Volume 13, No. 5
September 2015
ISSN: 1545-679X

INFORMATION SYSTEMS EDUCATION JOURNAL

In this issue:

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **EDSIG**, the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is six times per year. The first year of publication is 2003.

ISEDJ is published online (http://isedjorg). Our sister publication, the Proceedings of EDSIG (http://www.edsigcon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the 1st Edition of Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org.

2015 AITP Education Special Interest Group (EDSIG) Board of Directors

INFORMATION SYSTEMS
EDUCATION JOURNAL

Why Phishing Works: Project for an Information Security Capstone Course

Lissa Pollacia
lpollaci@ggc.edu

Yan Zong Ding
yding@ggc.edu

Seung Yang
syang2@ggc.edu

Information Technology
Georgia Gwinnett College
Lawrenceville, GA 30043, USA

Abstract

This paper presents a project which was conducted in a capstone course in Information Security. The project focused on conducting research concerning the various aspects of phishing, such as why phishing works and who is more likely to be deceived by phishing. Students were guided through the process of conducting research: finding background and related work on the topic, determining the hypothesis, development of the survey system, data collection, analysis of the results, and writing of the academic paper. This project was very successful in that students gained in-depth knowledge about phishing, developed an understanding of research and academic writing, and learned to statistically analyze data to support or refute their hypothesis. Educators who are teaching a capstone course in Information Security may be interested in this project because it is an appropriate level for undergraduate seniors, it can be accomplished in one semester, and the participants can be other students at the institution.

Keywords: Security Capstone Course, Security Research Project, Phishing, Student Research

1. INTRODUCTION

Many undergraduate programs in Information Security require a capstone course at the senior-level. This paper describes a project that is appropriate for a capstone course in information security. The authors conducted this project in the capstone course for three semesters. It was successful in achieving the following goals for students in the course: (1) develop a deeper understanding of one area of information security, (2) learn how to conduct research in the computing field, and (3) learn how to write an academic paper.

The project focuses on *phishing*, a type of attack in which attackers use spoofed (phishing) email to deceive users and motivate them to visit and reveal confidential information at fraudulent (phishing) websites. These websites are designed to closely mimic and impersonate real, legitimate sites. Each year phishing attacks succeed in scamming millions of users and stealing billions of dollars from the victims (Hong, 2012). The purpose of the project was to answer questions such as "why phishing works?" and "who is more likely to fall for phishing?"

The project was conducted for three semesters and was successful from both practical and pedagogical viewpoints. The project had sufficient depth and provided challenging material for the students; however it could be completed in one semester. In addition, the study was structured so that there are no consequences to the study participants, thus the project was readily approved by our Human Subjects Board (HSB).

The project also supports the push in STEM education to provide more opportunities for *Scientific Inquiry* (Yager, 2009; Zubrowski, 2009). The National Research Council (NRC) defines Scientific Inquiry to be activities in which learners study a question, formulate hypotheses, collect and evaluate evidence, and then communicate and justify their conclusions (NCR, 2006). Many scientific educators believe that scientific inquiry is critical to helping students develop 21st-century skills and knowledge that are needed to be successful today (Rhoton, 2010).

2. RELATED WORK

The past decade saw a great deal of research activities in the area of phishing. See the excellent survey of Hong (2012) for the state of phishing.

Dhamija et al. (2006) conducted the first published study of phishing. In the study, each participant was shown 20 websites, some real and some fake, and was asked to determine whether each given site was legitimate or fraudulent. For sites that they determined to be fraudulent, the participants were also asked to give their reasons for their decisions. The study found that well designed phishing sites fooled over 90% of the participants. Many participants did not verify the correctness of the sites' URLs or were not able to distinguish between legitimate and fraudulent URLs. Even fewer understood the SSL security indicators, such as "HTTPS" in the URL, the padlock icon, and the certificate. Many participants incorrectly based their decisions on how professional the content of the viewed web pages look, failing to understand that the content of a web page can be easily copied. Moreover, visual deception attacks successfully fooled even the most experienced participants. Examples of visual deception include using visually deceptive text in closely mimicked URLs (e.g. using the number "1" in place of the letter "l", or using two "v"s for a "w"), hiding a hyperlink to a rogue site inside an image of a legitimate hyperlink, and using an image of a real site in the content of a phishing page. Following the work of Dhamija et al. many other researchers led similar studies which show that the findings of Dhamija et al. continue to hold and users remain vulnerable to phishing (Hong, 2012).

Downs et al. (2006) conducted the first study of phishing email messages (as opposed to phishing websites) and how users respond to them. Just as in the case of judging websites (Dhamija et al., 2006), the study of Downs et al. found that users often base their judgments of email messages on incorrect heuristics. Users fall particularly for spear phishing, which involves email messages sent to a specifically targeted group, such as members of a community, employees of an organization, or customers of a business. For example, users who have an account at a company would tend to trust email messages that appear to be sent from the company, and many think that since the company already had their information, it would be safe to give it again. The findings of Downs et al. were confirmed in the work of Jagatic et al. (2007), which showed that people were 4.5 times more likely to fall for social phishing, i.e. phishing email sent from an existing contact, than standard phishing attacks, and it is for this reason that criminals heavily target online social networking sites. Moreover, social phishing was more successful when the phishing email messages appeared to be from a person of the opposite gender.

