Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Analysis of Student Vulnerabilities to Phishing

Janet L. Bailey, Ph.D.
University of Arkansas Little Rock, jlbailey@ualr.edu

Robert B. Mitchell, DBA
University of Arkansas Little Rock, rbmitchell@ualr.edu

Bradley K. Jensen, Ph.D.
Microsoft, bjensen@microsoft.com

Analysis of Student Vulnerabilities to Phishing

Janet L. Bailey, PhD
University of Arkansas Little Rock
jlbailey@ualr.edu

Robert B. Mitchell, DBA
University of Arkansas Little Rock
rbmitchell@ualr.edu

Bradley K. Jensen, PhD
Microsoft
bjensen@microsoft.com

ABSTRACT

Phishing attacks were responsible for $3.2 billion dollars in losses during 2007 and the number of attacks is increasing daily. According to the United States Computer Emergency Readiness Team, phishing was the top security threat during the first quarter of 2007, comprising 48% of all reported incidents. The purpose of this study was to identify the level of student awareness related to specific phishing tactics. Findings revealed that while students are unlikely to provide personal information in response to an email request, they can be easily tricked by numerous other tactics. This paper reports the findings of the study in addition to listing suggested points to include in classroom discussions on phishing. Education is the most powerful tool available for combating the growing phishing security threat and student vulnerability.

Keywords

Phishing, phishing toolkit, socio-technical, cyber security, student vulnerabilities

INTRODUCTION

As electronic communications become more sophisticated and pervasive in the daily work environment, cyber security risks increase for both the individual user and businesses with whom the user maintains a relationship. One of the most prevalent techniques for compromising personal and organizational information is phishing. Of the top security threats and vulnerabilities reported by the United States Computer Emergency Readiness Team, phishing was the top cyber security incident for the first quarter of 2007, with 48% of all incidents reported (Quarterly Trends and Analysis Report, 2008).

MAGNITUDE AND COST OF PHISHING

Phishing is defined as "an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication" (Wikipedia, 2008). The Gartner report (Litan, 2007) notes "Phishing attacks are escalating, becoming more surreptitious, and are often designed to install malware that steals user credentials and sensitive information from consumer desktops." Trends reported by Symantec support the findings of the Gartner study. The Symantec Probe Network detected a total of 196,860 unique phishing messages during the first half of 2007 for an average of 1,088 unique messages per day, an increase of 18% over 2006. Their network blocked an average of 12.5 million phishing messages per day during the same period, an increase of 53% over the previous year (Symantec Internet Security Threat Report: Trends for January-June 2007, 2007). The Gartner survey, representative of the U.S. adult online population, found that 124 million people indicated that they had definitely received or think they received a phishing email, a 118% increase in three years. The study noted that an average of about 80 phishing emails had been received per person in the year ending in August, 2007 (Litan, 2007).

In addition, the Gartner study reported that 3.3% of the individuals (3.6 million) thought or were sure they had received phishing emails and were impacted financially, an increase from 2.3% in 2006. The per incident dollar loss, though, was $886, down from the $1,244 average in 2006, and about 1.6 million individuals were able to recover 64% of their losses in 2007 up from the 54% recovered by 1.5 million individuals in 2006. However, due to the increased volume of attacks, $3.2 billion was lost to phishing in 2007 (Litan, 2007) up $500 million from 2006 (Keizer, 2007). In a phishing attack involving a

financial loss, there are three parties: the consumer, the financial institution, and the phisher. Losses recovered by consumers are, in actuality, passed on to the financial institution (Zorz, 2008). During 2007 the financial institutions bearing the greatest losses were banks, PayPal and eBay (Litan, 2007).

PHISHING TECHNIQUES AND TARGETS

As online attacks have increased, the methods have become increasingly sophisticated and/or automated. Symantec observed three phishing toolkits were responsible for 42% of all attacks between January and June 2007 (Symantec Internet Security Threat Report: Trends for January-June 2007, 2007). Phishing toolkits are software systems available for purchase on the web, which allow less skilled, and thus greater numbers of, phishers to enter the game (Zorz, 2008). The phisher can also lease time on a compromised web server and typically can purchase 30,000 email addresses for $5 (Ramzan, 2007).

