PHISHING FOR UNDERGRADUATE STUDENTS

Carl J. Case, Ph.D.
St. Bonaventure University
ccase@sbu.edu

Darwin L. King, CPA
St. Bonaventure University
dking@sbu.edu

ABSTRACT

Electronic phishing attempts have grown to unprecedented levels. Phishing can result in identity-theft and can clog email servers. Because educators have a vested interest in student electronic behavior, this study was conducted to empirically investigate the incidence of undergraduate phishing attacks. Survey data was collected each semester during a three-consecutive semester period. Results suggest that student phishing problems are minimal. Only 26% of respondents indicated receiving phishing email. Of those individuals, merely 16 phishes were received per month. In addition, 97% of undergraduates ignored the phishing email and did not respond to any phishing requests during the previous year.

Keywords: phishing, electronic mail, empirical study, undergraduates, survey

INTRODUCTION

According to the Federal Trade Commission, the number of fraud-related complaints received annually has increased by 24% from a level of 542,378 in 2003 to 674,354 in 2006 (Reilly and Swanson, 2004; FTC, 2007). The most common complaint is that of identity theft. In 2002, there were 161,896 identity theft complaints (Konrad, 2005). By the end of 2006, there were 246,035 complaints. This accounted for 36% of all fraud-related complaints received by the FCC and has been the most common complaint filed for seven-consecutive years. The second most common complaint is shop-at-home/catalog sales-related, which is only 7% of all complaints. It is feared, however, that most crimes go unreported and that there were 8.4 million victims of identity theft in 2006 (Monahan, 2007). Identify theft may come as a result of supervisors who steal their employees' identities (Mehta, 2006). Or, a more insidious method is through the use of phishing. Javelin Strategy & Research estimates that 1.7% of identity theft is a result of phishing attempts (Epstein, 2005).

Phishing can be described as an electronic attempt to fraudulently acquire sensitive information such as usernames, passwords, and credit card data by masquerading as a trusted entity in an electronic communication (Wikipedia, 2007). Phishing scams began in the mid-1990s as a method of gaining free Internet access (Fisher, 2005). The success of online banking and bill paying of 2003 marked the beginning of the type of phishing activity that is seen today. As a result, the Anti-Phishing Working Group, a consortium of security vendors, banks, and other concerned parties began recording unique phishing attacks.

Although this history of modern phishing has been brief, it has been dramatic. The Anti-Phishing Working Group reports that there were only 198 unique phishing sites at the start of 2004. But, there were 457 by September of 2004, 5,200 by September of 2006, and 14,191 by September of 2006 (Toland, 2005; Gibbs, 2005; Keizer, 2006). This is an increase of over 7,000% in two and one-half years. There has also been a noteworthy increase in the number of brands hijacked. In October of 2004, there were 46 brands spoofed (Fisher, 2005). By July 2006, there were 154 brands hijacked. The result, according to Gartner, is that between May 2004 and May 2005, roughly 1.2 million U.S. computer users suffered phishing losses valued at $929 million (Kerstein, 2005).

Vendors have made efforts to combat the problem. During the second half of 2006, the Symantec Probe Network detected 166,248 unique phishing messages (a 6% increase from the first half of the year) and blocked over 1.5 billion phishing messages (Turner, 2007). In other words, 8.48 million phishing messages were blocked each day.

Consumer reaction to phishing is varied. In a 2005 study, 55% of respondents stated that he/she would delete a suspicious electronic mail that asked for security reasons to click on a link, log into their account, or enter personal information (Epstein, 2005). Twenty-nine percent would call or otherwise contact their bank to determine if the electronic mail message is legitimate. Twenty-eight percent would report the electronic mail message to their bank. Ten percent indicated that they would click on the link but not enter personal information with the belief that they are safe. And, three percent would comply with the electronic mail message instructions.

Information systems faculty are entrusted with developing and promoting professional computing behavior. Of interest to educators, therefore, is whether our undergraduates are prone to phishing electronic mail and if so, do they respond in an appropriate manner when an attack occurs. Because little empirical evidence is available, this study investigated student behavior with regard to electronic mail usage and phishing incidence.

