https://doi.org/10.48009/1_iis_2016_80-88

Issues in Information Systems
Volume 17, Issue I, pp. 80-88, 2016

PHISHING: ARE UNDERGRADUATES AT RISK AND PREPARED?

Carl J. Case, St. Bonaventure University, ccase@sbu.edu
Darwin L. King, St. Bonaventure University, dking@sbu.edu

ABSTRACT

The extraordinary losses as a result of new and recent phishing attacks is disconcerting and troubling in the business community. Because business students will become the future targets of business phishing attacks, this study was undertaken to examine the trends relative to student phishing. Results demonstrate that currently only about one-fifth of students receive phishing email and that during the five-year study period, both the percentage of students receiving phishing email and volume of phishing email have decreased. Moreover, in terms of behavior, few students respond to phishing email or have been a victim of identity theft. Overall, although there is room of educational improvement, students are likely prepared to face the phishing battle upon entrance into the working world. Results also suggest that the technological and instructional solutions utilized in academia may provide similar benefits for businesses in fighting the war against phishing.

Keywords: Phishing, Electronic Mail, Identity Theft

INTRODUCTION

Phishing, a social engineering scam in which an email user is duped into revealing personal or confidential information that the scammer can use illicitly, is reaching epidemic levels (Webster, 2016). In 2014, for example, BitPay lost $1.8 million due to phishing (Sjouwerman, 2015). In 2015, Malwarebytes discovered a phishing attack targeting Amazon customers (Umawing, 2015). The deceptive email claimed to be from the Amazon customer service department and falsely stated that a small number of accounts were breached and required the victims to complete a verification process or their account would be restricted. A Wombat study further found that 85% of firms were victimized in 2015 and 60% of firms indicated that the rate of phishing has increased (Wombat, 2016). The result of the attacks being that 44% of firms had productivity losses, 42% had malware infections, 36% faced consequences related to the loss of proprietary information, 22% had compromised accounts, and 20% had to deal with damage to their reputation. Ponemon calculated the total cost to be $3.8 million for a 10,000 person company (Wombat, 2016).

Another insidious result of phishing attacks is identity theft. The IRS launched 1,492 criminal investigations into identity theft in 2013, a 66% increase from the previous year, and flagged 14.6 million suspicious tax returns from 2011-2013 (Associated Press, 2014). A survey of 768 global companies found that 75% experienced a fraud incident in the past year, a 14% increase in 3 years, with 81% of companies affected by fraud reporting insider perpetrators (Kroll, 2016). The industries with the highest percentage of fraud prevalence include the manufacturing, retail, wholesale, distribution, technology, media, and telecommunications sectors. Interestingly, whistleblowers were responsible for exposing 41% of fraud incidents.

The increase in phishing attacks is especially troubling given the increasing reliance upon email. In terms of consumers, there were approximately 3.3 billion email accounts worldwide at the beginning of 2016 (Radicati, 2014)]. Relative to volume, an estimated 247 billion email messages are sent each day with the average consumer email recipient receiving approximately 416 emails each month and 91% of consumers checking their email at least once each day (Bickerton, 2015). In terms of business users, there were approximately one billion corporate email accounts worldwide at the beginning of 2016 (Radicati, 2014). Although an estimated 116 billion corporate email messages per day were sent in 2012, business email volume is predicted to grow by 28% from the 109 per day in 2014 to 139 per day in 2018 (IBM, 2013). On average, workers in the UK, for example, spend at least a quarter of their day managing email (Daily Mail Reporter, 2012). Not only has email interaction been found to be important in building customer ties (Murphy, 2013), 83% of U.S. knowledge workers indicated that email was critical to their success and productivity at work (Auby, 2010).

Of recent note is the relatively new and devastating technique known as spear-phishing. Spear-phishing, also known as CEO fraud and business email compromise, targets businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments (Krebs, 2015). The process involves spoofing or hijacking the email accounts of business executives or employees. In January 2015, for example, the FBI reported that businesses lost $215 million in such scans during the previous 14 months. In February 2015, an employee-owned commodities trader Scoular Company lost $17.2 million and, in June 2015, technology firm Ubiquiti Networks Inc. lost $46.7 million. In July 2015, the Pentagon email network used by the Joint Chiefs of Staff was spear-phished (Lubold and Paletta, 2015).

