SECUREPURDUE NEWS
www.purdue.edu/securepurdue

March 2008
Volume 1, Issue 15

All the news that's secure to print.

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

Wikipedia defines "social engineering" as "a collection of techniques used to manipulate people into performing actions or divulging confidential information." With regard to e-mail scams and phishing, creativity in social engineering continues to reach new levels. At Purdue we have seen this recently with clever socially engineered e-mail ranging from how to claim tax refunds to very specific messages regarding Purdue e-mail systems and accounts. The objective is clear: to manipulate you into believing the message is real and taking some dangerous action that puts you, your computer system, and Purdue at risk.

Those of you who are aware of these schemes are frustrated and have commented that "somebody should do something about this!"

Many people are trying to do something. ITaP alone spends over $100K annually implementing tools that directly reduce these types of messages and those efforts do make a difference. In January, almost 23 million e-mail messages were received for @purdue.edu addresses. Almost 17 million of those messages were quarantined as potentially dangerous or just "junk" before reaching the intended recipient's e-mail inbox. That means that 74% of all inbound messages were isolated. Additionally, another 4 million attempts to deliver e-mail were completely rejected because they were coming from known dangerous sources.

Even with all that work, many fraudulent e-mail are still getting through and increasingly clever attempts are finding victims. In addition to all the work I mentioned, one of the "somebodies" that still needs to "do something" is each one of us.

During a recent round of socially engineered e-mail specifically directed at Purdue, over 80 Career Accounts were compromised by people giving up their password in response to the request. Almost 3500 incident reports were received by the Incident Response team related to issues with these accounts. One compromised account alone resulted in 528 incident reports! Purdue University e-mail was "blacklisted" four times during this period by three different major internet e-mail services. That means ALL e-mail from Purdue to ANY users of these e-mail services was rejected. Important messages to friends, colleagues, collaborators, business partners, alumni, perspective students, and many others were either delayed or discarded. All of this cost, effort, and frustration occurred just because some of us "fell for it."

The reality is that, no matter how clever our programmatic efforts succeed to find and eliminate dangerous e-mail, there will always be a new way around our efforts and dangerous messages will still get through. SecurePurdue will continue to do everything we can to keep you informed as new creative schemes come along, but by the time we communicate with you, some number of the new schemes have already made it into Purdue inboxes.

CISO continued, Page 2

In this issue

Beware of Tax Scams

It is "that" time of year again, when we need to gather up our financial information and begin to prepare our tax returns. Tax preparation season is stressful for everyone; however, falling for an IRS-related scam circulating on the Internet can make tax preparation even more onerous. The Internal Revenue Service frequently issues alerts for tax-related scams making the rounds on the Internet and through e-mail. Many e-mail based scams may inform the recipient that they have a large, unclaimed tax refund. However, in order to receive the purported refund, the recipient must go to an IRS web site and enter personal information such as bank account routing numbers and PINS. When the recipient goes to the web site indicated in the phony e-mail, they are actually navigating to a phony cite. If the recipient enters their personal information on that cite scammers actually receive it and are able to initiate transactions out of the recipient's bank accounts.

Similar e-mail scams alert the recipient that they are being criminally investigated by the IRS for submitting a faxed tax return or other incorrect return information. The e-mail may attempt to divert the recipient to a phony web page or encourage them to click on the attachment to the e-mail. Many times the link and attachment attempt to download malware to the recipient's computer that could allow the scammers access to the data on that computer.

Other scams circulating on the Internet suggest that people navigate to a particular web site in order to make a tax-deductible donation in the aftermath of a particular tragedy, such as this summer's southern California wildfires or similar disasters. Again, the web site looks like a real IRS web site, but is instead a phony web site where scammers can gather the potential donor's personal information for later fraudulent use. The IRS does not send out unsolicited e-mails or ask for detailed personal and financial information via e-mail.

Additionally, the IRS never asks people for the PIN numbers, passwords or similar secret access information for their credit card, banks or other financial accounts. Members of the public who receive an unsolicited e-mail claiming to be from the IRS should never click on any links in the message, open any attachments, or provide any personal or financial information to the sender.

