familiar with or is it very close to the domain name you know?

When conducting a text Google search, there is a "preview" feature. A small set of arrows shows to the right of the text search entries. If you hover your mouse over it, it will display an image of the page to let you see if the page matches your search or if it looks legitimate.

You can set up your browser to warn you of sites that try to install add-ons, block reported attack sites or web forgeries. Those will help to prevent bad things from happening. Also, set the browser to never remember passwords for sites. These options will be listed under the Browser/Options. The illustration shows the Firefox browser option but any browser will have Internet settings options.



It is always important to protect your computer with updated anti-virus and anti-malware software to block suspicious sites and to prevent attacks.

Purdue Salvage: Secure Data and Electronic Recycling

We are able to utilize a service provided by the University Warehouse and Surplus Department and want to remind staff and departments about this service.

The "Recycling for the Future Program," promotes data security and electronic device recycling. It offers a systematic, auditable and reliable process for the disposal of electronic storage media containing University data. These items are shredded with an industrial shredder at the University Warehouse. In addition to increased data security, the shredded by-products are disposed of in an environmentally friendly manner.

For more information, go to: https://www.purdue.edu/salvage/sustain.aspx

Plan Your SANS Training for 2012-2013

For those of you wanting training that SANS provides, they will be offering their OnDemand series of training at deep discounts from June 1 - July 31, 2012.

OnDemand courses give you a span of time to complete the training online by yourself. This is a web-based training that offers a diverse series of courses. A typical four to six day course content, offered in the OnDemand module can cost $4,175, and will be offered for $1000. That is a $3,175 discount. Courses that span 1 - 3 days will cost $500.

It saves $450 to bundle the GIAC certification with the course training expense when you register. Otherwise, GIAC certifcation costs $999.00

The "window" for registering for OnDemand Training and Voucher Credits is June 1 - July 31.
+ SANS Long Courses = $1,000 (4-6 day classes)
+ SANS Short Courses = $500 (1-3 day classes)
+ Minimum order size per transaction: $3,000

Some of the courses will be released this year, as they continually update the content of the courses to be current with technology and the changing threats.

To read more about SANS online training and assessments, go to:
http://www.ren-isac.net/programs/sans_ondemand.html

Contact Cherry Delaney for more information:
cdelaney@purdue.edu, 765-496-1288.

Nathan Heck Deputized

Nathan Heck, IT Security and Policy, IT Security Engineer, was sworn in by Tippecanoe County Sherriff Tracy Brown as a special sheriff's deputy in June, 2012. Nathan was sworn in as a special deputy in order to complete forensic investigations with chain of custody issues for the Purdue University Police Department and other local law enforcement agencies. Nathan frequently takes part in forensic investigations of Purdue University IT resources following a security incident affecting those resources.

LinkedIn Hack

In the past couple of weeks, two major sites have reported security incidents involving the loss of their customer's password information. These events highlight the importance of proper password management. Many people use the same password for multiple online services. This is not always a secure practice." Why shouldn't I use the same password for all my accounts? Once one website is hacked and your password is exposed, access to all your other websites is now compromised as well if you used the same password.

So what can you do to protect yourself from security incidents such as this
1) Longer, harder = better. Use a complex password that's not easily guessed. It should be a mix of letters, numbers, and punctuation. If you need some hints on choosing a good password, see the article on the SecurePurdue web site on choosing a good password:
http://www.purdue.edu/securePurdue/bestPractices/passTips.cfm

2) Use a different password for each of your accounts. Do not use the same password on LinkedIn and your Purdue Career Account – use different passwords! In the event of a security incident, the impact to you will be minimized since you only use that password on that one site.

SECURITY RESOURCES

- SANS OnDemand Training
http://www.ren-isac.net/programs/sans_ondemand.html

- TED Talks: Gary Kovacs: Tracking the Trackers
http://www.ted.com/talks/lang/en/gary_kovacs_tracking_the_trackers.html

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

- GrandParent Scam Alert from FBI
https://www.purdue.edu/salvage/sustain.aspx