Symantec, an information protection firm that operates one of the largest global data-intelligence networks, found nearly a doubling of organizations being attacked (2015). In 2013, 43% of large enterprises, 33% of medium businesses, and 19% of small businesses were targeted in spear-phishing campaigns. However, in 2014, 83% of large enterprises, 63% of medium businesses, and 45% of small businesses were targeted. Moreover, in 2014, there was an average of 73 spear-phishing emails detected per day. The industries targeted with the greatest volume of spear-phishing attacks are the manufacturing, service, finance, insurance, and real estate sectors. In terms of job role, sales and marketing personnel were the most targeted, with 1 in 2.9 of them being targeted at least once. Operations were second at 1 in 3.8 individuals and finance was third at 1 in 3.3 individuals. In terms of job level, managers were the most targeted with 26% of managers being targeted at least once.

Given the apparent increase in corporate phishing and, in particular, its new menacing iteration named spear-phishing, this research was conducted to examine several questions. What is the state of phishing with regard to undergraduate business students? Is there a trend? Is the incidence similar to levels found in industry? Are business students likely to be victims? Results are important given that business students are the future business professionals that will be entrusted in protecting organizational resources. Ultimately, these findings will be helpful in determining if students will be adequately prepared to face the criminal challenges that will be present when they enter the corporate workforce.

PREVIOUS RESEARCH

Previous research studies have examined business email behavior and anti-phishing approaches. In addition, the authors conducted two exploratory research studies to better understand undergraduate business student email behavior and to establish a baseline for future research.

In terms of business email behavior, Huang and Lin (2009) found that e-mail has to a great extent replaced face-to-face communication and is the preferred way to communicate in the office environment. The researchers also found that people are ruled by e-mail and few could not control the impulse to incessantly check for new email and had feelings of loss upon seeing an empty in-box. All of the study participants further indicated that they respond quickly to every email message, regardless of its urgency.

A comprehensive literature review of 16 doctoral theses and 358 research papers in the field of phishing research found that there are eight categories of anti-phishing approaches (Swapan, 2012). These include: stop phishing at the email level; security and password management toolbars; restriction list; visually differentiate the phishing sites; two-factor and multi-channel authentication; take-down, transaction anomaly detection, log files; anti-phishing training; and, legal solutions. The review also found that phishers mainly target the innocent consumers who happen to be the weakest link in the security chain. Moreover, various usability studies found that neither the server-side security indicators nor the client-side toolbars and warnings were successful in preventing vulnerable users from being deceived.

In addition, a user study designed to assess whether improved browser security indicators and increased awareness of phishing found that users successfully detected only 53% of phishing websites even when primed to identify them and that they generally spend very little time gazing at security indicators as compared to website content when making assessments (Alsharnouby, Alaca, & Chiasson, 2015). However, researchers found that gaze time on

browser chrome elements did not correlate to increased ability to detect phishing. Moreover, users′ general technical proficiency did not correlate with improved detection scores.

Moreover, Mohammad, Thabtah, and McCluskey (2015) conducted a survey of the state of the art research on phishing attacks. The researchers found several approaches were proposed to mitigate these attacks. Anti-phishing measures may take several forms including legal, education and technical solutions. Research has indicated that in many instances, the identification of phishing websites is performed manually by the user. There are, however, computational technologies that can automate the process of predicting phishing websites. Unfortunately, filtering methods such as blacklist and whitelist-based detection approaches fail to deal with zero-days phishing websites. On the other hand, heuristics-based detection approaches have a possibility to recognize these websites. However, the accuracy of the heuristics-based approaches may fall remarkably if some environmental features change. Thus, users would become doubting the protection system and would ignore the warnings raised from detection systems.