Most phishing methods have used link manipulation (a technical disguise), such as a slightly altered or masked URL or a subdomain, to redirect the user to the phisher's website. The use of the "@" symbol in the link can successfully fool the individual as to which URL will actually be opened since the server ignores all characters preceding the @. Using filer evasion phishers can outwit antiphishing software by using images instead of text in the emails (Recognize Phishing Scams and Fraudulent Emails, 2008; Wikipedia, 2008). A more sophisticated method of web forgery involves cross-site scripting (CSS or XSS). With this method a phisher finds corporate web site flaws, which allow modification of the script. The phisher can then hijack a legitimate session when a user logs onto the site. The phisher sends an email to a user, luring them to a legitimate web site. When the user logs onto the site, the phisher siphons identify information (Krebs, 2006).

Phishing may also involve social engineering. The phisher may obtain information from a user by posing as a credible individual (new employee, support person, or superior), possibly even showing credentials. Human interactions skills (social skills) are used in getting bits of information from one person and then another until sufficient data have been collected to compromise a system (National Cyber Alert System Cyber Security Tip ST04-014, 2007). Social engineering is especially worrisome since Internet users may be over four times as likely to fall prey to phishing schemes if they are solicited by someone who appears to be an acquaintance (Jagatic, Johnson, Jakobsson, & Menezer, 2007). A variant of social phishing known as "spear phishing" was reported by the SANS Institute to have been on the rise in 2007, with a focus on executives. Spear phishing is a very focused plan of attack in which certain specific information is known about the individual or organization; thus, the email seems credible. The SANS report noted that spear phishing has been highly successful (80% success rate) against U.S. military targets (Vaas, 2007). In yet another example, spear phishers sent fraudulent emails to Minnesota-based Supervalu from what appeared to be two of their approved suppliers directing future payments to new bank accounts. Fortunately, although nearly $10 million was deposited into the bogus accounts prior to discovery of the scam, the vast majority of the funds were recovered before withdrawal by the phishers (Vijayan J. , 2007).

Organized phishing attacks on students are common. One of the most recent widespread attacks, impacting schools such as Columbia University, Duke University, and Princeton University, to name a few, was documented in January of 2008. The email accounts and faculty that were victimized were used to send additional spam in a lottery scam (Lemos, 2008). Wagner (2006) states that students are prime targets for phishing, due to their inexperience yet feeling of invincibility; they are often naïve regarding virtual security threats. Thus students must be taught to avoid the traps of phishing predators. When students fall prey to phishing schemes and compromise their identity, financial institutions and other transaction processors are also impacted due to the ripple effect of who absorbs the financial loss. Thus far financial institutions have chosen to absorb the costs rather than change their static systems of personal identifiers, a change that would cost them even more (Zorz, 2008).

SOCIO-TECHNICAL COMBAT APPROACH

A combination of socio-technical methods should be used to combat the methods of phishing. Technical protection is needed at the user side as well as at the network gateway. At minimum firewalls, intrusion detection software, and spam filters can help combat phishing. In addition, combinations of the following should be considered: use a version of browser that contains antiphishing components, open attachments or click on links in emails only from trusted individuals, allow only approved components to be connected to the network, enforce rigorous password policies for individuals and devices, and monitor

suspicious network connection attempts. Layered solutions should be used to protect from not only receiving phishing emails but also sending "spam" phishing emails (Botnet threats and solutions: Phishing, 2006).

Today's security problems in general are the result of inadequate user awareness, a fact that emphasizes the human element is more important than technology (Alun, Potter, & Beard, 2006; Desman, 2003; Vijayan J. , 2007). Yet as with security risks in general, a crucial and possibly more important approach is educating users on the tools and knowledge available to protect themselves from phishing attacks (Vijayan J. , 2005). "The likelihood is that future phishing, or whatever phoolware follows it, will continue the cat-and-mouse game with security software. Perhaps our greatest mistake is excessive reliance on technology solutions:" (Berghel, 2006). Unfortunately, the 2007 Gartner study emphasizes that consumer awareness education programs of the government and financial services organizations thus far have not been very effective (Litan, 2007). To protect personal and corporate resources, organizations must implement both awareness and experiential training programs. An individual may become aware of phishing and associated tactics, but appropriate user responses are often assured only through formalized training designed to provide experience in spotting and appropriately responding to phishing emails (Kenney, 2007). Educational institutions of higher learning have an obligation to partner with organizations in raising awareness and, thus, protection against phishing tactics.

Projections indicate that in the near future cybercrime will continue; and, thus, consumer education will be of increasing importance.

