FISSEA Poster, Website and Security Trinket Contest

Entry Form

PLEASE REVIEW RULES BEFORE COMPLETING ENTRY FORM. **All entries must be received by February 5, 2008.** NO LATE ENTRIES WILL BE ACCEPTED. E-mail entries to fissea-contest@nist.gov.

Name of submitter: Rian Campbell

Organization: Federal Reserve Bank of Richmond

Type of entry (poster, website, newsletter, motivational item and/or training/educational exercise/scenario):

Newsletter

Title of Entry:

Security Bits & bytes, Winter 2008

Description of Entry:

The National Information Security Awareness team based at the Federal Reserve Bank of Richmond, develops security awareness training and materials for the 20,000 Federal Reserve System employees. Security Bits & Bytes, the FR's national security newsletter is published quarterly and delivered in paper and online to all employees. Staff are also able to subscribe to the newsletter online, receiving customized e-mail notifications when Security Bits & Bytes is available.

Winter 2008

Security Bits & Bytes

Information Security News for Federal Reserve Employees

Stray Boarding Pass Provides Ticket to Trouble

Picture this… You've just stepped off the plane at the end of a business trip. Your arms are full with your carry-on, laptop bag, magazines you were reading. As you walk through the terminal, you lighten your load by dropping your magazines and boarding pass stub into a nearby trash bin. You think nothing of it – you're just another anonymous traveler passing through the airport.

A few minutes later, a stranger approaches the trash bin and casually pulls out your discarded goods. A half hour later, he's sitting in front of a PC entering your frequent flyer number from the boarding pass onto your airline's Web site. From there, without using a password, he has full access to your personal details – such as passport number and expiration date, nationality and date of birth. In another 15 minutes, he has used that information on publicly available Web databases to find out where you live, who lives with you, where you work, where you went to school and even how much your house was worth when you bought it! All of this happened in the hour since you left the plane.

It sounds like a far-fetched story, but it actually happened to British Airways passenger Mark Broer. We often hear of ways to protect ourselves online – while shopping, banking – but there are still ways to leave a "paper" trail when you least expect it. How about those magazines you tossed at the airport? Did they include a mailing label with your name and address (which can be used to gather even more personal data about you)?

In all cases, and especially when traveling, take care with your personal and Bank information. Regardless of how trivial you think it may be, treat it as "top secret." It is!

Source: http://www.guardian.co.uk

Did You KNOW?

$3.6 million – the number of U.S. adult victims of phishing attacks in 2007, compared to 2.3 million in 2006. Of those consumers who received phishing e-mails last year, 3.3% reported financial losses because of the attacks.

According to consulting firm Gartner, financial Financial losses are on the rise because phishers are now targeting debit cards, rather than credit cards, according to Gartner Consulting. Financial institutions have processes in place to protect consumers from phishing attacks, but now better procedures are still needed for debit cards. *Source: VeriSign, Inc.*

Laugh ☺ Lines

Below is a sampler of tongue-in-cheek definitions straight out of *The Devil's Dictionary 2.0:*

Blog (n.) A diary desired by no one and available to everyone.

E-mail (n.) A form of text communication similar to — but far rarer than — spam.

Social Engineering (n.) [To receive the definition of this term along with a free laptop and a 60" high-def TV, please e-mail your name, address, credit card # (for shipping and handling) and SSN to just.kidding@rich.frb.org. It's that easy!!!]

Spam (n.) The definition of "social engineering" e-mailed to 100 million of your friends.

Source: www.cs.oonline.com

"You've got mail."

Breaking News: Adolescents and their Parents Disagree!

Think you know how much time your kids spend online and what they're doing? You may be surprised.

Earlier this year, Webroot Software surveyed more 600 kids between the ages of 11 and 17 along with their parents. While 70% said their parents ask about their online activities, you be the judge whether these cyberkids are being truthful with their moms and dads.

More than half of the teenagers admitted to buying things online, but 71% of their parents said their children had never made an online purchase. Only 30% of parents said their children use instant messaging and social networking sites like MySpace and Facebook, while 40% of the kids admitted to participating in those sites daily.

Forty-five percent of the polled pre-teens and teens said they spend an average of three or more hours on the Internet daily, but 76% of parents think their kids

continued on page 3

Phishing Hits Home

Were you one of the 73 million adults who received a phishing e-mail between May 2004 and May 2005? Gartner, a leading technology research firm, estimates that nearly 2.4 million online shoppers lost money as a direct result of phishing. Do you know how to avoid being the next victim?

The e-mail message on the right was submitted by an FR employee and is a real example of a phishing e-mail. See if you can find the subtle clues that prove this message is a hoax. *Answers follow.*

From: payments-messages@amazon.com
Sent: Wednesday, October 19, 2005 3:28 AM
Subject: Amazon Payments Billing Issue

Greetings from Amazon Payments .

Your bank has contacted us regarding some attempts of charges from your credit card via the Amazon system. We have reasons to believe that you changed your registration information or that someone else has unauthorized access to your Amazon account Due to recent activity, including possible unauthorized listings placed on your account, we will require a second confirmation of your identity with us in order to allow us to investigate this matter further. Your account is not suspended, but if in 48 hours after you receive this message your account is not confirmed we reserve the right to suspend your Amazon registration. Amazon is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft.