Finally, a role play scenario experiment of user ability to differentiate between phishing and genuine emails demonstrated limitations in the generalizability of phishing studies (Parsons, et.al, 2015). Only half of the 117 participants were explicitly informed that the study was assessing the ability to identify phishing emails. Results indicate that the informed participants were significantly better at discriminating between phishing and genuine emails than the uninformed participants. As a consequence, studies where participants are directly asked to identify phishing emails may not represent the performance of real world users given that users are rarely reminded about the risks of phishing emails in real life. In addition, researchers found that because participants' performance differs greatly in terms of category (e.g., type of sender) of emails, caution should be used when interpreting the results of phishing studies that rely on only a small number of emails and/or emails of limited diversity. Thus, when designing and interpreting phishing studies, researchers should carefully consider the instructions provided to participants and the types of emails used.

Relative to undergraduate business student email behavior, the authors conducted an exploratory study in 2006-2007 (Case and King, 2008). Results indicated that 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 phishing emails, 6.6 Amazon.com phishing emails, 6.2 eBay phishing emails, and 7.8 other phishing emails per month. Other phishing email included PayPal, loan payoff, bank accounts, myspace.com, and car loans. In terms of percent of respondents, 19% indicated receiving credit card phishing emails, 14% eBay phishing emails, 12% Amazon.com phishing emails, 9% Nigerian scam phishing emails, and 3% other phishing emails. Overall, only 26% of respondents reported receiving at least one phishing email per month. The average quantity of phishing electronic mail received per month was 16.4 messages, accounting for 7.5% of the total electronic mail received by undergraduates per month. Only 3% of undergraduates indicated responding to at least one phishing electronic mail during the previous year.

A subsequent study conducted by the authors empirically investigated the state of phishing from 2007 to 2010 (King and Case, 2012). Phishing emails as a percentage of total emails received increased slightly from 7.4% to 7.7%. Comparing the phishing scams by type, the credit card schemes remained constant with 23% of students reporting them in 2007 and 24% in 2010. Amazon.com schemes were reported by 17% of students in 2007 and 19% in 2010. eBay frauds were reported by 16% of students in 2007 and by 15% of students in 2010. Nigerian frauds were received by 10% of students in 2007 and 6% in 2010. Of note is that 2% of students responded to at least one phishing email. The study also found that the percentage of students reporting that he or she had been the victim of identity theft increased from 4% in 2007 to 6% in 2010. Moreover, although students reported in 2007 that 29% knew of someone who had been a victim of identity theft, the percentage increased to 36% in 2010.

Because the state of phishing is continually evolving, this study was conducted to examine the current status of undergraduate phishing. In addition, this study builds upon prior research by exploring the latest trends.

RESEARCH DESIGN

This study employs a survey research design. The research was conducted at a private, northeastern U.S. university. An Electronic Mail Behavior 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 Business Information Systems, Business Telecommunications, System Analysis and Design, Introduction to Financial Accounting, Introduction to Managerial Accounting, Management and Organization Behavior, Business Policy, and Women in Business. A convenience sample of class sections and faculty members was selected. The surveys were collected each semester during a five-consecutive year or 9 semester period (from Fall 2011 through Fall 2015) in academic classrooms.

The survey instrument was utilized to collect student demographic data such as gender and academic class. In addition, the survey examined student behavior with regard to the type and of volume of various types of email received. The survey also examined the incidence of identity theft and respondent response to phishing email. To ensure consistency, the same questions were asked during each of the 9 semesters.

Because of the sensitivity of the subject and to encourage honesty, no personally-identifiable data were collected and respondents were informed that surveys were anonymous, participation was voluntary, and responses would have no effect on their course grade. As a result, the response rate was nearly 100 percent.

RESULTS

A sample of 1,668 usable surveys was obtained. Table 1 indicates that 60% of the respondents were male and 40% were female. This 60/40 ratio has remained fairly consistent over the identified five-year period.

Table 1. Gender Response Rate By Academic Year

	2011	2012	2013	2014	2015	Total
Male	60%	59%	59%	59%	61%	60%
Female	40%	41%	41%	41%	39%	40%
Count	359	384	359	353	213	1668

The response rate by academic class is relatively equally distributed. Table 2 illustrates that 17% of respondents were freshmen, 36% were sophomores, 21% were juniors, and 26% were seniors.

