SECUREPURDUE NEWS
www.purdue.edu/securepurdue

December 2012
Volume 7, Issue 4

All the news that's secure to print.

## FROM the CISO

By David Shaw
Chief Information Security Officer
IT Security & Policy

Well the holiday season is in full swing now and many of you have already started shopping. Black Friday is past and Cyber Monday is well under way. Reports indicate that Black Friday sales topped 1 billion dollars this year for the first time ever. As I write this column, Reuters is reporting that online sales are up 24% in the early hours of Cyber Monday.

Mobile device sales accounted for 16% of the Black Friday sales this year. This is a 63% jump from just one year ago. That translates into a lot of people purchasing these new devices and many of them will connect to the Internet via WiFi or cellular connections.

As you start to enjoy any new mobile device, or really any device that connects to the Internet, take advantage of some common sense security practices. There are many sites offering some very good tips like those we offer in the Mobile Device section of SecurePurdue (http://www.purdue.edu/securepurdue/bestpractices/mobileDevice.cfm). Some of the main tips are listed here:

• Keep the operating system up to date. When the vendor provides an update, apply it as soon as possible. This is one of the first lines of defense.

• Only download apps from a trusted location and from trusted developers. Mobile malware continues to increase. If you use your device for anything more than simple web surfing, think about the applications you add because you are likely giving them access to other parts of your device as well.

• When using public WiFi 'hotspots' at your local coffee shop or restaurant, remember that unsecured sites make it easy for others to snoop on your online activities.

## In this issue



You should avoid doing online shopping or checking financial accounts on unsecured WiFi.

• Especially on mobile devices, set a password or at least a PIN to lock your phone after only a few minutes of inactivity. This is a first line of defense if your device gets lost or stolen. If possible, also set up remote wiping and remote locating features.

• Before you decide to sell, trade or otherwise dispose of a mobile device, make sure you delete all of you personal information. In many cases there is a factory reset to help accomplish this task. If you don't know how to delete the information, you can typically ask your cellular provider or check with the mobile device vendor.

Mobile devices are making great advances in their capabilities. These advances lead us to use them for more and more of our daily activities. By following a few basic security precautions you can enjoy the convenience these devices offer without putting yourself at risk.

If you're giving a mobile device as a gift, provide our safety tips to the gift recipient so they can practice safe mobile computing.

## Social Networking: The Promise and Perils

During the Cybersecurity Awareness event held October 5, a panel of presenters, Professor Eugene Spafford, Professor Lorraine Kisselburgh, David Shaw, Chief Information Security Officer and Kyle Bowen, Director of Informatics, spoke about their knowledge and use of social networking.

Kyle Bowen, Director of Informatics, has used this media for engaging students at the University. His group has developed Mixables, a tool for real-time sharing outside the real-time classroom. It promotes collaboration among class participants outside the time and physical restraints of a classroom. Students are able to share content and media privately.

Mixables is an example of a good use of social networking in the educational environment. Since its introduction in September 2012, over 7,965 student connections have occurred. They have shared over 6,996 links and listened to over 8,376 podcasts.

Kyle's group has also created Hotseat, a tool that promotes collaborative small discussions in and out of the classroom. Hotseat integrates Facebook, Twitter, mobile apps and text messaging to help engage members of a class. If you have ever taken a class in large lecture hall with over 500 attendees, you will appreciate this tool in helping to bridge the sense of isolation you may have felt. This is a great way to use social networking. It enhances the classroom experience and utilizes online connection in an offline setting.

There are worries associated with social networking. Many people are lured into Facebook with a sense of privacy, something Kyle called "privacy Zuckering".

Facebook changes their privacy settings very frequently which means, you as a consumer of it, must frequently check to see if your sense of privacy is still valid or may require some tweaks to gain back the privacy you want.

Facebook and other social networking sites do listen to consumers. When Facebook made changes in their policies and people responded negatively, they backed off.

