



FROM the CISO



By David Shaw
Chief Information Security Officer
IT Security & Policy

Several people have asked me recently whether there has been an increase in phishing emails and if so, what are we in security doing to protect students, staff and faculty. My answer is pretty much the same. We are noticing more phishing emails because more people are realizing that they are phishing emails or at least they are questioning it. I think this is a good sign; not that we are seeing more phishing emails but that people are questioning them more. It says that our awareness efforts are working. Awareness and education are the primary defenses to phishing.

Phishing emails are those emails that look like they are from an official source and attempt to get you to open an attachment, click on a link to a web page or simply ask you to submit your username and password (or other personal information) via email. The goal is to steal this information and either use it to access your accounts or steal your identity in some way.

The approach is not new. Phishing has been around since the mid 1990s. This may surprise some people that the practice has survived so long and the security field has not eradicated it. If only it were that simple. While the practice has been around for a while, it continues to morph and it becomes harder and harder to tell the difference between a real email and a phishing one. Some studies estimate that 50% of the population cannot tell the difference between a phishing email and one that is legitimate. (To see if you fall for the bait, check out our phishing quiz on the Secure Purdue website.)

Phishing isn't going away anytime soon. Why you ask? Because it is still an effective method. The criminal can send out thousands of these emails and they only need a small percentage of victims to actually 'take the bait'. But it doesn't have to happen to you.

Table of Contents

Are you Smarter than Your Smart Phone?	2
Plan Your Professional Training for 2013-2014	2
Secure Purdue Newsletter - Why We Exist	2
Social Engineering: Think Before Reacting	3
Security Threats of 2012	4
SECURITY RESOURCES	4
Do Not Track Legislation	4
Jailed Hacker Hacks!	4

The best advice I can give anyone about protecting themselves from phishing emails is to suspect any email that contains a link or an attachment, especially if you were not expecting it from the sender.

If you get an email from your bank or some other organization and it contains links, an attachment or asks you to submit something like your password or other personal information verify that it is legitimate first. Call the organization and ask them about the email. If you get something here at Purdue, contact the help desk or your local IT support. Don't just take the bait!

Are you Smarter than Your Smart Phone?

If you walk around on campus you will notice many people using their cell phones. Stand in line at Starbucks and most people will be reading from their phone. Smartphones get their name because they have calculators, apps to help your efficiency, have access to the internet, YouTube entertainment; they can do a lot of things. You need to be smart in using your phone. Use sound judgment about revealing your location. You're smarter than your phone if you know you think critically about the sensitivity of the data you put on or access through your phone. You are smarter than your phone if you protect it with a password.

While attending the first Purdue Information Fair for incoming freshman students, I asked many parents if they password locked their cell phones. Many said yes, but because their employers required it. Is your data any less important than your employer's? If you're not thinking critically about what you do with your phone, it may be smarter than you.

Plan Your Professional Training for 2013-2014

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, 2013.

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 \$4,410, and will be offered for \$1350. That is a \$3,060 discount. Courses that span 1 - 3 days will cost \$675.

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

The "window" for registering for OnDemand Training and Voucher Credits is June 1 - July 31.

+ SANS Long Courses = \$1350 (4-6 day classes)

+ SANS Short Courses = \$675 (1-3 day classes)

GIAC = \$579

+ Minimum order size per transaction: \$4,000

Some courses listed in the OnDemand series may be undergoing updates during your contract period but they will be released before your contract expires with SANS. You have four months to complete the online training.

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.

Secure Purdue Newsletter - Why We Exist

The information provided in the quarterly SecurePurdue newsletter is intended to increase the security awareness of the Purdue community end users and to help you choose to act in a more secure manner within your work environment. While some of the articles may relate to maintaining your personal technology, the increased awareness is intended to help improve Purdue's overall cyber security posture. This is especially critical as employees access their work network from their home computer.

We have definitely blurred the lines of work and personal business as members of our community bring Smartphones and iPads/tablets to the workplace. Increased productivity is a by product but so is increased security risks.

In order for any communication to be effective, it has to be read, shared, and affect behavior positively. Computer security awareness has to be as ingrained in your day to day concerns as locking your house, car door or educating yourself on emerging threats. The yearly flu alert is sent out each year, there are also reports on emerging cyber threats. They help give a lay of the cyber land for the upcoming year from visiting the events that have already happened and seeing what trends are occurring. Add reading more on cyber threats to your yearly schedule just as you update yourself on flu shots, changes in IRS laws, property tax issues, anything that affects your personal matters. More can be read on page 4 about cyber trends for 2013.

Organizations have permission and are encouraged to redistribute this newsletter in whole for educational, non-commercial purposes.

I don't always
TAKE TESTS *using* BLACKBOARD,
but when I do,
I DON'T USE MOBILE DEVICES.

STAY CONNECTED,
my friends.

ITaP
INFORMATION TECHNOLOGY AT PURDUE

itap.purdue.edu/learning/tools/blackboard/learn_res/student.cfm

SPOTLIGHT

Social Engineering: Think Before Reacting

In the context of computer security, social engineering is the art of manipulating people into performing actions or divulging information. It is deception for the purpose of information gathering, fraud or computer system access.

When it comes to social engineering what works better than the lure of the freebie? Free USB drives were scattered in a parking lot by researchers to see how people respond. In one study, 60% of the people who picked up one of the USB drives then plugged it into their PC. But when the researchers scattered USB drives that had a Department of Homeland Security logo on them, they found that 90% of people who picked up one of the drives plugged it into their PC. Maybe they thought they would contain national secrets but at the least, they were free or maybe.... they contained a bug to monitor their every activity on the computer!