Dodge et al. (2007) performed a study of the effectiveness of phishing at the United States Military Academy (USMA West Point) over a period of two years. The participants of the study were the entire student body of USMA. Over time the authors developed a system that periodically generates phishing email messages, sends the messages to students, and tracks the students' responses to these messages. The study showed a failure rate of approximately 40%, that is, about 40% of the spoofed messages that appeared to be sent from an administrative office within USMA resulted in a student clicking an embedded link in the message and disclosing confidential information to unauthorized users, or opening attachments that could potentially contain malicious code.

Sheng et al. (2010) conducted the first large-scale study of demographic factors in susceptibility to phishing. They found that women were more susceptible to phishing than men, likely because women appeared to have less exposure to technical knowledge and training than men. They also found that young participants of ages 18 to 25 were more susceptible to phishing than other age groups, possibly because that they had less experience and less exposure to education and training in computer security. In the meantime, the authors found that good educational materials reduced participants' chance of falling for phishing by 40%.

Since lack of knowledge is the primary reason why users fall for phishing, many researchers studied the effects of education and training in helping users prevent phishing (Kumaraguru et al., 2007; Sheng et al., 2007; Kumaraguru et al., 2009; Kumaraguru et al., 2010). Kumaraguru et al. found that simply emailing anti-phishing materials to users is ineffective, as people are used to receiving and ignoring such warning (Kumaraguru et al., 2007). They found that users learn more effectively in embedded training, where users are presented training materials after they fall for an attack. Kumaraguru et al. developed an embedded training system called PhishGuru (Kumaraguru et al., 2009; Kumaraguru et al., 2010). PhishGuru periodically sends simulated phishing email messages to users in training, and when users fall for such a message, they receive an intervention email message that explains to them that they are at risk for phishing attacks and teaches them how to protect themselves against phishing. Study showed that with this approach, participants' chance of falling for phishing reduced by 45%, even one month after the training. Sheng et al. developed an educational game called Anti-Phishing Phil that teaches users basic security concepts related to phishing, and then tests users on what they learned (Sheng et al., 2007; Kumaraguru et al., 2010). Studies showed that this approach improved novices' ability to identify phishing by 61%.

Our information security capstone project was very similar in nature to and draws from the methodologies of the above-mentioned studies on phishing. The main difference is that those studies were conducted by professional researchers, whereas our project was for undergraduate seniors in a capstone course. We are not aware of published scholar articles on capstone courses in information security. However, there is a wealth of literature on capstone courses in IT or IS related disciplines. All those articles show that capstone projects benefit students and add values to a program of study. For instance, Dunlap (2005) shows, based on the analysis of student's outcomes in a software engineering capstone course, that capstone projects promote problem-based learning which enhances students' self-efficacy in learning and problem solving. Such self-efficacy is crucial for remaining competitive in computing related fields that are constantly and rapidly evolving. Gupta & Wachter (1998) and Lesko (2009) show that capstone projects bolster critical thinking and stimulates students' creativity to integrate various concepts and skills, apply the integrated skills to solve problems, and acquire practical knowledge. Our capstone experience confirms all these findings.

There is also literature on methods to deliver capstone courses. Lynch et al. (2004) define four models of delivery. The first is the industry-sponsored model, where students play the role of early career employees within a company. The second is the studio model, where students collaborate with experts and mentors. The deliverables are defined, but their content is flexible. The third is the traditional model, where students collaborate in teams. The deliverables are defined, but there is little interaction with and support from the faculty. The fourth is the directed model, where students form small groups and work closely with the faculty. The groups are provided with a clearly defined set of requirements, milestones and deliverables. The directed model is the model we adopted to deliver our capstone course.

3. THE PROJECT

This section describes the capstone project and how it was organized and implemented. The course was Information Technology (ITEC) 4810, Systems and Security Capstone. The authors taught the course in Spring 2012, Fall 2012, and Spring 2013. The work was self-contained, i.e., the work completed in one semester. The authors were assigned to team-teach the course.

Students were divided into groups of three. We found that three students per group worked better than four per group, because with a smaller group size each student had a sufficient amount of responsibility. The purpose of the project was to research various aspects of *phishing*, using students on our campus as participants. The research attempted to answer questions such as "Do people recognize certain indicators of phishing?" and "Which participants are more likely to fall for phishing?" Students in the class were able to choose their own questions and generate hypotheses, which were then tested using data collected by a web-based survey system (which they also developed).

We delivered the capstone course using the *Directed Method* as defined by Lynch et al. (2004). We not only defined the project, but also organized the project into components and subcomponents, and set a timeline of milestones and deliverables. For each subcomponent we covered the background and tools that the students needed to complete the deliverables on time. We chose to adopt this method of delivery because the students had never been involved in this type of project before.