> Gartner sees no way out of this dilemma unless e-mail providers are motivated to invest in solutions to keep phishing e-mails from reaching consumers in the first place, and unless advertising networks and other 'infection point' providers (which theoretically can be any legitimate Web site or service) are motivated to keep malware from being planted on their Web sites to reach unsuspecting consumers (Litan, 2008, p. 13).

STATEMENT OF THE PROBLEM AND RESEARCH METHODS

This study was designed to identify the current level of knowledge of phishing tactics among students in order to determine their vulnerability. Students, as established in the literature, are viewed as easy prey by phishers which makes them vulnerable at a time when finances are generally stretched thin. Additionally, decisions made by students also affect the organizations for which they work. An understanding of student knowledge and likely behaviors is necessary for developing a program of study to help them protect themselves and those around them. The following questions were addressed:

1. What is the level of awareness of college students regarding phishing tactics and results?
2. How do students react to specific phishing tactics?
3. Is there a difference in the way students of differing demographics react to specific phishing tactics?

One hundred sixty undergraduate students in required freshman- and junior-level business core information system courses from a single campus participated in the study during the Spring 2008 semester. None of the sections had covered the topic of security thus far in the semester. Participants responded to a questionnaire containing demographic data and awareness questions rated on a five-point Likert scale ranging from very unlikely (1) to very likely (5).

RESEARCH FINDINGS

Table 1 presents the finding for the group as a whole. The percentages in the response column for the first nine questions indicate the percent of students who would engage in risky behavior based on the occurrence of the event described in the "Item" column. Risky behavior was defined as not being very likely or likely to have engaged in safe behavior. Thus, the higher the percentage, the greater the risk to the individual and to the organizations with which the student has a relationship. Coupled with the fact that 74% of respondents access their online accounts at least once a week (item #10 Table 1), the vulnerabilities take on a frightening proportion.

Item #	Item	Response N=160
#1	If you received an email containing the logo and web address from your bank or one of your credit card companies requesting that you verify information such as your date of birth, social security number, account number, etc., and the email were addressed to "Dear customer" – how likely are you to click on the link and provide the requested information?	8%
#2	If you received an email containing the logo and web address from your bank or one of your credit card companies requesting that you verify information such as your date of birth, social security number, account number, etc., and the email were addressed to you personally – how likely are you to click on the link and provide the requested information?	17%
#3	If you receive an email requesting that you click on a link to go to another site to provide personal information, how likely are you to key the URL into the address bar instead of clicking on the link?	88%
#4	When you are redirected to a site to provide personal information, how likely are you to check the address bar to make sure the URL starts with https://?	63%
#5	When you are redirected to a site to provide personal information, how likely are you to check for the yellow lock near the bottom of the screen?	57%
#6	If you have arrived at a site by clicking on a link in an email and the yellow lock is displayed, how likely are you to double click on the yellow lock?	81%
#7	If you click on a link and are directed to a site, how likely are you look at the address line to see if it shows the same address that appeared in the email link?	64%
#8	How likely are you fill out an email form asking for personal financial information if the email appeared to be from a trusted site and was addressed to you personally?	8%
#9	When you receive an email and attachment that you weren't expecting from a friend, how likely are you to contact your friend to verify he or she sent the email before you open the attachment ?	79%
#10	Report logging into online accounts more than once a week	74%
#11	Understand characters preceding the @ in a link are ignored	21%
#12	Report never having received a phishing email	36%

Table 1. Responses from All Participants

Students, as a whole, are well informed and, therefore, well protected against phishers when it came to the receipt of emails from financial institutions requesting personal information. They also demonstrated a good understanding of the inadvisability of filling out an email form requesting personal financial information even if it appeared to be from a trusted site. Unfortunately, their level of knowledge seems to end at that point, as seen in Table 1. Eighty-eight percent of the respondents would fall prey to the URL masking technique. This finding is problematic due to the frequent use of URL masking. Since 64% of the respondents do not check the URL in the address bar to see if the URL matches the one in the link, the issue becomes a serious concern.

Results were more positive for student awareness of the importance of checking for secure website signs—https:// and the yellow security lock. Even so, the majority still report engaging in risky behavior in these areas as well. With 81% of respondents reporting that they would not double-click on the yellow lock to ensure its validity, in all likelihood the vast majority of students are not aware that the lock can be counterfeited. This finding is validated when one considers that 43% of students reported looking for the lock while only 19% would check to make sure that it is legitimate.

Surprisingly, 79% of individuals would open an unexpected email attachment from a "friend" making them vulnerable to spyware and key loggers. Perhaps over-reliance on antivirus software has led to this complacency.