<http://www.informationweek.com/security/vulnerabilities/mcafee-takes-belize-social-engineering-1/240145852?queryText=usb%20drives%20social%20engineering>

Millions of student loan financial data were stolen but the theft didn't involve hackers breaking through complex technology protecting the data in layers of security. The theft was completed by taking the safes the CD's were stored in and rolling them out of the building using office chairs. The data must be protected at all levels, physical and digital. Know where the data is stored physically and limit access to it.

With a \$4 Cisco shirt bought at a thrift store one successful social engineer posed as a service technician to gain access to a facility. He did his research and knew there was a horse race that day and his mark had updated her social website saying she was on her way to the race. With a few well timed moves, he and his partner were inside the large facility free to plant rootkits, and set up a wireless access point.

While in the cafeteria getting "lunch" he planted USB keys with names like Payroll or Strategy. The USB's had rootkits on them or autorun rootkits. The USB's were placed next to the coffee machine, and in a restroom next to the sink, likely places someone would lay it down and forget it. He knew who to ask for and how to get in. He also brought cookies!

Luckily, this happened to be a test of the vulnerability of the company and all the information was shared to improve the security. What they succeeded in doing could have cost the company multiple billions of dollars had they been bad guys.

Another way social engineers work is through browsing social media sites. Social media sites provide a door into the private world of users with names, locations, vacation information that can be used to scam targets out of money or information. It pays to limit who can see your most personal information.

Practice restraint in what you share and what pictures you post. Don't open the email or IM with pictures of someone's wonderful spring break if you don't know them. Pictures are such an easy way to get people to click. Just know they could contain malware.

We have recently been plagued with phishing emails. These were targeted to students at Purdue, something called spear phishing. Students were notified their certificate of authenticity would soon expire. They could easily fix the problem by sharing information to get everything updated.

Phishing emails have a pattern.

1. They warn of dire consequences if you don't do something immediately
2. They ask for you to provide personal information back to them
3. They may provide a link to a webpage where you can log in and fix whatever they say needs attention.
4. They may offer something too good to be true. It is too good to be true.

NEVER give private account information through email. Purdue will never send an email message asking users to reply with a password or other confidential personal information such as Social Security numbers or bank account numbers. Messages requesting such information are fraudulent and should be deleted.

Think before clicking on links in emails. Go to the source of the problem. If it is a bank email saying there is a problem, go to the bank website. If you have a voice mail stating a problem with your bank account, don't call the number from the voice mail. Look at your credit card and call the number printed on



the back of the card.

Think before you act. If someone comes to your work environment, make sure they are who they say they are if you don't know them personally. Would you just let this person come into your house without any other verification?

Security Threats of 2012

2012 was a year of Android attacks, more than 35,000 malicious programs. This is about six times what it was in 2011. As the Android platform became more popular, the hackers followed with ways to hack into them. One way to avoid Android attacks is to only download apps from reputable sites. Expectations are that 2013 will have more targeted attacks.

There were attacks on software and gaming developers like Adobe, Oracle, Microsoft and Sony.

Activist groups like Anonymous made headlines repeatedly attacking for political issues. The arrest of LulzSec's Xavier Monsegur and many prominent 'Anonymous' hackers didn't stop hacktivists' activities.

If you have a LinkedIn account, you may remember it being hacked in June 2012. DropBox announced it was hacked with leakage of user account details. *This might be a time to remind you not to use the same password on all your websites!!*

Computer Security Predictions for 2013

Well, more of the same is likely to happen. How is that for a bold statement or prediction! Hackers will get more sophisticated. I have noticed this in the phishing emails. It used to be it was easy to spot them because the spelling was bad and the grammar poorly written. Now, they are getting better at both.

Mobile devices are carried everywhere so they expand the perimeter to secure. This includes the use of cloud services.

There are more nation-state cyber espionage directed at oil platforms in the Middle East. This doesn't mean we are safe from cyber attacks aimed at financial or critical infrastructure.

The good news is that now is a great time to work in computer security or promote our field to young people.

Do Not Track Legislation

I set my browser to tell websites I visit to not track me. Proposed legislation would allow the US Federal Trade Commission (FTC) to enforce the intent of my request against companies that do not comply. The FTC would restrict online companies to collect only the data necessary to deliver their content or services. The bill would require online companies to destroy or anonymize personal information they no longer need. Opponents claim that self-regulation is working and this legislation is unnecessary. They say that the do-not-track bill would financially hurt Internet companies who deliver targeted advertising. This would be another reason I prefer to not be tracked or targeted for advertisements.

For more information, go to:

http://www.computerworld.com/s/article/9237266/Tech_groups_question_new_do_not_track_bill?taxonomyId=17

Jailed Hacker Hacks!

It is hard to keep the criminal from doing what got them put in jail to begin with. From the United Kingdom is the story of a hacker sentenced to five years in prison. Nicholas Webber was the mastermind behind Ghostmarket<dot>net, a forum for hackers to trade malware and stolen credit card information.



While in prison, Nicholas was permitted to attend technology classes. Oops, he then hacked into the prison's computer system. Luckily, the prison had a closed network at the time.

To read more, go to:

<http://www.v3.co.uk/v3-uk/news/2252112/jailed-cyber-crook-hacks-prisons-network-while-locked-up>

SECURITY RESOURCES

- USB as Freebie Lure

<http://www.informationweek.com/security/vulnerabilities/mcafee-takes-belize-social-engineering-1/240145852?queryText=usb%20drives%20social%20engineering>

- Do Not Track Legislation

http://www.computerworld.com/s/article/9237266/Tech_groups_question_new_do_not_track_bill?taxonomyId=17

- Jailed Hacker Hacks!

<http://www.v3.co.uk/v3-uk/news/2252112/jailed-cyber-crook-hacks-prisons-network-while-locked-up>