RESEARCH DESIGN

This study employs a survey research design. The research was conducted at a private, northeastern U.S. university. A Student Electronic Mail instrument was developed by the authors and administered to undergraduate students enrolled in a School of Business course. The courses included a variety of subjects such as BIS-310 “Business Information Systems”, BIS 320 “Business Telecommunications”, ACCT-202 “Introduction to Managerial Accounting”, MSC-301 “Management and Organization Behavior”, and MSC-413 “Business Policy.” A convenience sample of class sections and faculty members was selected. The surveys were collected each semester during a three-consecutive semester period (from Spring 2006 until Spring 2007).

The survey instrument was utilized to collect student demographic data such as academic class, major, and gender. In addition, the survey examined student electronic mail behavior. Students were asked to estimate the number of various types of electronic mail messages they received each week.

All surveys were anonymous and completed in an academic classroom. The response rate was 100 percent. Students were also informed that results would have no effect on their semester grade.

Survey responses were converted into a computer-based database management system to improve the ease of tabulation. A program was written to summarize and filter data.

RESULTS

A sample of 585 usable surveys was obtained. Table 1 indicates that 370 (63%) of the respondents were male and 215 (37%) were female.

TABLE 1
Response Rate By Gender

	Percentage	Count
Male	63%	370
Female	37%	215
Total	100%	585

Table 2 illustrates respondent academic major. The students who participated included accounting majors (27%), marketing majors (22%), management science majors (19%), finance majors (9%), business information system majors (3%), undecided business majors (12%), and other non-business majors (8%).

TABLE 2
Response Rate By Major

Major	Percentage	Count
Accounting	27%	156
Marketing	22%	130
Management Science	19%	109
Finance	9%	53
Business Information Systems	3%	18
Undecided Business	12%	69
Non-business (other)	8%	37

The response rate by academic class is relatively equally distributed. Table 3 illustrates that 22% of respondents were freshmen, 23% were sophomores, 26% were juniors, and 29% were seniors.

TABLE 3
Response Rate By Academic Class

Class	Percentage	Count
Freshmen	22%	130
Sophomore	23%	137
Junior	26%	150
Senior	29%	168

Responses were first examined with regard to type and quantity of electronic mail received per month (Table 4). Results indicate that 20% (45 messages) of electronic mail received per month is class-related messages. In addition, 12% (26 messages) are non-class-related from friends and family. Moreover, 46% (100 messages) of electronic mail received is spam. Finally, 22% (49 messages) of electronic mail is “other mail” such as from notice boards, campus clubs, and so on. Overall, each student reported receiving an average of 220 electronic mail messages per month.

TABLE 4
Messages Received by Type Per Month

Type	Average # of Messages Per Month	Percent of Total Messages
Class-related	45	20%
Friends or family	26	12%
Spam	100	46%
Other (notice boards, campus clubs, etc.)	49	22%
Overall	220	100%

Table 5 examines the type and volume of phishing electronic mail received. In terms of volume, the most prevalent type of attack was with regard to credit cards. Respondents indicated receiving 8.8 electronic mails per month phishing for credit card data. Undergraduates also indicated receiving 7.2 Nigerian scam phishes, 6.6 Amazon.com phishes, 6.2 eBay phishes, and 7.8 other phishes per month. Other phishes included PayPal, loan payoff, bank accounts, myspace.com, and car loans. In terms of percent of respondents, 19% indicated received credit card phishes, 14% eBay phishes, 12% Amazon.com phishes, 9% Nigerian scam phishes, and 3% other phishes. Overall, only 26% of respondents reported receiving at least one phish per month. The average quantity of phishing electronic mail received per month was 16.4 messages. This accounts for 7.5% of the total electronic mail received by undergraduates per month.

TABLE 5
Response to Phishing Electronic Mail

Type of Phishing Request	Number of Electronic Mail Messages Per Month	Percent of Students
Credit Cards	8.8	19%
eBay	6.2	14%
Amazon.com	6.6	12%
Nigerian scam	7.2	9%
Other	7.8	3%
Overall Average	16.4	26%

Finally, undergraduates were asked if they responded to at least one phishing electronic mail in the past year. Only 3% indicated responding to a phish while 97% indicated not responding.

