ISSN: 1545-679X

Information Systems Education Journal

Volume 5, Number 36 http://isedj.org/5/36/ December 11, 2007

In this issue:

Getting A Hook On Phishing

Charles E. Frank
Northern Kentucky University
Highland Heights, KY 41099 USA

Laurie A. Werner
Miami University Hamilton
Hamilton, OH 45011 USA

Abstract: Despite increased user awareness, phishing activities represent a serious threat to information security. Phishing sites are increasingly sophisticated and continue to defraud users. Computing professionals need to know how phishing works. This paper presents a series of laboratory exercises to educate future computing professionals about the mechanics of phishing attacks. These laboratories teach students how an email "from" address can be spoofed, how phishing emails can lure their victims, and how easy it is to produce a fraudulent web site and a phishing email. This paper discusses how future computing professionals can minimize phishing vulnerabilities.

Keywords: phishing, security, spam, phishing email, laboratory activity

---

Recommended Citation: Frank and Werner (2007). Getting A Hook On Phishing. *Information Systems Education Journal, 5* (36). http://isedj.org/5/36/. ISSN: 1545-679X. (Also appears in *The Proceedings of ISECON 2007:* §3523. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/5/36/**

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: http://isedj.org/ • Contact person: Don Colton (editor@isedj.org)

This paper was selected for inclusion in the journal as part of the ISECON 2007 best papers group. Best papers received preliminary reviews by three or more peers placing them in the top 30% of papers submitted and final reviews placing them in the top 15% by three or more former best papers authors who did not submit a paper in 2007.

EDSIG activities include the publication of ISEDJ, the organization and execution of the annual ISECON conference held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates.

Getting a Hook on Phishing

Charles E. Frank
Northern Kentucky University
Department of Computer Science
Highland Heights, KY 41099
frank@nku.edu

Laurie Werner
Miami University Hamilton
Department of Computer and Information Technology
301E Mosler Hall
1601 University Blvd
Hamilton, Ohio 45011
wernerla@muohio.edu

ABSTRACT

Despite increased user awareness, phishing activities represent a serious threat to information security. Phishing sites are increasingly sophisticated and continue to defraud users. Computing professionals need to know how phishing works. This paper presents a series of laboratory exercises to educate future computing professionals about the mechanics of phishing attacks. These laboratories teach students how an email "from" address can be spoofed, how phishing emails can lure their victims, and how easy it is to produce a fraudulent web site and a phishing email. This paper discusses how future computing professionals can minimize phishing vulnerabilities.

KEYWORDS: phishing, security, spam, phishing email, laboratory activity

1..INTRODUCTION

The Anti-Phishing Working Group (APWG, 2007) gives this definition of phishing: "Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials." Spoofed emails use social engineering to lead consumers to counterfeit web sites designed to trick them into divulging sensitive information such as usernames, passwords, credit card numbers, and social security numbers. Technical subterfuge can plant key logging software on an unsuspecting user's system to steal personal and financial information.

While writing this paper, one of the authors received an email requesting that he complete an "online client form" at Commerce Bank. Clicking on the link within the email took him to a web site with the bank's logo, which asked for his customer id and password. After he entered fictional information, he pressed the "Confirm & Exit" button. He was taken to the real Commerce Bank web site. This was a typical phishing exploit. It is fair to ask, "Is it not obvious when an email is a phishing attack?" Research data suggests otherwise. Users fail to recognize fraudulent emails and websites, and assume that valid emails and websites are bogus, with astonishing regularity (Robila, 2006). Thus, phishing presents a significant threat to e-commerce growth, from banking to shopping on-line.

According to the Anti-Phishing Working Group (APWG, 2007), "The number of unique phishing web sites detected by APWG rose to 55,643 in April 2007, a massive jump of nearly 35,000 from March…April 2007 saw the number of brands being attacked rise 174...more non-financial brands…including social networking, VOIP, and numerous large web-based email

providers." Lininger and Vines (2005) estimate that "3-5% of the people who receive the email go on to surrender their information to crooks." In an ironically amusing *eWeek* slide show, Vargas (2007) attributes spam-scam gullibility to a level of innocence. "This naïveté occurs at both ends of the age spectrum, the researchers' claim, with computer-savvy youth being naïve to business practices, and older, business-savvy people being less computer-savvy and more trustful of apparent virtual e-businesses than younger people."