The final item in Table 1 reflects the number of respondents who claim to have never received a phishing email. With the predominance of phishing in today's marketplace, it is much more likely that 36% of the respondents do not know what phishing is than that they have never received a phishing email.

Tables 2 through 5 report the data categorized by the collected demographics where differences were observed. The numbers in the description correspond to the item # from Table 1.

Table 2 compares the responses between students in each of the two courses selected for participation. Overall the participants in the freshman-level course engage in less risky behavior than the students in the junior-level course. While at first glance this finding does not seem to make sense, a closer look at the demographics reveals that the students in the freshman-level course on average are older with 35% of the students being 26 years old or older while only 30% of the junior-level course are 26 years old or older. Additionally, 46% of the freshman-level students work full-time while only 43% of the junior-level students work full-time. The age and work experience may translate into greater caution. It should be noted, however, that despite the fact that more of the freshman-level students exercise more caution than the junior-level students, the majority report that they would make decisions resulting in vulnerability to phishing attacks in the same areas as Table 1.

Description		Freshman-level	Junior-level
N		89	71
#1	Likely to respond to Dear Customer email	7%	8%
#2	Likely to respond to personally addressed email	13%	21%
#3	Unlikely to type URL	84%	92%
#4	Unlikely to check address bar for https://	62%	65%
#5	Unlikely to check for yellow lock	55%	59%
#6	Unlikely to double click yellow lock	75%	87%
#7	Unlikely to verify address match	57%	73%
#8	Likely to complete email form request	7%	8%
#9	Unlikely to verify attachment validity	73%	86%
#10	Frequent online account activity	69%	80%
#11	Understand characters preceding @ ignored	18%	25%
#12	Report never receiving phishing email	35%	36%

Table 2. Responses by Course

Table 3 reports the differences between male and female respondents. On all items except number 8, males are more cautious although, once again, they tend to make poor decisions that make them vulnerable. Further analysis of the demographics reveals that age and work experience do not come into play in the differences found in this table. Thirty percent of male respondents are 26 years of age or older compared to 35% of females. Thirty-five percent of the male respondents work full time compared to 49% of the female respondents. Further research is needed to determine if these differences are unique to this study and, if not, why the differences exist.

Description		Male	Female
N		86	74
#1	Likely to respond to Dear Customer email	5%	11%
#2	Likely to respond to personally addressed email	16%	18%
#3	Unlikely to type URL	84%	92%
#4	Unlikely to check address bar for https://	59%	68%
#5	Unlikely to check for yellow lock	56%	58%
#6	Unlikely to double click yellow lock	77%	85%
#7	Unlikely to verify address match	59%	70%
#8	Likely to complete email form request	11%	4%
#9	Unlikely to verify attachment validity	78%	80%
#10	Frequent online account activity	78%	69%
#11	Understand characters preceding @ ignored	25%	17%
#12	Report never receiving phishing email	33%	39%

Table 3. Responses by Sex

On most items, working respondents are more cautious than their full-time-student counterparts, as seen in Table 4.

Description		Full	Part	School Only
N		71	64	24
#1	Likely to respond to Dear Customer email	4%	11%	8%
#2	Likely to respond to personally addressed email	13%	19%	25%
#3	Unlikely to type URL	86%	86%	96%
#4	Unlikely to check address bar for https://	62%	61%	71%
#5	Unlikely to check for yellow lock	54%	61%	54%
#6	Unlikely to double click yellow lock	79%	80%	88%
#7	Unlikely to verify address match	63%	63%	71%
#8	Likely to complete email form request	6%	8%	13%
#9	Unlikely to verify attachment validity	76%	83%	79%
#10	Frequent online account activity	79%	69%	71%
#11	Understand characters preceding @ ignored	25%	21%	13%
#12	Report never receiving phishing email	34%	39%	29%

Table 4. Responses by Work Schedule

As shown in Table 5, the category of greater than 6 years of email use has a lower percentage of individuals who engage in poor decision-making than any other category with the exception of two items: keying the URL into the address bar and double clicking on the yellow lock. While 87% would not key the URL into the address bar, 42% would verify that the URL in the address bar is the same as the one they clicked. The high percentage of respondents that would not double click on the yellow lock reveals the danger of complacency and the advantage phishers have when they develop a new scheme.