Facebook is free – you are the product. You are the one being used here while you may think the service is for you, it is really a way to monetize revenue for the social network owners.

You, as a consumer of this environment, must make decisions on how much you want to give up your privacy to network with others. Is giving out your email address and phone number worth the savings from a coupon? You may want to help by filling out a survey but do they really need all that information about you? Be protective of your privacy.

## Lock Computers While Away From Workstations

The approved process for leaving your computer powered on while you are away is to use the keystroke combination; Ctrl, Alt, Delete or WIN+L. This will lock your computer. This is the most secure process to ensure no one can inadvertently see files you have access to.

WIN 7's hibernation mode is not secure. By default, it reopens without requiring a password. If you placed your machine in hibernation, it will not securely protect the files open or prevent unauthorized access to data you may have left access open to. If you want to change the default setting to lock while in sleep mode, go to the Control Panel/System and Security. On the right side of the screen, under Power Options, select the Require a password when the computer wakes. Save this change.

Hibernation is intended as a power saving mode only and by default does not protect access to your files and the programs you may have left open before the machine was put in hibernation status. If you use a laptop, use the same process to securely lock access.

Apple Max OS X users can go to System Preferences, click Security, click the General tab and check the box, Require password to wake this computer from sleep or screensaver. Then, go to System Preferences, click Desktop & Screen saver, click the Screen Saver tab and set a Start screen saver time.

On computers running Linux, the procedure for locking your screen varies by the Linux distribution, so check with the documentation for your version of Linux.

An alternate procedure for all three operating systems is to log out of your computer when you are going to be away for some time.

# SPOTLIGHT

**Question about safe email practices:**
I'm cautious about clicking on links in an email but have also heard that just opening a bogus e-mail, even if I don't click on any links, can sometimes cause problems. Is that true? If I'm suspicious of an e-mail, I'll use preview to read it, but I don't know if that is 'safe' or not either.

**Answer:**
It is always best to read your email in "Plain Text" mode by default. If you trust the email then switch to "HTML" or "Rich Text" mode to see all the pictures fonts and other graphic things.

Using the preview pane alone will not protect you as the malicious code is in the HTML email and the preview pane parses and runs that code when it attempts to display the email. Using the reading pane and displaying all emails in Plain Text, by default, is the safest way to do it.

### Use a Safe Personal Identification Number PIN

Banks make you use them, phone security locks use them, and they are your main means of protecting your personal data. So don't make it easy for someone to guess them. Use something other than your birthdate, social security number, or other easily guessed number. No street address, or license plate number. They are visible to others and easily guessed. Instead, use a portion of an old unused phone number, as long as it isn't four digits all the same, like 8888. You might use a phone number you frequently call, like your favorite pizza take out place.

If you use a word for your PIN, base it on a phrase that is meaningful to you, such as 2423 "All good boys do" (AGBD).

The top 10 PINs cellphone thieves love:
1. 1234
2. 0000
3. 2580 (keypad sequence top to bottom)
4. 1111
5. 5555
6. 5683 (spells "love")
7. 0852 (bottom-to-top keypad sequence)
8. 2222
9. 1212
10. 1998

To read more about safe use of PINs, go to: http://pubs.aarp.org/aarpbulletin/201211?pg=39#pg39

### Fake HR Address Verification Email

If you received an email that resembles the following email, it is a phishing attempt. Remember, we Don't Just Click It!