Since the number of Phishing websites is growing as the number of brands attacked expands, it is safe to assume that phishers would not invest the time and effort to send these emails and create the fraudulent websites if significant numbers of user-victims did not unwittingly disclose valuable account and personal information.

Dharmija, Tyger and Hearst (2006) conducted a usability study that produced some striking results. "Good phishing web sites fooled 90% of participants." Twenty-three percent of the college-educated participants "did not look at browser-based cues such as the address bar, status bar and the security indicators, leading to incorrect choices 40% of the time." User education and computer sophistication do not immunize us against phishing. Dharmija, Tyger and Hearst (2006) "found that some visually deceptive attacks can fool even the most sophisticated users." Surprisingly, "neither education, age, sex, previous experience, nor hours of computer use showed a statistically significant correlation with vulnerability to phishing." (Dhamija, 2006)

James (2007) notes that phishers have become more sophisticated. It is no longer obvious whether an email is a valid communication from your bank or a phishing solicitation. It is no longer obvious whether a web site asking for account information originates from an actual bank's server or from a fraudulent phishing site.

2. LAB EXERCISES

McKinney (2006) found that laboratory activities in college courses have many benefits, in particular "deeper learning, developing skills wanted by industry." Thus, we devised a series of six laboratory exercises to provide our computing students some valuable spam-scam defenses. Since we believe that it is important for future computing professionals to understand how phishing attacks work, the exercises start with analyzing phishing emails and websites and proceed to the mechanics of actually creating a phished scenario. Jakobsson and Myers (2007) agree with this strategy: "As often seen in computer security, the defenders have to wear the hat of the attacker to understand how to best do their jobs."

While allowing students to act as attackers, we create an opportunity to expound the legal and ethical consequences of malicious hacking. We incorporate several ethical discussions, including the immorality of stealing using phishing, into the post lab discussions. For our protection, in accordance with our institutional requirements, and to emphasize the gravity of hacking, students sign the "Computer Security Statement of Ethics" (Computer, 2007) at the beginning of the phishing exercises.

Phishing IQ Test

In Lab Exercise 1 (Phishing IQ, 2007), we have our students take the ten question online SonicWall Phishing IQ Test (2007). Each question displays an email message with the actual active URL link in the status bar. The test taker indicates whether each email is legitimate or is phishing. After scoring, the Phishing IQ Test provides an explanation of both legitimate and counterfeit indicators within each email. From these descriptions, the students learn what indicators identify the authenticity of an email message. Robila and Ragucci (2006) made use of the Phishing IQ test in a non-majors course, with a significant improvement in students' ability to identify threats. Jakobsson and Myers (2007) remark, "the author has seen many computer security experts fair quite poorly on this quiz." Indeed, the Phishing IQ Test (2007) web site states that only 6.2% have answered all ten questions correctly. At the very least, the Phishing IQ test offers a starting point for studying phishing, whether the instructor's goal is to present phishing in breadth or in depth.

Lab Exercise 1 - Phishing IQ Test
Go to http://www.sonicwall.com/phishing/ and take the SonicWALL Phishing IQ Test. Print and hand in the final screen, which gives your test results. Before you begin, note that only 6.2% of the test takers have gotten all 10 questions correct. Your professor did not get a perfect score. Report your results honestly. You will not be graded on how many questions you answered correctly. At the end of the test, read the "Explain Answer" for **all** of the questions.

1. What was your score on the Phishing IQ Test?
2. Which questions did you answer correctly? For the phishing emails, what identified them as suspect to you?
3. For the questions you missed, describe two keys that identified the email as phishing or legitimate, depending on how you misjudged it.

Analysis of Phishing Laboratory

A successful phishing email has a compelling message. It may use the targeted institution's logo and graphics to give the appearance of authenticity. The fraudulent web site is often a copy of the targeted institution's login page with modifications to the code behind it, intended to steal user credentials. The MillerSmiles.co.uk website (2007) contains an archive of phishing swindles collected since 2003. As of June 15, 2007, the MillerSmiles database included 189,493 scam reports. The non-profit Anti-Phishing Workgroup (APWG, 2007) web site has similar archives, and recently collaborated with MillerSmiles. In Lab Exercise 2 (Analysis, 2007) the student analyzes several emails and web sites from the archives. This activity has a twofold purpose: first, to expose how the scenario and the wording of the email lure the victim and secondly, to identify the technical tricks which provide the email and scamming web site the appearance of legitimacy.