Description		2-4 yrs	4-6 yrs	>6 yrs
N		16	44	97
#1	Likely to respond to Dear Customer email	19%	9%	5%
#2	Likely to respond to personally addressed email	25%	23%	13%
#3	Unlikely to type URL	100%	86%	87%
#4	Unlikely to check address bar for https://	63%	70%	60%
#5	Unlikely to check for yellow lock	94%	61%	49%
#6	Unlikely to double click yellow lock	81%	77%	82%
#7	Unlikely to verify address match	81%	70%	58%
#8	Likely to complete email form request	6%	14%	5%
#9	Unlikely to verify attachment validity	75%	86%	75%
#10	Frequent online account activity	75%	68%	77%
#11	Understand characters preceding @ ignored	40%	18%	20%
#12	Report never receiving phishing email	67%	36%	30%

Table 5. Responses by Length of Email Use

SUMMARY AND CONCLUSIONS

The respondents of this study demonstrate a good understanding of the inadvisability of responding to emails from what appears to be a financial organization. Unfortunately, their sound decision-making abilities stop at that point. These results emphasize the need for education on phishing.

Academicians have the opportunity to send informed consumers into the workforce where they can protect not only themselves but their organizations. In order to adequately prepare and motivate students to increase and maintain their level of awareness instructors should incorporate content not only on how to recognize phishing emails and fraudulent websites but also on the cost and magnitude of the phishing problem. Students need to understand the ripple effect caused by this phenomena. They need to understand that even if they as a consumer are reimbursed for a loss, a financial institution has had to bear that loss – a loss that ultimately impacts shareholders and consumers. Students need to understand the significance of the types of information that can be obtained by phishers as illustrated by the military example earlier in this paper.

Over-reliance on technical solutions for protection is dangerous but common. The best defense is a continuing education program. Phishers will not stop generating new ideas nor will they cease to communicate or sell information to each other over the web; thus greater numbers of attacks are facilitated. Money is readily available by defrauding those foolish enough to fall prey to the latest scam.

Sometimes the latest scam is actually an old trick revamped for a new purpose. Take, for example an email attachment. At one point in time, individuals had become more cautious about opening an attachment they were not expecting even if it appeared to come from a trusted source because attachments at that point in time were often Trojan horses designed to deliver viruses. Anti-virus software has become sophisticated enough to catch and eliminate infected attachments as a major concern but now the same scheme is being used to deliver spyware and key-loggers to systems. The results of this study revealed that 79% of the respondents would open an attachment they were not expecting without verifying that it had been sent by a friend.

Suggested points to include in class discussions include:

In 2007

- $3.2 billion was lost to phishing
- Per incident dollar loss was $886 (Litan, 2007)

- 3.6 million individuals thought or were sure they had received phishing emails and were impacted financially
- Symantec's Probe Network blocked 196,860 unique phishing messages in the first six months
- Symantec's Probe Network blocked 12.5 million phishing messages per day in the first six months
- Three phishing toolkits (these toolkits automate the phishing process) accounted for 42% of all attacks in the first six months (Symantec Internet Security Threat Report: Trends for January-June 2007, 2007)

Things to look for in scam email and websites

- An "official" looking sender's email address which is easily altered
- Generic email greeting – Dear User indicates mass mailing
- False sense of urgency – threats that your account is in "danger" are typically fraudulent
- Key phrases such as "Verify your account"
- Fake links – move the mouse over the link to see if the URL changes
- Slightly altered URLs – i.e. www.micosoft.com instead of www.microsoft.com
- Links containing the @ symbol – characters preceding the @ will be ignored
- Out-of-place lock icon – should appear on status bar not the web site window
- Security certificate – double click on the lock icon to display the security certificate. If the certificate does not appear, the lock is counterfeit. (Recognize Phishing Scams and Fraudulent Emails, 2008)

How to handle suspicious email

- Do not respond
- Check http://www.millersmiles.co.uk/ to search for the email
- Report it to
    - The Anti-Phishing Working Group at http://www.antiphishing.org/
    - The Federal Trade Commission (FTC) at http://www.ftc.gov/bcp/edu/microsites/idtheft//
    - The organization that the email appears to be from – i.e. Paypal, Chase, etc.
    - The FBI

What to do after responding to a phishing email

- Report the incident
- Change passwords on all online accounts
- Routinely review credit card and bank statements for fraudulent activity
- Use the latest anti-phishing products and services (Recognize Phishing Scams and Fraudulent Emails, 2008)