On the other hand, good planning and organization by the instructors and proper guidance to the students would make the project more accessible and manageable. There are two major components of the project that run concurrently throughout the semester. One was the "research" component of the project, in which students conducted the research, collected the data, analyzed the data, and wrote a paper about the project and the results. The second component was the "development" side, which consisted of developing the web-based survey system. The survey system was used to collect the data and test the hypotheses. The research component is discussed below in this section, and the development component is discussed in Section 4.

The research component of the project requires that the students:

(1) Acquire fundamental knowledge of phishing

(2) Conduct library research into the current phishing literature

(3) Determine one or more hypotheses

(4) Create web pages and email messages, and develop survey questions

(5) Statistically analyze the data

(6) Interpret the results of the analysis and write the academic paper

Acquire fundamental knowledge of phishing
The students in the capstone course were primarily seniors in the Systems and Security concentration, and therefore had some fundamental knowledge of phishing. However, to immerse them into the topic, we required the students to read three in-depth articles about phishing: (1) "Why phishing works" (Dhamija et al., 2006); (2) "You've been warned: An empirical study of the effectiveness of Web browser warnings" (Egelman et al., 2008); and (3) "The State of Phishing Attacks" (Hong, 2012). We assigned discussion questions and created discussion forums on these articles in the online learning management system. The students were required to participate in these online discussions, as well as in-class discussions.

Conduct library research into current phishing literature
We contacted the library staff at our institution, who taught a short course on conducting research using our library resources. Although most of the students had been through a similar presentation in the past, they indicated that it was helpful to have a review of these research skills, particularly with respect to the current topic.

Each group was given the assignment to find at least three additional papers related to phishing. After reading these papers, they were required to write the "Background and Related Work" section of their own paper and give an oral presentation in class. The presentations not only gave students experience in public speaking, but also increased their breadth of knowledge concerning phishing.

Determine the hypotheses
Each student in the group was required to develop at least one research question and hypothesis. Therefore, each group would research at least three hypotheses. Some examples of hypotheses are:

- Male participants are able to identify phishing attempts better than female participants.
- Information Technology majors will be more likely to identify phishing attempts than non-IT majors.
- Phishing email is more effective if it contains familiar content or comes from a source that participants recognize.
- Over 50% of participants will be unable

to identify a phishing site when the URL is the only indicator.

- Users with training are less susceptible to phishing than those without training.

Students queried the database containing data collected by the survey system, and then tested all these hypotheses by performing statistical analysis. In order to help students test the last hypothesis on the above list, we did a simple control study. That is, we selected a small control group of participants, and gave a short training session on phishing basics before the control group participated in the study. The data for the control group and that for other participants are stored separately. It may be interesting to note that of the list of sample hypotheses given above, the first one (male vs. female) was refuted, while all the others were confirmed in the study.

Create web pages and email messages, and develop survey questions

Once the hypotheses were developed, then the groups were required to create web pages and email messages, some of which were legitimate and some of which were phishing attempts. These were to be presented to the survey participants as images of the web pages and email messages. Due to restrictions placed by our institution's Human Subjects Board (HSB), the participants would not interact directly with a live phishing site or a live phishing email message, but rather with static images of the phishing site or messages. The survey questions from all of the groups were collected and organized into one cohesive survey.

When participants entered the survey, they first viewed and accepted the Informed Consent information, which was required by the HSB. Next came a demographics form, which collected demographic data such as sex, age, major, class level, etc. that was needed to analyze the hypotheses. This was followed by 10 to 12 screens, which displayed the images of real or phishing web pages and email messages. For every image, the participant was asked to identify whether this was legitimate or fake (phishing). We used a 4-point Likert scale: Strongly Agree, Agree, Disagree, and Strongly Disagree. We did not include the neutral option (Neither Agree nor Disagree), as we wanted the participant to choose one way or the other. Appendix 1 shows an example of an image and survey question presented to participants. This is an example of a phishing site which mimics the site of Fidelity Investments (note the misspelling of the word "fidelity" in the URL.)

Those who identified this screen as a phishing attempt, were asked a follow-up question to further identify which indicator led them to this conclusion. Indicators included bogus URLs, lack of a padlock, strike-through of https, and errors in the content of the page or message. This gives more detail concerning what "gave away" the image as a phishing site or email. Appendix 2 shows the follow-up image and question to the image shown in Appendix 1. Note the boxes surrounding such areas as the URL, the menu, the logo, and the content.

Creating images of phishing sites

Creating images of phishing sites was the component that students enjoyed the most. Making an image of a real site is relatively easy – one simply visits the site and takes a screenshot. A vast majority (about 80%) of the images used in the survey were images of phishing sites, and we encouraged students to be as creative as possible in creating those. However, developing a realistic phishing image is non-trivial. Simple approaches such as using photo-editing software to modify the image of a real site do not work, as they do not produce realistic looking images. The best approach was for the student to create a phishing site first, then take an image of that. We demonstrated a few tools for constructing phishing sites. For instance, we introduced a web crawler known as HTTrack that allows one to copy the content of an entire website to a local computer and based on that come up with a site that mimics the original site.