Lab Exercise 2 - Analysis of Phishing
Go to http://www.millersmiles.co.uk/, an archive of phishing scams. Choose three different phishing scams from the archive that have both an email and a web site. Keeping in mind what you learned in exercise 1, answer the following questions about these scams.

1. Give the link to the phishing scam.
2. What scenario is used in the email? What is the type of scenario?
3. How does the wording of the email lure the recipient to click on the link?
4. What technical tricks are used to give legitimacy to the email?
5. Where is the location of the phisher?
6. Is there anything in the email that indicates this is a phishing scam?
7. What information does the web site collect from the victim?
8. What technical tricks are used to give legitimacy to the website?
9. Discuss whether the web site appears legitimate? Is there anything that indicates this is a phishing web site?

Spoofed E-Mail Laboratory

Although the technique is readily available in trade books such as James (2005) and Cole (2001), computing students may not know how to spoof an email sender. In Lab Exercise 3 (Spoofed, 2007), the students forge an email from a classmate to themselves. James (2005) discusses which parts of the email header can and cannot be forged. Besides exposing the spoofing mechanism, the purpose of this exercise is to raise the question of email authentication as a valuable countermeasure to phishing.

Lab Exercise 3 - Spoofing Email
In this lab, you will send a spoofed email from your lab partner to yourself. This will illustrate how phishing can spoof the sender's email address.
1. Open a command shell.
   Start | Run
   cmd
2. Telnet to the mail server on port 25.
   C:> telnet mail.nku.edu 25
3. We have to identify by saying HELO
   HELO
4. Enter the spoofed sender and the recipient of the email. "partner" is your lab partner's email address. "you" is your email address.
   MAIL FROM: partner@nku.edu
   RCPT TO: you@nku.edu
5. Use the DATA command to send the message.
   Subject: Test
   Write some message
   to you from your partner.
6. Enter a period on a separate line to send the email and "QUIT" to terminate telnet.
   .
   QUIT
7. Check your email. Print out and hand in the email message.

Phishing Web Site Laboratory

In Lab Exercise 4, students discover how easy it is for a phisher to build a realistic looking fraudulent web site. First, the students copy a login page from a financial institution to their desktop and determine that the links all work. Second, they locate the event handler that needs to be changed. Third, students modify an instructor-provided website.

For legal reasons, we do not fake an actual financial institution's web site. As an alternative, we have the students fake the university registration site's login page in the lab using C#.NET web form in a closed lab environment.

Phishing Email Laboratory

In Lab Exercise 5 (Phishing email, 2007), the students construct a legitimate looking, compelling HTML email with a link to a version of the phishing web site of Lab Exercise 4. The students have a rich array of model phishing emails in lab exercises 1 and 2. The main grading criterion is the effectiveness of the email, as judged by the instructor. The main purpose of this exercise is to see the small amount of effort invested in creating a credible phishing email.

Lab Exercise 4 - Phishing Web Site
In this lab, we will construct a phishing web site to steal a username and password.
1. Go to the US Bank login page. It is located at
   a) http://www.usbank.com or
   b) https://www4.usbank.com/internetBanking/RequestRouter?requestCmdId=DisplayLoginPage.
2. Right click on this page and copy it to a folder on your desktop.
3. Check the links on the page. Do they work? Hand in your answer with this assignment.
4. Show the page's source code. View | Page Source.
5. Find the action event within the form tag. Edit | Find | "action". This is the code behind that needs to be changed to produce a phishing web site. For legal reasons, we are not going to build a phishing web site for a real financial institution. Instead, we are going to create a login page for Northern Kentucky University's Norse Express using C#.Net.
6. Create a web form the fakes the Norse Express login page as best that you can. It is located at https://express.nku.edu/ia-bin/tsrvweb.exe?&WID=W&tserve_tip_write=%7C%7CWID&tserve_trans_config=astulog.cfg&tserve_host_code=HostZero&tserve_tiphost_code=TipZero.
7. Write the "Click Event" for the "Login button". The event handler should append the text in the "Student ID:" and "Pin" textboxes to the end of a file. Then, your web site should redirect the user to the real login page.
8. Demonstrate your program to your instructor.
   Show your instructor the code for your click event handler.
   Show your instructor the contents of the file that records student ids and pins.

