Analysis of an Anti-Phishing Lab Activity

Laurie Werner
wernerla@muohio.edu

Jill Courte
courteje@muohio.edu

Miami University Hamilton
Department of Computer and Information Technology
301C Mosler Hall
1601 University Blvd
Hamilton Ohio 45011

Abstract

Despite advances in spam detection software, anti-spam laws, and increasingly sophisticated users, the number of successful phishing scams continues to grow. In addition to monetary losses attributable to phishing, there is also a loss of confidence that stifles use of online services. Using in-class activities in an introductory computer course is one way of familiarizing students with phishing and teaching them how to recognize a phishing email in order to avoid becoming victims. This paper analyzes one activity based on an online phishing IQ test.

Keywords: phishing, information security, crimeware, lab activities, computing literacy

1. INTRODUCTION

Despite many advances in anti-spam software and email filters, the success of phishing crimes continues to escalate. Consumer groups and security specialists both crowned phishing as a serious security threat in 2007. Consumer Reports listed phishing as one of four major online hazards, along with viruses, spam and spyware. (Consumer Reports, 2008) The SysAdmin, Audit, Network, Security Institute (SANS) reported that spear phishing attacks are among the most critical on their annual top-20 list of Internet threats. (SANS, 2007)

Since 2004, the monetary losses due to phishing emails have steadily increased. Taking the bait can cost users a few dollars from a single online purchase or become the gateway to total identity theft. In 2007 alone, the Federal Trade Commission (Staff Report, 2008) reported $1 billion in losses due to phishing scams. In September 2006, Consumer Reports annual *State of the Net* article indicated that the "median cost per phishing incident was $850 — five times higher than the median cost of $165 in 2005." In the 2007 *State of the Net* article, Consumer Reports found that "Eight percent of respondents submitted personal information in response to conventional phishing e-mails in the past two years, a number that has remained unchanged over the past two years." Consumer Reports also agreed with the FTC that US consumers lost $1 billion through phishing scams in 2007. Even the Federal Deposit Insurance Corporation (FDIC) has a website dedicated to Phishing Scams where they begin with a simple definition: "The term *phishing* – as in fishing for confidential information - refers to a scam that encompasses fraudulently obtaining and using an individual's personal or financial information." (FDIC, 2008)

Beyond financial losses, there is a loss of trust in institutions whose brands are hijacked, and consumer confidence in e-commerce declines. Tom Longstaff, CERT's deputy director for Technology agrees: "The real insidious part of phishing is not the money that they lose. It's not the money the customers lose, and it's not the money that the financial institutions lose. Those are very bounded, and they tend to be fairly easily recouped. What really gets damaged most in a phishing attack is the relationship between the client and the financial institution. Because now, clients can't really trust that they're interacting correctly with their institution, and institutions can't trust that clients are always going to do the right thing because they can be easily led down this garden path." (Longstaff, 2007)

Authors Jakobsson and Ramzen and the Federal Trade Commission (FTC) agree that education has a role in thwarting phishing attacks as well as crimeware in general. Jakobsson maintains that "a typical user does not know how to identify a phishing email" and that "most people want to trust what they see," making the user education process complex but essential. (Jakobsson, 2007) At a recent FTC summit "there was consensus that more school-based education on computer security, cybersafety, and cyber ethics is a good idea." (FTC, 2008)

Phishing attacks do not appear to be decreasing any time soon. According to the latest monthly report from the Anti-Phishing Working Group (APWG, 2008), "The total number of unique phishing reports submitted to APWG in January 2008 was 29,284, an increase of over 3,600 reports from the previous month." Worse yet, users who are hooked by a phishing email might be instrumental in future attacks on others. Visiting a fraudulent website can result in installation of crimeware on a user's machine. A key-logging Trojan can grab the unsuspecting user's passwords and account information, while masquerading malware can turn a user's computer into a bot that distributes malware to other users.

2. PHISHING IQ TEST AS A CLASSROOM ACTIVITY

Frank and Werner suggested that using an online phishing IQ test as a lab activity could be a valuable tool in the security component of a general education computer literacy course. (Frank, 2007) To further that work, we tested the value of the Sonicwall phishing IQ test (www.sonicwall.com/phishing) as a learning tool from the student's perspective. Before and after questionnaires were designed to determine if the Sonicwall phishing IQ test could effectively teach students about phishing email scams and improve their confidence in their ability to detect a phishing email.

In the summer of 2008, 45 students in four sections of an introductory computing course voluntarily completed a short pre-test survey before taking the ten question online SonicWall Phishing IQ Test (Sonicwall, 2008) followed by a post-test survey. Questions on the pre-test survey included demographic and general questions about their phishing knowledge, as well as 2 questions used to measure the effectiveness of the activity, *I know what phishing is*, and *I am confident in my ability to detect a phishing email*. On the post-test survey, students entered their phishing IQ test score and again answered the questions: *I know what phishing is*, and *I am confident in my ability to detect a phishing email*. Most questions used a 5-point scale ranging from strongly agree (1) to strongly disagree (5).