The students installed and configured a DNS server to establish a phishing site with a desired domain name. Then they set up a web server with HTTPS and created a privately signed certificate. Next they copied the mimicked legitimate web site contents using HTTrack and modified the source code to create the desired content for the phishing site. The students also installed an SMTP (sendmail) server and created phishing email messages.

Ethics

During this part of the course we repeatedly emphasized professional ethics. We reiterated that these tools were introduced in order to complete their project and to better understand phishing attacks. We emphasized that any attempt to use those tools to launch phishing attacks is considered criminal behavior. These students are in the Systems and Security concentration of our ITEC major, therefore it is important that they thoroughly understand the professional ethics involved. All students understood this and took it seriously.

Statistically analyze the data

The students in the Systems and Security concentration are required to take a statistics course, and therefore have some statistical foundation. However, the statistics course is at the sophomore level, and the students in the capstone course are mostly seniors. Therefore, a short review of hypothesis testing was needed (approximately one week of classes).

We chose to model the responses in the binomial form by summing Strongly Agree/Agree and Strongly Disagree/Disagree responses separately. Students analyzed the data based on the following steps for hypothesis testing:

Step 1. Develop the null and alternative hypotheses
Step 2. Specify α
Step 3. Decide if the test is one-tail or two-tail
Step 4. Choose the formula and calculate the test statistic
Step 5. Compute the p-value
Step 6. If p-value ≤ α, then reject Ho and fail to accept Ha; otherwise accept Ho

The groups were required to turn in a document containing a formal statement of their hypotheses, along with the statistical analysis, which they had conducted. This document would become the next section of their written paper.

For example, one group had a hypothesis which states that most (i.e. over 50%) of users will be unable to identify a phishing site when the URL is the only indicator of phishing. Formally, the alternative hypothesis Ha and null hypothesis Ho are given as follows:

- Ha: More than 50% of attempts will fail to identify phishing websites that have fraudulent URLs as the only indicator of phishing.
- Ho: Less than or equal to 50% of attempts will fail to identify phishing websites that have fraudulent URLs as the only indicator of phishing.

All of the groups together had developed four phishing pages that have fraudulent URLs as the only indicator of phishing. Therefore, participants' answers to the survey questions for these four images allowed this group to test the hypothesis. Answers that chose "strongly agree" or "agree" are considered correct, and answers that chose "disagree" or "strongly disagree" are considered incorrect. This is obviously a one-tail test. The group set α to be 0.05. Applying the correct formulas to the survey data, the group computed a t-value, and then computed a p-value using the Microsoft Excel TDIST function. The resulting p-value is tiny and significantly less than α. Therefore, with a confidence level of 95%, the group rejected the null hypothesis and concluded that most people would fail to identify phishing websites when the URL is the only indicator for phishing. Appendix 3 shows the summary of the group's statistical test for this hypothesis.

Interpret the results of the analysis and write the academic paper

For this component of the project, we followed these characteristics of Scientific Inquiry, as defined by the National Research Council (NRC):

- Learners formulate explanations from evidence to address scientifically oriented questions.
- Learners evaluate their explanations in light of alternative explanations.
- Learners communicate and justify their proposed explanations.

For this section of their academic paper, students were asked to explain what the statistical evidence had shown. This was accomplished by having group meetings, meetings of group members and faculty members, and also general class discussion. We found students in other groups could be quite helpful in discussing and offering explanations.

As previously stated, two purposes of the course are to engage students in scientific inquiry and to learn how to write an academic paper. By the time we reached this point in the semester, most sections of the paper were already written. Essentially, all that remained was the results of the analysis and the conclusions. The advantages of this approach are two-fold: (1) We were able to review sections of the paper and make suggestions/corrections as the project unfolded, and (2) students were not overwhelmed by the task of writing an entire paper at the end of the semester.

Each group gave an oral presentation at the end of the semester, which supports the NRC goal of communicating and justifying their proposed explanations.

4. TECHNICAL DEVELOPMENT OF THE SURVEY SYSTEM

The survey system was developed using LAMP (Linux, Apache 2.2.3 web server, MySQL 5.0 database, and PHP 5.1.6 in CentOS 5.3). This platform was chosen because it is a popular platform for website development and has a large supporting community.

The development process was divided into four tasks: database development, web page development, phishing image development, and creation of a survey system, including OS and software installation. The survey system development tasks were assigned to two development groups: a database development group and a web development group. The database development group designed the database schema and ported the web page and email images into the database. The web development group installed LAMP software and created web pages for the survey. The survey system development time was tight, so we used the Rapid Application Development (RAD) model to minimize planning time and get a working system as soon as possible. Using RAD, revisions of the system occur as it is being developed.

The database development group created a database schema to store the survey questions and the data that would be collected. The major challenge faced by the group was to design a logical data model with many unknown factors and implementing it within a very short period of time. The logical data model had to support various survey types, which were unknown at the time of its design. The survey system needed to be ready by approximately two-thirds into the semester so that the students could test their survey questions with phishing images before the system was released to participants.