Lab Exercise 5 - Phishing Email
My version of the phishing web site is temporarily hosted at the URL from Lab 4. It will be taken down after this class. In Labs #1and #2, you looked at examples of spoofed emails. In this lab, you are to design an HTML email with a link to my fake login page from Lab 4. The email should request the student login. Your email should look legitimate and should have a compelling message. Send the email to your instructor at _____.

Online Shopping Service Laboratory

Lab Exercise 6 (Phroogle Lab, 2007) is based on a case study in Jakobsson and Myers (2007). It utilizes their fake shopping website, Phroogle (2007), to reveal the mechanics of a potential phishing threat.

The user enters a product name, such as a laptop computer or digital camera, that she is interested in buying. Phroogle returns a price 10% below the lowest price found on Yahoo! Shopping. Phroogle then requests that the user enter either her credit card or banking account information. "Phroogle demonstrates that a phisher could easily exploit shopping agents to set up an effective phishing attack." (Jacobsson 2007) The purpose of the online shopping exercise is twofold: to show how fruitfully an online shopping service such as Google Shopping (2007) or Yahoo! Shopping (2007) can be phished and to convince students that phishing is a serious threat to them personally as well as to the future of e-commerce.

3. COMPANY PRACTICES

It is common for companies to email their customers using HTML and scripting languages to enhance the email's appearance and usability. These emails may contain an HTML replica of the login page. Alternatively, these emails may contain a link to the login web form at the company's web site. Email is a convenient and cost effective way for a company to communicate with its customers. Yet the emails can easily be phished.

Lab Exercise 6 - Phroogle
This lab illustrates a potential phishing manipulation of a shop-bot like Google Shopping, which used to be name Froogle, or Yahoo Shopping. This lab is based on a case study found in Jakobsson and Myers' fake shopping phishing site named Phroogle. (Jakobsson, 2007)

1. Read Jakobsson & Myers, Sect. 1.6.
2. Go to Google Shopping at http://www.google.com/products . Type in the text box "apple ipod nano 4gb". Print out this page and attaching it to your assignment.
3. Go to Yahoo! Shopping at http://shopping.yahoo.com/. Type in the text box "apple ipod nano 4gb". Print out this page and attaching it to your assignment.
4. Go the fictitious phishing site http://homer.informatics.indiana.edu/cgi-bin/phroogle/phroogle.cgi. Type in the text box "apple ipod nano 4gb". Explore the options on this site. Print out one of the Phroogle order pages.

Ignore the logo of a fish hook coming out of a laptop computer. Write a paragraph discussing how effective this phishing technique is. How would a user know that this was a phishing rather than a legitimate site?

Companies have been slow to protect users from phishing swindles, leaving the burden of protection on the users. Users suffer when their credentials are compromised, not the companies that they are trying to patronize. Schneier (2007) maintains that companies will not fully protect users until required to do so by law and with stiff penalties. "The organizations we trust to protect our personal information do not suffer when information gets exposed." Companies are beginning to implement some anti-phishing protections, such as dynamic security skins and two-factor authentication. Both of these require some effort on the part of the user.

When Vanguard, the mutual fund company, sends an email requesting that a customer

login to her account, it tells her to "Go to Vanguard.com". Rather than clicking on a link in the email, the customer types the provided Vanguard URL into the browser. This requires a small amount of additional work, presumably to ensure that the URL is valid. However, a similar phishing email might direct the user to enter the URL for a bogus website. For example, the email might ask the user to enter the URL www.vanguardlogin.com into her browser. Since the URL appears legitimate, it might not raise suspicion.