TABLE 6
Response to Phishing Electronic Mail

	Yes	No
I responded to at least one phishing electronic mail during the past year	3%	97%

CONCLUSIONS AND FUTURE RESEARCH

Results indicate that students receive a considerable number of electronic mail messages per month. On average, students get 220 messages per month, or 7-8 per day, in their inbox. The vast majority, approximately 46%, are spam messages. Twenty-percent are class-related, 26% are from friends or family, and 49% are from other sources such as clubs and notice boards.

Relative to phishing, the largest percentage of students received credit card information requests. Nineteen percent of respondents indicated receiving credit card phishes. Fourteen percent received eBay phishes, 12% received Amazon.com phishes, 9% received Nigerian scam phishes, and 3% received other phishes such as PayPal and myspace.com. In terms of volume, the most common type of phish was credit card-related. Undergraduates reported receiving 8.8 per month. Other types included 7.8 other phishes (such as PayPal), 7.2 Nigerian Scam phishes, 6.6 Amazon.com phishes, and 6.2 eBay phishes.

Student response to phishing electronic mail was strongly positive. Only 3% of undergraduates indicated responding to at least one phishing electronic mail during the previous year. This result is consistent with the 2005 study that found only 3% of respondents complied with a phishing electronic mail request for data.

There are four important implications from the study. One finding is that electronic mail resources have a high waste factor. Nearly half of electronic mail received is spam. Unfortunately, only one out of five messages is class-related.

A second implication is that phishing attacks against undergraduates are not common. Only 26% of respondents indicated receiving phishing electronic mail. Of those receiving phishes, only 16 were received per month (or one every two days). In addition, only 16% of spam was identified as phishing attempts. This may be a result of several factors. It is possible that vendor efforts with regard to phish-filtering are becoming more effective. The study organization does utilize Barracuda, one of the leading spam filters, but does not employ a phishing filter, per se. Thus, phishing incidence would likely be higher without the spam filter. Moreover, undergraduates may not have yet developed electronic records that can be stolen. Or, phishers are targeting more economically prosperous individuals.

A third implication is that students may be practicing responsible computing behavior. Further research is needed to explore if and where the behavior was learned or if the behavior will need to be reinforced in the future.

A final implication is that phishers appear to be equal-opportunity brand hijackers. Nearly all brands identified in the study were equally spoofed in volume.

The limitations of this study are primarily a function of sample size and type of research. Even though responses were relatively equally distributed among academic class, future research utilizing a more equal gender distribution of respondents and using additional universities would increase the robustness of results and generalizability. Another limitation relates to the self-reported nature of the survey.

REFERENCES

Delio, Michele (2005). “IT Tackles Phishing.” *Infoworld.com,* Volume 27 Issue 4, 30-35.

Epstein, Jonathan D. (2005). “We’re getting smarter about ‘phishing’ scams, but too many get hooked.” *The Buffalo News*, July 9, D8.

Fisher, Dennis (2005). “Phishing Inc.” *eweek.com*, Volume 22 Issue 10, 20-24.

FTC (2007). “FTC Announces Annual List of Top Consumer Complaints.” February 7, http://www.ftc.gov/opa/2007/02/topcomplaints.shtm

Keizer, Gregg (2006). “Spoofing Spirals Up.” *informationweek.com*, Volume 1106, 58.

Kerstein, Paul L. (2005). “How Can We Stop Phishing and Pharming Scams?” *CSO*, July 19, http://www.csoonline.com/talkback/071905.html

Konrad, Rachel (2005). “Wondering if it was ID theft.” *The Times Herald*, February 27, D-1.

Mehta, Stephanie N. (2006). “Your Lousy Boss May Be An Identity Thief Also.” *Fortune*, Volume 154 Issue 12, 34.

Monahan, Mary (2007). “Your data’s less safe today than it was two years ago.” August 20, http://www.javelinstrategy.com/2007/08/20/your-datas-less-safe-today-than-two-years-ago/

Reilly, Shannon and Keith Simmons (2005). “Consumer Complaints up 17%.” *USA Today*, February 8, 2.

Toland, Bill (2005). “Gone Phishing.” *The Times Herald*, December 18, B-1.

Turner, Dean (2007). “Symantec Internet Security Threat Report.” *Symantec Enterprise Security*, Volume XI (March), http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

Wikipedia (2007). “Phishing.” http://en.wikipedia.org/wiki/Phishing