The Sonicwall Phishing IQ test contains 10 questions, with each question displaying an email message including the actual URL link in the status bar. The test taker indicates whether each email is legitimate or is phishing. After scoring all questions, the test provides an explanation of both legitimate and counterfeit indicators within each email. From these descriptions, we hope the student learns what indicators identify the authenticity of an email message.

We hypothesized that the phishing IQ test would help non-computing major students feel more confident about detecting a phishing email. There was no discussion of computer security topics or of phishing in the class prior to the day of the surveys. Since we were not the instructors for the four sections of the introductory course, one of us went to each class as a guest speaker, distributed the surveys, and assisted students in following the directions. After all students finished the post-phishing IQ test survey, they heard a short lecture followed by a discussion of phishing. All three instructors for the four sections later sent

emails to us indicating that the students were very pleased with the experience.

	Agree or Strongly Agree	Disagree or Strongly Disagree
I believe that it is safe to open any email that is not in my junk or spam folder.	6 (14%)	29 (66%)
I am comfortable with using email.	35 (78%)	5 (11%)
I think phishing presents a risk to the security of my computer.	28 (62%)	2 (4%)
I think phishing presents a risk to my personal security.	33 (73%)	2 (4%)
I think that antivirus software will protect me against phishing.	12 (26%)	15 (34%)
I know someone who has been harmed by phishing.	7 (16%)	22 (49%)

Table 1. General Phishing Knowledge

Student profile

Of the 45 students who participated, 24 (53%) were female and 21 (47%) were male, and most ranged in age from 18-26 (56%). Almost all were non-computing majors and a variety of majors were represented, with most students from either nursing (30%) or business (30%). Most were in their sophomore (25%), junior (34%) or senior (25%) year. Most had completed some level of college algebra or calculus (75%). The course they were completing is a typical non-majors survey course of various aspects of computing including history, programming languages, formal logic, and ethical and social issues related to computing.

3. RESULTS

Table 1 shows the student responses to the general phishing knowledge questions asked on the pre-survey. As shown in the table, most had some awareness of the hazards of phishing emails, recognizing them as a threat to personal safety. Table 2 shows the scores reported by students for the Phishing IQ test. The most common scores reported were 70% or 60% (53% combined), with only 2 students reporting a perfect score.

Reported score	N
100 %	2 (5%)
90%	2 (5%)
80%	4 (9%)
70%	13 (30%
60%	10 (23%
50%	5 (11%)
40%	7 (16%)
20%	1 (2%)

Table 2. Phishing IQ Test Scores (self-reported)

Table 3 shows the results of the pre- and post-test questions, *I know what phishing is*, and *I am confident in my ability to detect a phishing email*. T-tests were performed and show that the phishing IQ test significantly affected student's perceived ability and confidence in detecting phishing emails. For the question *I know what phishing is,* the number of students who agreed or strongly agreed went from 16 to 30, with $t(44) = 3.34$, $p < .01$. For the question, *I am confident in my ability to detect a phishing email*, the number of students who agreed or strongly agreed went from 15 to 23, with $t(43) = 2.12$, $p < .05$. Our results indicate that students significantly changed their confidence level in their ability to define what phishing is, and to detect a phishing email.

	I know what phishing is.	I am confident that I can detect a phishing email.

Pre-test Agree or Strongly Agree	16 (35%)	15 (34%)
Pre-test Disagree or Strongly Disagree	13 (29%)	15 (34%)
Post-test Agree or Strongly Agree	30 (68%)	23 (52%)
Post-test Disagree or Strongly Disagree	5 (11%)	5 (11%)

Table 3. **Pre- and Post-test Questions**

The post-test also included a question, *I think that the phishing exercise helped me understand more about how to identify phishing emails*, with the results shown in Table 4, indicating that most students strongly agreed that the phishing IQ test helped them do so.

	I think that the phishing exercise helped me understand more about how to identify phishing emails.
Agree or Strongly Agree	35 (80%)
Disagree or Strongly Disagree	4 (9%)