What are companies doing to protect users from phishing scams? In 2005, Dhamija and Tygar (Dhamija, 2005) introduced dynamic security skins, which place "a very low burden on the user in terms of effort, memory and time." Many companies, such as Vanguard (2007), Bank of America (Bank, 2007), and PNC bank (PNC 2007) recently adopted this technique. The Vanguard group login page uses one page for entering the user name and a second page for entering the password. On the password page, Vanguard displays a user selected "security image" that the user has previously chosen and given a title. The user selects an image from a set provided by Vanguard. Typical images are animals, flowers, cars, teddy bears and scenery. The user titles the image. For example, a cat or dog's image might be titled with a pet's name. The user visually verifies the image and its name, before logging in. Incorporating the customization step into the login process makes it very difficult to produce a fraudulent copy of the login web page. Bank of America (Bank, 2007) describes its security skin protocol to users as follows:
SiteKey protects you from identity theft and fraud in two ways:

1. You know it's really us - when you see your SiteKey, you can be certain you're at the valid Online Banking website at Bank of America, and not a fraudulent look-alike site. Only enter your Passcode when you see the SiteKey image and image title you selected.
2. We know it's really you - we display your SiteKey when we recognize you as the true owner of your account. If you don't sign in from the computer you told us to recognize, we'll ask a challenge question.

One of the authors recently received notification of changes in her credit union's Home Banking log in. The credit union now requires enrollment in a Multi-Factor Authentication process "to ensure an extra layer of security for your online account(s)." (Credit Union, 2007) Figure 1 in the Appendix shows the sample enrollment form.

After completing the phishing lab exercises, students are prepared to discuss the role of vendor and user in the anti-phishing war. As banks add some features to thwart phishers and enhance security, users must participate in the security process. It is surely worth a few extra keystrokes for a larger measure of security.

4. PHISHING PROTECTION

Nielsen (2004) contends that computer security is too complicated to place the burden on users to protect themselves. He argues, "The only real solution is to make security a built-in feature of all computing elements." The success of phishing and recent research (Robila, 2006), is evidence that all levels of users are vulnerable. As recently as June 30, 2007, Elinor Minor, a ten-year tech Internet reporter, "fell for one of those silly phishing scams. The kind that I previously took sanctimonious pride in having avoided." (Mills, 2007) What protections are available for users at home or at the workplace?

Secure your web browser: The Firefox 2 browser contains built-in phishing protection that warns users of suspected web forgeries and offers to take the user to Google to find the real web site. (Firefox, 2007) This feature is enabled by default. Information security should see that its company's employees use browser and email software that provide phishing protection. CERT has a useful site for browser tips. (CERT, 2007)

Update everything regularly: Operating system, AV and firewalls, Applications such as MS office. In addition to the browser checking for forgeries, AV and firewall software can thwart the phishers Trojans.

Use Anti-Spam filters: The authors have found that although the anti-spam filters used at their universities catch a high percentage of phishing emails, some get through the filters. Professional phishers can test their emails against popular anti-

spam filters and tune them to bypass the filters. Therefore, users must question emails from unknown sources.

Use at least two spyware removal tools: Run them regularly. (McDowell, 2006)

Exercise extreme caution when downloading files to your system. (McDowell, 2006)

Do not accept any **free internet offers**. (McDowell, 2006)

5. CONCLUSION

Experts agree that phishing is a very real and continuing threat to the IT industry. In an interview with IT Pro, Dave Cole of Symantec Security Response team stated that "it's more important than ever to be vigilant… This means protecting users *and* infrastructure. It's not enough just to have a firewall…. these phishing attacks up the ante at the desktop." (Interview, 2005) As educators, we can use lab activities efficiently and effectively to integrate anti-phishing savvy into existing courses.

A current general education computer literacy course should incorporate a computer security component. (Werner, 2005) The Phishing IQ test and the Analysis of phishing labs would be an attractive addition to a computer security module in a non-major's course. A recent paper successfully teaches "people about strategies to avoid falling for phishing attacks" (Sheng, 2007) using an interactive game that takes only fifteen minutes. Exposing the non-technical student to the phroogle website (Lab 6) could create more discerning on-line shoppers.

The spoofing email lab (Lab 3) could serve a two-fold purpose in a computing major's first network fundamentals course at the juncture where technical aspects of email are presented. For example, in their Computer Networking text, Kurose and Ross (2008) provide an email lab very similar to the Spoofing Email Lab described above, as a way of introducing protocols and port numbers. Simultaneously suggesting the concept of spoofing email introduces spam as a topic for discussion or assignment. A course that includes web page design and construction could assimilate a phishing element into the web site construction, similar to Labs 4 and 5.