As shown in Appendix 4, the group tried to make the database schema as simple as possible but also general enough to support various types of survey questions. The group created the initial conceptual model using E-R diagrams with justifications. They collected feedback from the other students and revised the design as needed. Then the group normalized the database, and developed the physical design of the database structure with MySQL. The group worked together with other students to put the survey questions and images into the database, then to test and debug the survey system.

Designing the reusable survey web pages was one of the key challenges for the web page development group. The web pages are designed to support different types of survey questions with minimal effort. To this end, the web pages were categorized into start and end pages, main question pages, follow-up question pages, and survey result report pages.

The start and end pages consisted of the informed consent form and an end-of-survey thank-you page. To each survey instance, the start page associated a session ID that was used to identify the instance. By utilizing the session IDs, the survey did not need to collect personal information from participants, but was still able to uniquely identify each survey instance.

The main question pages loaded question statements and a related image from the database using an internal question number. Then it recorded the participant's answer in the database. The same web page source code was reused by changing the question number until all of the main questions were given to the participant. The follow-up question pages also used the same source code, but were only displayed when a participant indicated that the image from the main question page was a phishing site or email image. Appendix 5 illustrates how the types of pages were used in the process flows.

The initial version of the survey system was developed in Spring 2012. The system was further enhanced by students in subsequent semesters.

5. CONCLUSIONS

This paper describes the project in an Information Security capstone course that the authors jointly taught in three separate semesters. The course was delivered using the directed method (Lynch et al., 2004), where milestones and deliverables are clearly defined and students are provided with necessary background and tools to complete the deliverables on time. The capstone project was very successful in that we were able to achieve the objectives: (1) students will develop a deeper understanding of one area of information security, (2) learn how to conduct research in the computing field, and (3) learn how to write an academic paper. Under proper organization and guidance, the students were able to complete a research project that was previously conducted by reputable professional researchers. The components of the capstone project reinforced and integrated skills in information security, networking, systems analysis and design, database design and implementation, web development, software development and testing, and statistics. The project was accomplished in one semester with very little additional resources other than the authors' expertise.

Additional experience with "soft skills" also occurred as a result of this project. Students learned to communicate and work with various groups, each having different responsibilities, and to coordinate their efforts. They were also responsible for contacting other instructors at our institution to solicit participants to take the survey. This was excellent experience for the workplace environment in which strong communication and teamwork skills are highly valued.

6. REFERENCES

Dhamija, R., Tygar, J.D., & Hearst, M. (2006). Why phishing works. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 581-590.

Dodge, R.C., Carver C., & Ferguson, A.J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73-80.

Downs, J.S., Holbook, M.B., & Cranor, L.F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the SOUPS Symposium on Usable Privacy and Security*, 79-90.

Dunlap, J. C. (2005). Problem-based learning and self-efficacy: How a capstone course prepares students for a profession. *Educational Technology Research and Development*, 53(1), 65-83.

Egelman, S., Cranor, L.F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of Web browser warnings. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1065-1074.

Gupta, J. N. D., & Wachter, R. M. (1998). A capstone course in the information systems curriculum. *International Journal of Information Management*, 18(6), 427-441.

Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM*, 55(1), 74-81.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94-100.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L.F., Hong, J., Blair, M.A., & Pham, T. (2009). School of phish: a real-world evaluations of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security*, 1-12.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., & Acquisti, A. (2007). Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. *Proceedings of the Anti-Phishing Working Group's Second Annual eCrime Researchers Summit*, 70-81.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., & Hong, J. (2010). Teach Johnny Not to Fall Phish. *ACM Transaction on Internet Technology*, 10(2), 1-31.

Lesko, C. J. (2009). Building a framework for the senior capstone experience in an information computer technology program. In *Proceedings of the 10th ACM conference on SIG-information Technology Education*, 245-251.

Lynch, K., Goold, A., & Blain, J. (2004). Students' pedagogical preferences in the delivery of IT capstone courses. *InSITE 2004 Informing Science and IT Education Joint Conference*, 431-442.

National Research Council (2000). Inquiry and the national science education standards: A guide for teaching and learning. Washington D.C.: National Academy Press.

National Research Council (2006). How Students Learn: History, mathematics and science in the classroom. Washington D.C.: National Academy Press.

Rhoton, Jack (2010). Science Education Leadership: Best practices for the new century.

Sheng, S., Holbrook, M.B., Kumaraguru, P., Cranor, L.F., & Downs, J.S. (2010). Who falls for phish? A demographic study of phishing susceptibility and effectiveness of interventions. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 373-382.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the Third Symposium on Usable Privacy and Security*, 88-99.