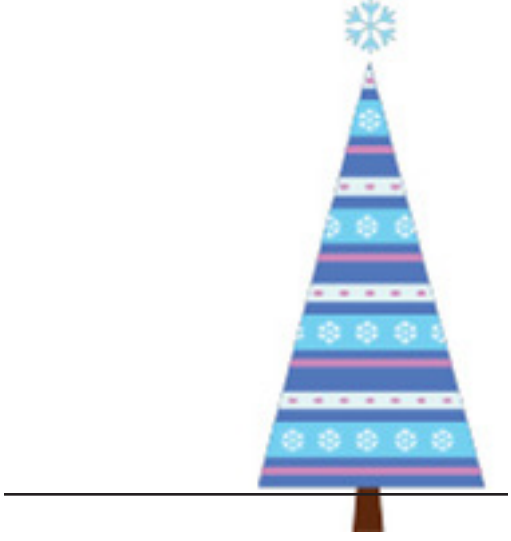
**From: Administrator [mailto:administrator@purdue.edu]**

Sent: Monday, November 19, 2012 10:18 AM
To:

Subject: To All Employee's - Important Address UPDATE

To All Employee's:The end of the year is approaching and we want to ensure every employee receives their W-8 to the correct address.Verify that the address is correct - https://local.purdue.edu/details.aspx?id=0687226735 If changes need to be made, contact HR at https://hr.purdue.edu/update.aspx?id=0687226735. Administrator,http://purdue.edu

ITaP Security and Policy warns the Purdue community that the University has been specifically targeted by spear phishing attacks made to look like they are coming from HR requesting correct address verification for the upcoming mailing of tax statements. These emails are not being sent from Purdue or Human Resources services. Report computer incidents to Purdue: http://www.purdue.edu/securePurdue/incidentReportForm.cfm



## Greatest Social Networking Rave or Next Malware Threat?

Pinterest is a great image sharing social networking site that has caught the attention of spammers. Just like the phrase, "follow the money," cybercriminals and scammers follow the latest social networking craze.

Pinterest's account security controls presently are primitive compared to other more mature social media sites like Facebook which offers two-factor authentication. Pinterest also does not have mature account recovery capabilities so make sure you are using a strong password because that is all you have to rely on to protect your account. There aren't any privacy or security settings as of yet.

Pinterest is a great marketing tool. Effectively, people share your product, or website with their friends. Businesses can gain exposure but this is not without risks. One of the risks is collaborator hijacking: a malicious user can follow your board, add you as a collaborator to their board then have their board appear on your profile. This has already happened to Barack Obama's and Starbucks boards. The only way to control this currently is to remove yourself from anyone's board who has added you to their board. An email notification alerts you to what is being done and gives you time to remove yourself/business from their board.

Pinterest is an image based app which makes it easy for the cybercriminals to add malicious code to an image. You are one click away from installing malware. To protect yourself against malicious image files, do not link to images outside of your control. Use only images you own, know are trusted or that you have uploaded to Pinterest yourself. The added benefit of this is it addresses legal risks concerning copyright infringement.

As with all scams, if it offers something incredibly awesome, doesn't quite look like the real Starbucks or causes you to pause, assume it is a scam to lure you. A site calling itself gimme4free created a collection of automated Pinterest bots. His images linked to his Amazon Affliliate account. When a genuine user clicked on his image, then bought a linked product, he made a few dollars commission.

Purdue uses social media. Most businesses, nonprofits, whatever cause, use it. This means that as part of an employee's job, they will be interfacing with multiple social media sites. How do you prevent bad things from happening?

1. There needs to be training of staff to prevent infection of their computers.

2. Use and Anti-virus software, but also use an anti-malware software.

3. Keep all software up to date - malware will seek vulnerabilities, so update all software regularly. This includes Windows, Adobe products and browsers.

4. Pinterest is new and online impersonation is a common problem with new social networking sites. Secure your brand name on Pinterest.

5. Aggressively report any boards offering up scams and spam to Pinterest.

A little attention to details and questioning when things don't add up can prevent a bad internet day.

# SECURITY RESOURCES

Mobile Device Best Practices
• *http://www.purdue.edu/securepurdue/bestpractices/mobileDevice.cfm*

ITaP reminds users to lock computers while away from workstations
• *http://www.itap.purdue.edu/newsroom/detail.cfm?NewsID=2709*

• Use a Safe Personal Identification Number (PIN)
*http://pubs.aarp.org/aarpbulletin/201211?pg=39#pg39*