Not all of our students will become security specialists, but most will live and work in an environment that is vulnerable to phishing scams. Let us begin teaching them to thwart phishers within existing non-major's courses as we prepare modules related to end-user security, and within computing major's courses in networking, security and e-commerce.

6. REFERENCES

Analysis of Phishing Lab (2007) web site, http://www.nku.edu/~frank/phishing/Analysis.htm.

APWG, Anti-Phishing Workgroup (2007) web site, http://www.antiphishing.org/

Bank of America (2007) log in page https://www.bankofamerica.com/index.jsp

Beck, L., Chizhik, A., McElroy, A., (2005), "Cooperative Learning Techniques in CS1: Design and Experimental Evaluation", Proceedings of the 36th SIGCSE Technical Symposium On Computer Science Education, St. Louis, Missouri, USA, February 23-27, pp. 470-474

CERT browser security tips, (2007), http://www.cert.org/tech_tips/securing_browser/

Cole, Eric, (2001) Hackers Beware: The Ultimate Guide to Network Security, Sams Publishing.

Computer Security Statement of Ethics, (2007), http://www.nku.edu/~waldenj1/classes/2006/fall/csc582/ethics-statement.html.

Credit Union (2007) website, http://www.gecreditunion.org

Dhamija, Rachna and Tygar, J. D., (2005**)** "The Battle Against Phishing: Dynamic Security Skins", Proceedings of the 2005 Symposium on Usable Privacy and Security, July 6-8**,** Pittsburgh, Pennsylvania, pp. 77-88.

Dhamija, Rachna, Tygar, J. D., and Hearst, Marti, "Why phishing works", Proceedings of the SIGCHI conference on Human Factors in computing systems, April 22-27, 2006, Montréal, Québec, Canada, pp. 581-590.

Firefox 2 Phishing Protection, (2007), http://en-us.www.mozilla.com/en-US/firefox/phishing-protection/.

Google Shopping (2007) web site, http://www.google.com/products.

Interview with Dave Cole, (2005), News Briefs, IT Pro, May-June 2005

Jakobsson, Markus and Myers, Stephen, (2007), Phishing and Countermeasures, Wiley-Interscience, New Jersey.

James, Lance, (2005), Phishing Exposed, Syngress Press, Massachusetts, pp. 98-99.

Kurose, James and Ross, Keith, (2008), Computer Networking: A Top-Down Approach, 4th edition, Addison-Wesley, Massachusetts.

Lininger, Rachael and Vines, Russell Dean, (2005), Phishing: Cutting the Identity Theft Line, Wiley, New Jersey.

McDowell, Karen. (2006) "Now That We Are All So Well-Educated about Spyware, Can We Put the Bad Guys out of Business?" Proceedings of the 34th annual ACM SIGUCCS Conference on User Services, Edmonton, Alberta, Canada, pp. 235 - 239

McKinney D. and Denton, L. (2006) "Developing Collaborative Skills Early in the CS Curriculum in a Laboratory Environment", Proceedings of the 37th SIGCSE Technical Symposium On Computer Science Education, Houston, Texas, USA, March 1-5, pp 138-142.

MillerSmile.uk.co. (2007), web site http://www.millersmiles.co.uk/

Nielsen, Jacob, (2004), "User Education Is Not the Answer to Security Problems", http://www.useit.com/alertbox/20041025.html

Phishing Email Lab (2007) web site, http://www.nku.edu/~frank/phishing/Email.htm.

Phishing IQ Test Lab (2007) web site, http://www.nku.edu/~frank/phishing/PhishingIQTest.htm.

Phishing Web Site Lab (2007) web site, http://www.nku.edu/~frank/phishing/WebSite.htm.

Phroogle Lab (2007) web site, http://www.nku.edu/~frank/phishing/Phroogle.htm

Phroogle (2007) web site, http://homer.informatics.indiana.edu/ cgi-bin/phroogle/phroogle.cgi.

PNC Bank, (2007), login page, https://www.accountlink.pncbank.com/.