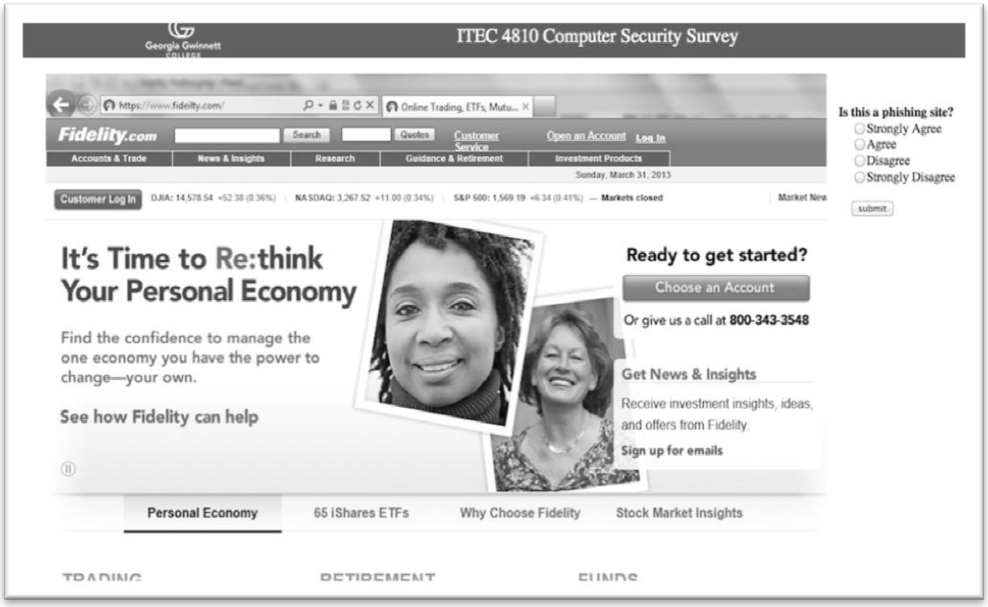
Smithenry, Dennis W. and Gallagher-Bolos Joan A. (2009). Whole-Class Inquiry: Creating student-centered science communities. Arlington, VA: National Science Teachers Association: NSTA Press.

Yager, Robert E. ed. (2009). Inquiry: The Key to Exemplary Science. Arlington, VA: National Science Teachers Association: NSTA Press.

Zubrowski, Bernard (2009). Exploration and the Meaning Making in the learning of science: Innovations in Science Education and Technology Series. Breinigsville, PA: Springer.

Appendices

Appendix 1. Sample Survey Image



ITEC 4810 Computer Security Survey

Is this a phishing site?

○ Strongly Agree
○ Agree
○ Disagree
○ Strongly Disagree

It's Time to Re:think Your Personal Economy

Find the confidence to manage the one economy you have the power to change—your own.

See how Fidelity can help

Ready to get started?

Or give us a call at 800-343-3548

Get News & Insights

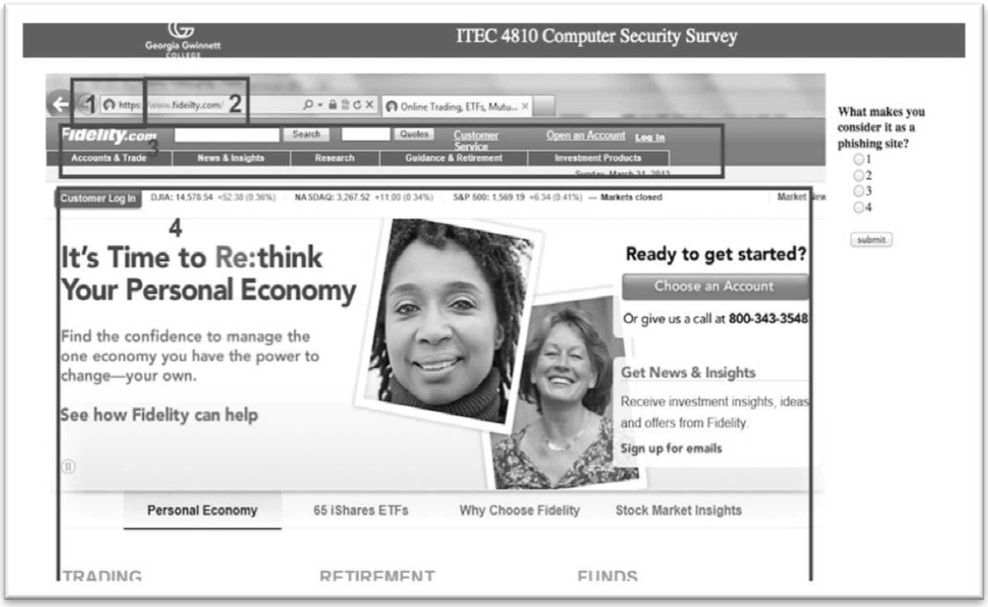
Receive investment insights, ideas, and offers from Fidelity.

Sign up for emails

DJIA: 14,578.54 +52.38 (0.36%) | NASDAQ: 3,267.52 +11.00 (0.34%) | S&P 500: 1,569.19 +6.34 (0.41%) — Markets closed

Sunday, March 31, 2013

Appendix 2. Follow-up Question



ITEC 4810 Computer Security Survey

What makes you consider it as a phishing site?