*The IRS **never** asks people for the PIN numbers, passwords or similar secret access information.....*

If you believe you have received an IRS-related scam, you are encouraged to forward the e-mails to phishing@irs.gov. Instructions for forwarding the e-mail are available at: http://www.irs.gov/individuals/article/0,,id=155344,00.html

For more information on IRS-related scams, visit the official IRS web site at http://www.irs.gov/, and execute a search for "scams" or "phishing."

CISO from Page 1

The best judge that "something isn't right here" will always be you. If you see something that seems suspicious, check on it BEFORE you take any other action. That effort will not only keep you safer, but will also keep the entire Purdue community safer.

As always, thank you for reading, and be careful out there.

Tax Scam continued

SPOTLIGHT

Be Careful with Digital Photo Frames

Digital photo frames are popping up in offices everywhere as a tech replacement for traditional picture frames that clutter workspaces. These photo frames showcase numerous digital pictures and often connect to a computer through a USB cable and appear as an additional mounted drive to the computer's operating system.

There have been a number of reports of consumers who discovered that their new digital photo frame attempted to install malware on computing devices connected to the frame.

The manner in which these attacks happen suggest that the malware was installed on the built-in memory of the frame either where the frame was manufactured, or at some point during the shipping process. It is also possible that the digital photo frames are purchased from retailers, malware is then loaded onto the frame, and then the frame is returned to the store for eventual purchase by an unsuspecting consumer. Similar reports have also been received for a number of other devices that can be connected to a computer through a USB connection, such as a GPS devices, digital cameras, and external hard drives.

Addam Schroll, a security analyst with IT Networks and Security, offers the following suggestions to help avoid malware problems with digital photo frames and other devices that connect to your computer through a USB drive:

-Make sure that your computer has good anti-virus protection with up-to-date virus signatures. Current anti-virus software may detect any malware when you connect such a device.

-Disable autoplay of ALL devices on Windows OS machines. This prevents the malware from being executed as soon as you plug the device in to your machine. Although it could still infect you later if you decide to run any of the executables found on the device.

-Consider operating your computer in “user” as opposed to “administrator” role. That way devices like the digital picture frame cannot be executed without the user being logged in as an administrator and having administrator privileges.

STEAM-CIRT NEWS

STEAM-CIRT is a security team and IT incident response team organized under the ITNS group within ITaP.

For more information about STEAM-CIRT and for security updates throughout the month, visit the STEAM-CIRT Web page at:

http://www.purdue.edu/securepurdue/steam/

Top 10 Purdue e-mail viruses

The following list is a 30-day snapshot of the most active e-mail viruses on the Purdue campus.

The maximum occurrences found in one day are listed with the names of each major virus.

(30-day snapshot as of March17, 2008)

Viruses	Max. Occurrences	Last Occurrence
W32/MyDoom-O	137	2
W32/Netsky-P	85	28
Mal/Iframe-E	71	6
W32/Mytob-Z	38	12
W32/Sality-AA	58	9

MILESTONES

Ask IT Security

Do you have a burning question about your computer security that you would like to ask one of the Information Technology Networks and Security staff? Do anti-virus installations or firewall configurations have you confused? Maybe you are concerned about wireless technology. Asking those questions just got easier. Now through June, security analysts and Identity Access and Management staff will be available once a month to answer questions in person.

Dates for in-person advice are March 26, April 30, May 28 and June 25.
Staff will be available from 11 a.m. to 1 p.m. at an information table in the west lobby of Stewart Center beneath the murals.

For more information, contact Cherry Delaney at 49-61288 or cdelaney@purdue.edu

SECURITY RESOURCES

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

• IRS Security
http://www.irs.gov/individuals/article/0,,id=155344,00.html
phishing@irs.gov to report phishing incidents

Other security resources for scam e-mail.

• Hoax Slayer	www.hoax-slayer.com
• Snopes.com (urban legends)	www.snopes.com