To confirm your identity with us click here:
https://www.amazon.com/exec/obidos/flex-sign-in/ref=pd_irl_gw_r/103-3177084-7567864?opt=oa&page=recs/sign-in-secure.html

After responding to the message, we ask that you allow at least 72 hours for the case to be investigated. Emailing us before that time will result in delays. We apologize in advance for any inconvenience this may cause you and we would like to thank you for your cooperation as we review this matter.

Thank you for your interest in selling at Amazon.com.

Amazon.com Customer Service
http://www.amazon.com

Phishers are continually finding new ways to fool consumers. This message, for example, looks legit and like it was sent from one of the Internet's most trusted companies: Amazon.com. Fortunately, the employee who received this message noticed some subtle hints that made it seem phishy:

1. The extra space before the period. Always check the grammar, spelling, punctuation and writing style of the e-mail message. Businesses go through many editors before publishing something to customers. If you see lots of errors, chances are it is a scam.
2. Again, there is a punctuation error — no period at the end of the sentence.
3. The e-mail requests that Amazon not be contacted about this message for 72 hours. Phishers need time to act on the information you've provided and don't want you to discover their scam too soon. Be wary of any message that does not provide immediate contact information.
4. Finally, the recipient of this message was alerted to the line "Thank you for your interest in selling at Amazon. com." This person had only purchased, never sold, items on Amazon. A lot of scams generalize their wording so they can send it to thousands of people without editing it. Look for things that appear out of the ordinary or do not apply to you.

Source: www.cio.com

Fresh Facts

"You May be a Spammer and Not Even Know it!"

HAVE YOU HEARD OF "BOTNETS?" They are quickly becoming one of the industry's worst information security threats. In fact, it is estimated that over 65% of spam worldwide is sent by botnets.

So, what is a botnet?

A **botnet**, short for **robot network**, is a network of compromised computers that are connected to a central "controller," or main computer controlled by a hacker. Your computer can fall victim to a botnet infection in the same ways it can pick up a worm or virus. Once infected, the bot software sends a notice to the controller. The controller then downloads more malicious software that can take complete control of your computer. All of this can happen without your ever realizing it.

If your computer is part of a botnet, the following could be installed and/or executed:

- ✔ Keystroke logger programs that specialize in capturing personal information including your user name, password, credit card and other financial information.
- ✔ Programs that are used to distribute spam. The next e-mail your neighbor receives regarding a hot stock tip or prescription drugs could be coming from your computer.
- ✔ Denial of service attack programs. The botnet controller can summon tens of thousands of bots, or zombies, to overwhelm web sites, computers or entire networks.

How can I tell if my computer is part of a botnet?

If you're infected with a worm or virus, it's likely you're also part of a botnet. Some of the symptoms of infection are: slow computer and Internet connection speeds; programs on your computer stop working; your hard drive is spinning while you're not using your computer.

How can I protect my computer?

- ✔ Do not click on links in suspicious e-mails.
- ✔ Never open an e-mail attachment unless you know what it is — even if it's from someone you know and trust.
- ✔ Do not visit and/or download free software from untrusted Web sites.
- ✔ Do not use free file sharing programs, as they often contain malware.
- ✔ Use a firewall to filter Internet traffic on your home PC.
- ✔ Use anti-virus and anti-spyware software on your home PC and keep all software up-to-date.

Source: http://www.msiisac.org

What's Bugging You?

A forum for those pesky information security questions

Dear Answer Bug,

My friend was taking some work home on a USB thumb drive, but somehow he lost it. The data was encrypted, though. Is everything okay?

— Concerned

Dear Con,

Losing data is never a good thing. But, since your "friend" took some safety measures, the problem will be easier to deal with.

If your "friend" used a strong encryption program to protect the entire drive, then the person finding it has simply gained a new toy. But there still might be some things to do.

What kind of data are we talking about? System passwords? Personnel files? Customer records? Even if the data is not compromised, we might still be obligated to notify others. Make sure your "friend" talks to the boss right away, so they can determine if steps need to be taken to protect customers, employees, or systems.

Many portable devices come with programs for safeguarding files with encryption or passwords. Some of these are better than others, so check with the Help Desk or the Information Security Department for recommendations.

And be more careful next time, okay? Don't carry around files that you don't need. Keep track of your thumb drive. Call PC Support if you need help encrypting an external drive. And check with the boss before copying highly classified information to a portable device.

— The Answer Bug

Source: Federal Reserve Bank of San Francisco

Breaking News: *continued*

are only online two hours or less a day.

The statistics become even more alarming – 43% percent of the children who use social networking Web sites said a stranger has invited them to meet within the past year. And almost 40% of the kids have received a sexually explicit e-mail or pop-up ad within the past year. One hundred percent of those surveyed use e-mail. Webroot's COO, Mike Irwin, cautions, "The good news here is that these potential problems can be largely avoided if parents apply the same vigilance to the online world as in the offline world. Direct and ongoing conversations with our kids, and establishing guidelines with the help of the right technology, will go a long way in supporting good judgment."