○ 1
○ 2
○ 3
○ 4

It's Time to Re:think Your Personal Economy

Find the confidence to manage the one economy you have the power to change—your own.

See how Fidelity can help

Ready to get started?

Or give us a call at 800-343-3548

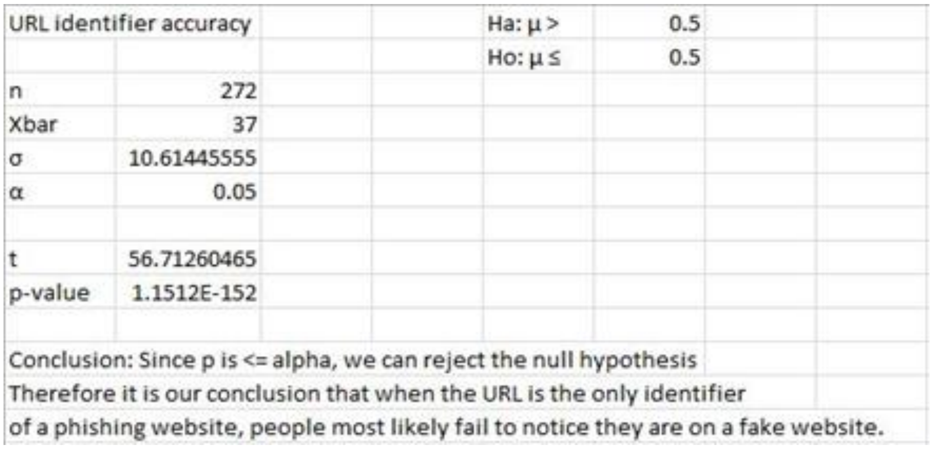
Get News & Insights

Receive investment insights, ideas and offers from Fidelity.

Sign up for emails

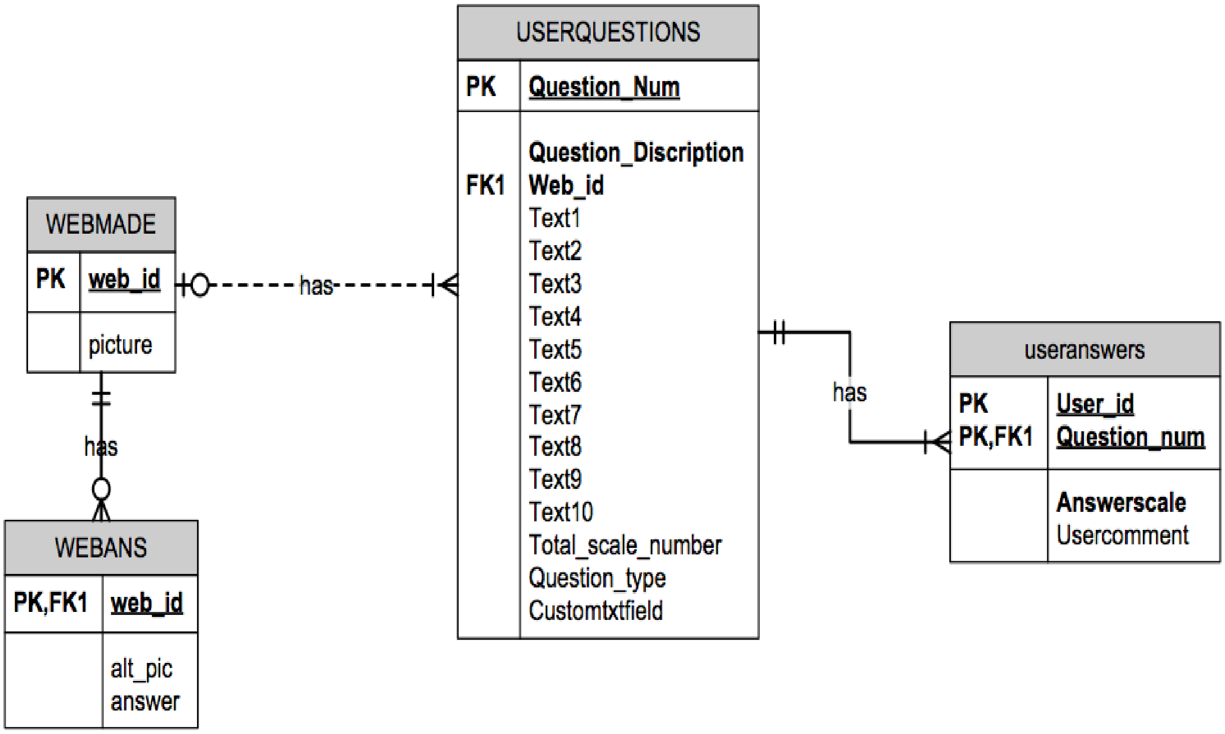
DJIA: 14,578.54 +52.38 (0.36%) | NASDAQ: 3,267.52 +11.00 (0.34%) | S&P 500: 1,569.19 +6.34 (0.41%) — Markets closed