Take a proactive defense

- Check http://www.millersmiles.co.uk/
    - Review daily scam updates
    - Search for specific emails
    - Read the latest news regarding phishing
- Implement a combination of the most current security technology and safe user practices
    - Install, update, and maintain firewalls and intrusion detection software
    - Use the latest browser and security patches
    - Practice awareness
    - Never email financial or personal data
    - Open attachments only from trusted sources – verify (Botnet threats and solutions: Phishing, 2006)

- Don't click links – phishers can display a fake URL in the address bar on the browser
- Type addresses directly into the browser or use personal bookmarks
- Verify security certificates by double clicking on yellow lock (Recognize Phishing Scams and Fraudulent Emails, 2008)
- Know Internet Explorer 7 colors
    - Red – phishing site that has been reported to Microsoft
    - White – page that is not supposed to ask for or display personal information
    - Yellow – suspicious website – may be fraudulent
    - Green – certified safe
- Remember that technology alone can not protect users and organizations from phishing
- Educate family, friends, and coworkers

Phishing attacks are growing more numerous each day. As long as there are con artists and people foolish enough to fall for their scams, phishing will be a problem. In other words, phishing is likely here to stay and the most powerful tool for combating the threat is education. It is up to educators to stem the phishing tide.

REFERENCES

1. Alun, M., Potter, C., and Beard, A. (2006) *Information security breaches survey 2006,* Retrieved February 26, 2008,from http://www.pwc.co.uk/pdf/pwc_dti-fullsurveyresults06.pdf

2. Berghel, H. (2006) Phishing mongers and posers, *Communications of the ACM* , 49,4, 21-25.

3. *Botnet threats and solutions: Phishing.* (2006) Retrieved February 25 from http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/wp01_phishingfinalproof.pdf

4. Desman, M. (2003) The ten commandments of information security awareness training, *Information Systems Security , 11,*6, 39-44.

5. Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menezer, F. (2007) Social Phishing. *Communications of the ACM , 50,*10, 94-100.

6. Keizer, G. (2007) *Phishers pinch billions from consumer' pockets,* Retrieved February 25, 2008, from www.computerworlduk.com/management/security/cybercrime/news-analysis/index

7. Kenney, B. (2007) From ID to IP theft. *Industry Week/IW , 256,* 7, 49.

8. Krebs, B. (2006) *Flaws in financial sites aid scammers,* Retrieved February 25, 2008, http://blog.washingtonpost.com/securityfix/2006/06/flaws_in_financial_sites_aid_s.html

9. Lemos, R. (2008) *Universities fend off phishing attacks*, Retrieved February 25, 2008, from http://www.securityfocus.com/print/news/11504

10. Litan, A. (2007) *Phishing attacks escalate, morph and cause considerable damage,* Stamford: Connecticut: Gartner, Inc.

11. *National Cyber Alert System Cyber Security Tip ST04-014.* (2007) Retrieved February 25, 2008, from http://www.us-cert.gov/cas/tips/ST04-01`4.html

12. *Quarterly Trends and Analysis Report.* (2008) Retrieved February 25, 2008, from http://www.us-cert.gov/press_room/trendsandanalysisQ108.pdf

13. Ramzan, Z. (2007) *AbBrief history ofpPhishing: Part ,.* Retrieved 2 25, 2008, from http://www.symantec.com/enterprise/security_response/weblog/2007/08/a_brief_history_of_phishing.html

14. *Recognize phishing scams and fraudulent eEmails.* (2008) Retrieved February 25, 2008, from http://www.microsoft.com/protect/yourself/phishing/identify.mspx

15. *Symantec Internet security threat report: Trends for January-June 2007.* (2007) Retrieved 2 29, 2008, from http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf

16. Vaas, L. (2007) Online attacks on people grow. *eWeek , 24,* 37, 26.

17. Vijayan, J. (2007) Phishers nearly pull off $10M scam of grocer. *Computerworld* , 41,44, 14.

18. Vijayan, J. (2005) Targeting the enemy within. *ComputerWorld , 39,* 32, 23-27.

19. Wagner, M. (2006) Who's phishing for your students? . Retrieved February 25, 2008, from http://education.zdnet.com/?p=80

20. *Wikipedia.* (2008) Retrieved February 25, 2008, from en.wikipedia.org/wiki/Phishing

21. Zorz, M. (2008) *Interview with Nitesh Dhanjani and Billy Rios, spies in the phishing underground,* Retrieved February 25, 2008, from http://www.net-security.org/article.php?id=1110