Robila, Stefan A and J. Ragucci, (2006), "Don't be a phish: steps in user education", Proceedings of the 11th Annual SIGCSE Conference on Innovation and Technology in Computer Science Education , Bologna, Italy, pp. 237 - 241

Schneier, Bruce and Ranum, Marcus. (2007) "Does secrecy help protect personal information?" Information Security Magazine, January 2007 , http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1256979,00.html

Sheng, Steve, and Magnien, Bryant, and Kumaraguru Ponnurangam and Acquisti Alessandro and Cranor, Lorrie Faith and Hong, Jason and Numge, Elizabeth (2007) "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish." Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania, pp. 88-99.

SonicWall Phishing IQ Test (2007) web site, http://www.sonicwall.com/phishing/.

Spoofed Email Lab (2007) web site, http://www.nku.edu/~frank/phishing/SpoofedEmail.htm.

Vanguard Group, Inc. (2007) login page, https://flagship.vanguard.com/VGApp/hnw/HomepageOverview.

Vargas, Lisa, (2007), "Slide Show: Sucking the Gullible Into 'Scam-Spam'", eweek, June 28, 2007, http://www.eweek.com/slideshow/0,1206,pg=0&s=25932&a=210554,00.asp, accessed June 29, 2007

Werner, Laurie, (2005), "Redefining Computer Literacy In The Age Of Ubiquitous Computing", Proceedings Of The 6th Conference On Information Technology Education, Newark, New Jersey, pp. 95-99

Yahoo! Shopping (2007) web site, http://shopping.yahoo.com/.

Appendix

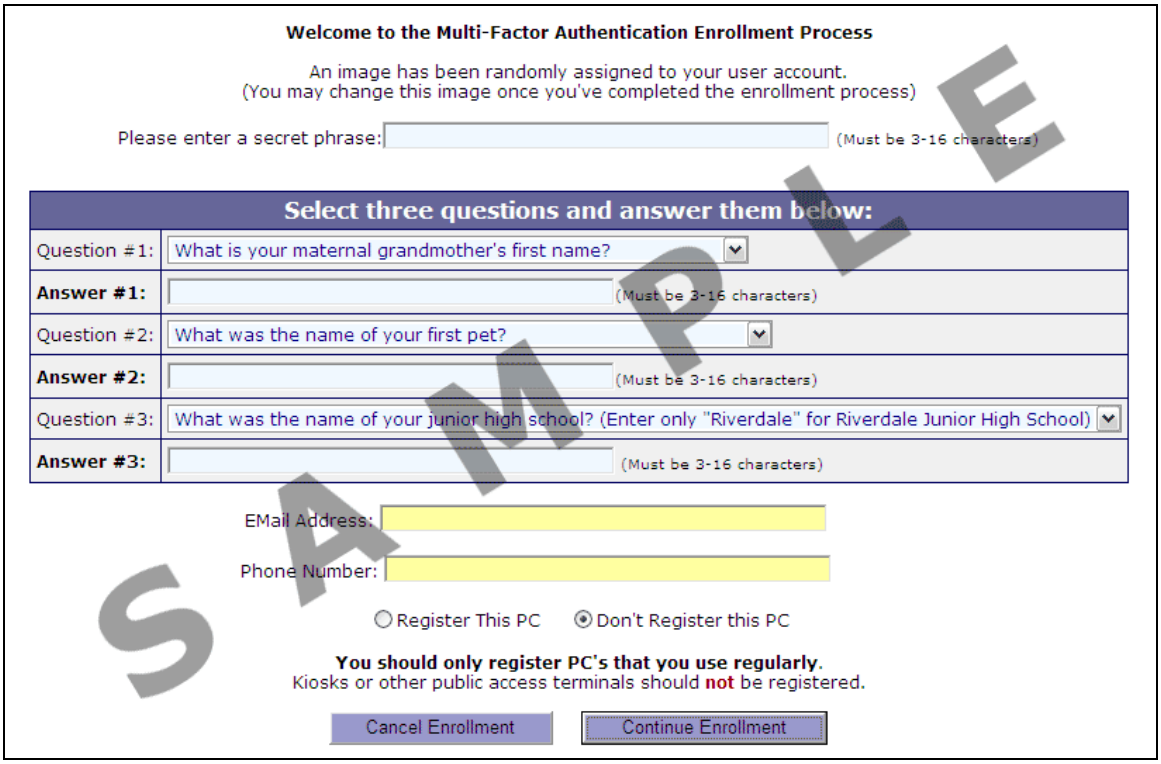

Figure 1