A list of links and resources to help keep your kids safe online can be found on the National IS Awareness site: Go to https://nisap.frb.org, select "IS Week 2006" and "Kids' Internet Safety" from the menu.

Attention Parents! What would you ask your teens if you could be assured an honest answer about their online activities? Submit your question(s) via e-mail us, and *Security Bits & Bytes* staff will interview a select group of kids for the real scoop. Results will be published in a future issue of the newsletter.

www.informationweek.com

Security Nightmares

Financial Crimes Hit Close to Home

Financial crime is a widespread concern among Americans. According to a survey, 40% say that they've been victims of identity theft or know someone who has. But the survey also reveals that people often leave themselves open to financial crimes, even in their own households, by using paper checks rather than direct deposit. Last year, 57,000 checks issued by the U.S. Department of Treasury were fraudulently endorsed, while problems with direct deposit payments were negligible. In fact, while paper checks make up about 20% of the total Social Security and Supplemental Security Income payments, they account for more than 90% of reported payment problems.

Source: National Security Institute Inc.

Security Breach Involves Babies

Georgia officials warned the parents of 140,000 babies that a security lapse exposed some of their personal and medical information to the risk of fraud. Earlier this year, the Georgia Department of Human Resources mailed letters to all parents of infants born in the state between April of 2006 and March of 2007. The letters informed the parents that paper records containing their Social Security numbers and information about their medical histories were improperly discarded.

Source: National Security Institute Inc.

Voters' Personal Info Leaked

About 100 computer discs with 1.3 million Chicago voters' Social Security numbers have been mistakenly distributed to aldermen and ward committeemen, and the whereabouts of at least six more CDs with the same information are unknown, according to the Chicago Board of Elections. Officials say that, so far, there has been no evidence of identity theft as a result of the lapse.

Source: National Security Institute Inc.

New Yorkers Most Vulnerable to ID Theft

ID thieves are taking a big bite out of the Big Apple. New York state has the highest rate of identity fraud, according to research from ID Analytics Inc. The report finds that Wyoming, Vermont and Montana have the lowest rates. Experts say that what's most meaningful about the research is that it can help identify specific areas where identity thieves may be operating in an organized manner. The data has actually been identified down to the ZIP code level, offering precise visibility into concentrations of identity fraud. The 10 worst states for ID fraud are: New York, California, Nevada, Arizona, Illinois, Hawaii, Oregon, Michigan, Washington and Texas.

Source: National Security Institute Inc.

FBI Losing Three to Four Laptops Every Month

Between three and four FBI laptop computers are lost or stolen each month on average, according to the Justice Department's inspector general. The FBI is said to have reduced the number of thefts and disappearances of laptop computers, but that not all problems were corrected as urged in a report five years ago. Perhaps most troubling, the FBI could not determine in many cases whether the lost or stolen laptop computers contained sensitive or classified information, according to the report.

Source: National Security Institute Inc.

Beware of "Drive-By Pharming" Attacks

Security researchers have discovered a hacking technique dubbed "drive-by pharming."

Here is how it works: Imagine that whenever you wanted to go to your bank, you picked up your phone directory, looked up the bank's address, and then drove there. In drive-by pharming, attackers essentially replace the paper phone book in your house with an online version that they created for when you surf the Internet. Thus, when you pick up that rogue phone book to get your bank's Web address, it'll actually give you the wrong one. Once you've arrived at this bogus cyber address, the attackers will have set up a fake bank Web site that looks just like your bank. When you do business with this fake bank, you'll give up all your sensitive account information. However, you'll never realize that you were at a fake bank, because you trusted the address you got from your "legitimate telephone book."

Here is how you can protect yourself: The good news about drive-by pharming is that it's easy to defeat. The key lies in the phony phone book. The attackers can only slip you that bogus book (which, in techno-speak, is actually a domain name server) by figuring out what kind of router you use on your computer (which is a simple operation), then trying to guess your password for that router. So the solution comes down to that age-old advice: Never use default passwords. And when you create a password, make sure it's a good one!

Source: National Security Institute Inc.

CSI: Campaign to Stop ID Theft

Uncover clues to keep your identity safe

If these "Security Nightmares" make you worry about losing your identity, rest assured that help is on the way. Coming to the Federal Reserve System soon, Information Security (IS) Week will feature activities to help you uncover the clues to keep your identity safe.

For National Information Security Awareness information, visit the Web site at https://nisap.frb.org. For general assistance, contact your District's Information Security staff.

***Bits & Bytes* Contributors**

Content by:
Federal Reserve Bank of Richmond—
Information Security

Editing and Graphic Design by:
Federal Reserve Bank of Richmond—PA/Graphics

Feedback & Suggestions

To share ideas for future *Bits & Bytes* stories or to offer feedback on the information contained in this issue, please contact: Rian Campbell (rian.campbell@rich.frb.org), (804) 697-8675, or Irina Piven (irina.piven@rich.frb.org), (804) 697-8609.