Appendix 1. Sample hypothesis testing by a group

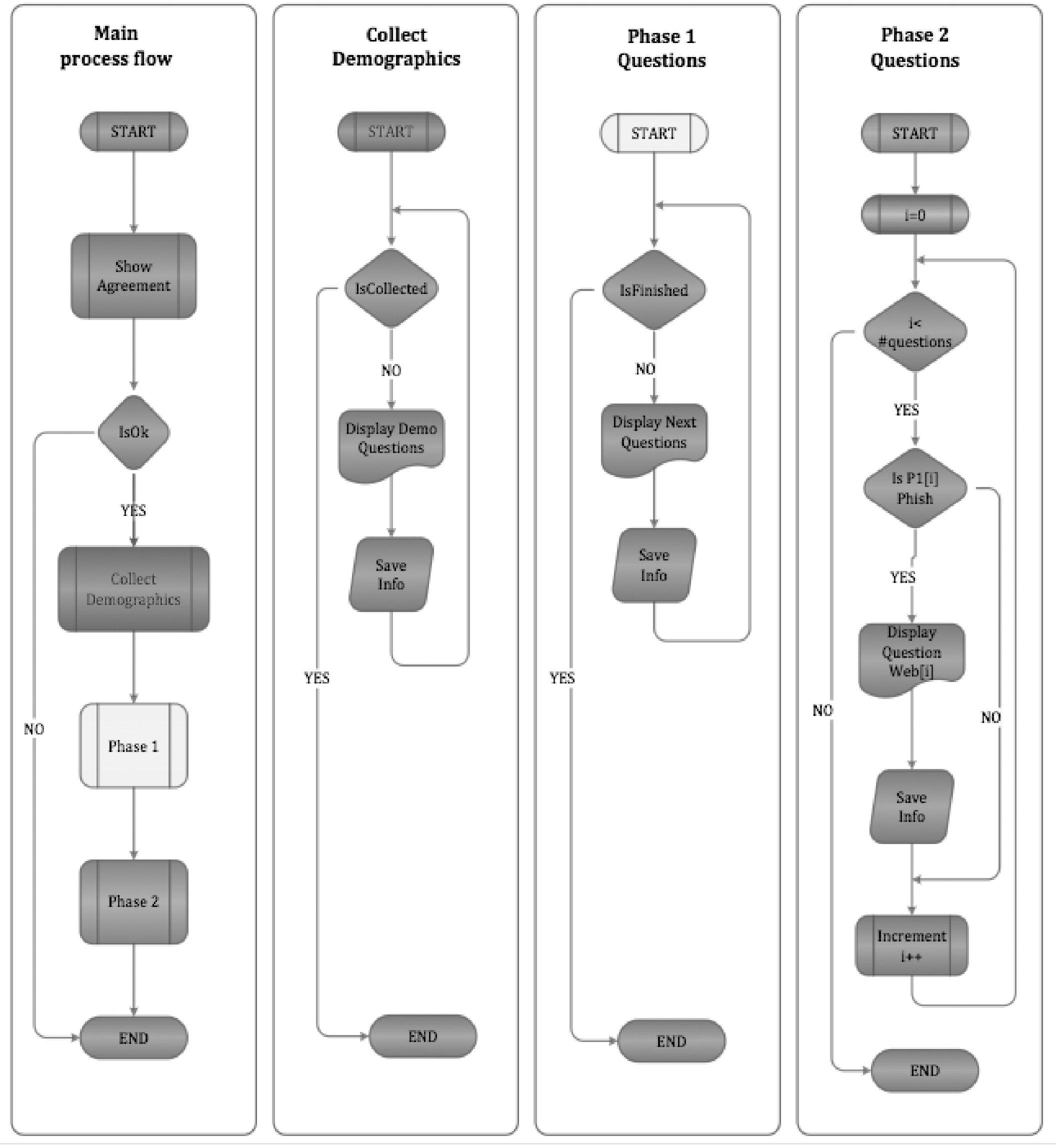


URL identifier accuracy			Ha: μ >	0.5
			Ho: μ ≤	0.5
n	272			
Xbar	37			
σ	10.61445555			
α	0.05			
t	56.71260465			
p-value	1.1512E-152			
Conclusion: Since p is <= alpha, we can reject the null hypothesis				
Therefore it is our conclusion that when the URL is the only identifier				
of a phishing website, people most likely fail to notice they are on a fake website.				

Appendix 4. E-R Diagram for the Survey System Database



Appendix 5


Main process flow
START
Show Agreement
IsOk
YES
NO
Collect Demographics
Phase 1
Phase 2
END
Collect Demographics
START
IsCollected
NO
YES
Display Demo Questions
Save Info
END
Phase 1 Questions
START
IsFinished
NO
YES
Display Next Questions
Save Info
END
Phase 2 Questions
START
i=0
i< #questions
YES
NO
Is P1[i] Phish
YES
NO
Display Question Web[i]
Save Info
Increment i++
END