Table 4. Perceived Usefulness of the Phishing Exercise

4. DISCUSSION

In previous studies, Robila and Ragucci found significant improvement in non-IT major students' ability to identify threats after they took a targeted Phishing IQ test. They found that "if an IQ test is developed using known services that a group of users have a high probability of using, then the element of inexperience with the company/service is eliminated." They successfully used a targeted IQ test to improve student skills at detecting phishing emails. Ninety-four percent of Robila and Ragucci's students agreed the targeted IQ test was helpful to them. (Robila, 2006) Kumaraguru et al hypothesized that users improve their ability to detect phishing emails after they have been deceived by one. Their experimental results "suggest that users are motivated to learn when the training materials are presented after users fall for the phishing emails (when users click on the link in the email). We believe this is because the embedded methodology directly applies the learning-by-doing and immediate feedback principles." This experiment "tested users to determine how well they retained knowledge gained through embedded training and how well they transferred this knowledge to identify other types of phishing emails.... In our experiments, we found that: (a) users learn more effectively when the training materials are presented after users fall for the attack (embedded) than when the same training materials are sent by email (non-embedded); (b) users retain and transfer more knowledge after embedded training than after non-embedded training". (Kumaraguru, 2007) In pedagogical terms, Kumaraguru et al found that reading about how to avoid being phished was ineffective; students need to get hooked by a phishing email or to misinterpret a legitimate email to fully recognize the extent of the problem and actually retain significant anti-phishing savvy.

Anandpara et al conducted a study using a phishing IQ test to show students what they did not know, and then exposed them to existing phishing education. To determine if they learned anything, the students took a new Phishing IQ test. In the second one, "a substantially larger portion of stimuli was indicated as being phishing in the second test, suggesting that the only measurable effect of the phishing education (from the point of view of the phishing IQ test) was an increased concern, not an increased ability." At first glance, it appears that Andapara et al's results contradict those of Robila and Kumaraguru. However, both of their studies used specialized versions of phishing emails, suggesting that the most effective way to use a generic phishing IQ test is to generate

awareness in novices, as a springboard for using existing tools, or to initiate a discussion as part of the security component of an introductory computer course. With respect to Andapara et al, we believe that although we do not want to increase fear of computing in our students, a healthy dose of skepticism and a bit of curiosity can be the first step to a broader yet practical component of security education in a non-major's literacy course.

5. CONCLUSION

Our results show that students felt significantly more prepared to recognize phishing attempts after taking the phishing IQ test. Computer use is ubiquitous in today's society and informed awareness of security issues such as phishing is a valid topic for any course of study. Prior to this study, we had received positive anecdotal comments from students and others regarding the Sonicwall test; the results of this study confirm that it is a valuable educational tool.

Unlike Anandpara et al, we did not subject the students to a second phishing IQ test since in our case, we were primarily interested in the perceived value of the Sonicwall test in particular. Future work could include the addition of a second phishing test to see if we could duplicate those results. Research shows that active learning exercises in general are valuable additions to today's classrooms, (Beck, 2005). Others agree that using this type of activity to raise awareness and knowledge of phishing is a worthwhile activity to add to any computing literacy course. (Werner, 2005)

6. References

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., and Roinestad, H., "Phishing IQ Tests Measure Fear, Not Ability," extended abstract, USEC, 2007.

APWG, Anti-Phishing Workgroup web site, , "Phishing Activity Trends Report Q1 2008", http://www.antiphishing.org/, last accessed October 7, 2008

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

Consumer Reports security website, "State of the Net 2008" http://www.consumerreports.org/security, last accessed October 7, 2008

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

Federal Deposit Insurance Corporation website, "Phishing Scams" http://www.fdic.gov/consumers/consumer/alerts/phishing.html, last accessed October 7, 2008

Frank, Charles and Werner, Laurie. (2007). "Getting A Hook on Phishing", Information Systems Education Journal, 5 (36). http://isedj.org/5/36/. ISSN: 1545-679X.

Jakobsson, Markus and Myers, Stephen, Phishing and Countermeasures, Wiley-Interscience, 2007.

Jakobsson, Markus and Zulfikar Ramzan, Crimeware: Understanding New Attacks and Defenses, Addison-Wesley Professional; 1st edition (April 16, 2008)

Kumaraguru, Ponnurangam, Yong Rhee, Steve Sheng, Sharique Hasan, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong.(2007). "Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer", APWG eCrime Researchers Summit, October, 4-5, Pittsburgh, PA, USA.

Longstaff, Tom, "Evolving Business Models, Threats, and Technologies: A Conversation with CERT's Deputy Director for Technology", www.cert.org/podcast/transcripts/8longstaff.pdf - 2007-10-15

MillerSmile.uk.co web site http://www.millersmiles.co.uk/. 2007, last accessed October 7, 2008

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.

SANS website, "Top-20 2007 Security Risks (2007 Annual Update)," http://www.sans.org/top20/?ref=3706, last accessed October 7, 2008

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 (2008) web site, http://www.sonicwall.com/phishing/, last accessed October 7, 2008

Staff Report by the Federal Trade Commission's Division of Consumer and Business Education and Division of Marketing Practices, "Roundtable Discussion on Phishing Education", July 2008, http://www.ftc.gov/os/2008/07/080714phishingroundtable.pdf, last accessed October 7, 2008

Werner, Laurie. "Redefining Computer Literacy in the Age of Ubiquitous Computing." (2005). Proceedings of the 6th conference on Information technology education, Newark N.J., October 20-22, pp95-99.