Table 2. Academic Class Response Rate By Academic Year

	2011	2012	2013	2014	2015	Total
Freshmen	18%	23%	6%	18%	23%	17%
Sophomore	47%	28%	35%	35%	33%	36%
Junior	15%	24%	23%	23%	23%	21%
Senior	19%	36%	36%	27%	21%	26%

Responses were first examined with regard to activity per year. Table 3 illustrates that for every year of the study, credit card phishing emails are the most common type of attack among students. This is followed by Amazon.com, eBay, Nigerian scam, and other phishing-type emails, respectively, in percentage occurrence. In terms of type by year, the percentage of students receiving credit card phishing email has decreased from 20% in 2011 to 18% in 2015. The percentage of students receiving Amazon.com phishing email has increased from 14% in 2011 to 16% in 2015. The percentage of students receiving eBay phishing email has decreased from 12% in 2011 to 8% in 2015. The percentage of students receiving Nigerian scam phishing email has decreased from 8% in 2011 to 6% in 2015. The percentage of students receiving other phishing email has remained stable at 4% in 2011 and in 2015. Overall, the percentage of students receiving any type of phishing email has decreased from 29% in 2011 to 21% in 2015.

Table 3. Percent of Students Receiving Phishing Email By Academic Year

Phishing Type	2011	2012	2013	2014	2015
Credit Cards	20%	20%	22%	23%	18%
Amazon.com	14%	15%	18%	19%	16%
eBay	12%	11%	12%	11%	8%
Nigerian Scam	8%	9%	10%	9%	6%
Other	4%	4%	5%	5%	4%
Overall Average	29%	29%	32%	31%	21%

Table 4 presents the volume of phishing email received per student per month for each of the study years. In 2011, for example, respondents reported receiving 8.2 credit card phishing emails, 6.5 Amazon.com phishing emails, 7.2 eBay phishing emails, 10.5 Nigerian scam phishing emails, and 10.1 other phishing emails per month. By 2015, the quantity per month of credit card phishing emails decreased to 4.7, Amazon.com phishing emails decreased to 4.9, eBay phishing emails decreased to 5.0, Nigerian scam phishing emails increased to 14.9, and other phishing emails decreased to 6.4. The relative quantity of each type of phishing email varied by year with no discernible pattern across the years. Overall, the average volume of phishing email decreased from 15.6 per month in 2011 to 14.9 per month in 2015. Moreover, the volume of phishing email as a percentage of all email received per respondent decreased from 7.4% in 2011 to 6.7% in 2015.

Table 4. Phishing Messages Received Per Month By Academic Year

Phishing Type	2011	2012	2013	2014	2015
Credit Cards	8.2	6.3	6.2	4.6	4.7
Amazon.com	6.5	11.0	6.2	5.3	4.9
eBay	7.2	10.0	7.6	3.8	5.0
Nigerian Scam	10.5	6.1	8.4	5.3	14.9
Other	10.1	13.3	16.2	2.5	6.4
Overall Average	15.6	17.2	15.7	9.1	14.9
As % of all email	7.4%	7.5%	5.7%	4.2%	6.7%

Next, the response rate to phishing emails and incidence of identity theft was examined by year (Table 5). In 2011, 2% of students responded to a phishing email, 7% were victims of identity theft, and 35% personally knew another victim of identity theft. In 2015, 4% of students responded to a phishing email, 7% were victims of identity theft, and 32% personally knew another victim of identity theft. Overall, there was little variance across the study years.

Table 5. Phishing Response and Identity Theft as a Percent of Students By Academic Year

	2011	2012	2013	2014	2015
Responded to Phishing Email	2%	3%	2%	3%	4%
Have been victim of identity theft	7%	5%	6%	6%	7%
Know another victim of identity theft	35%	32%	36%	35%	32%

Finally, Spearman Rho correlations were calculated to determine if there are potential relationships between study variables and whether the student responded to a phishing email (Table 4). The Spearman Rho correlation was utilized because it is a nonparametric measure of statistical dependencies between two variables (Conover, 1999). Results found that two variables had significant correlations with whether the student responded to a phishing email. Gender had a significant correlation at the .01 level and quantity of phishing email received had a significant correlation at the .05 level. In particular, males were much more likely than females to respond to a phishing email. Academic class, on the other hand, has no statistically significant correlation to behavior.

Table 6. Spearman Rho Correlations Between Study Variables and Phishing Response

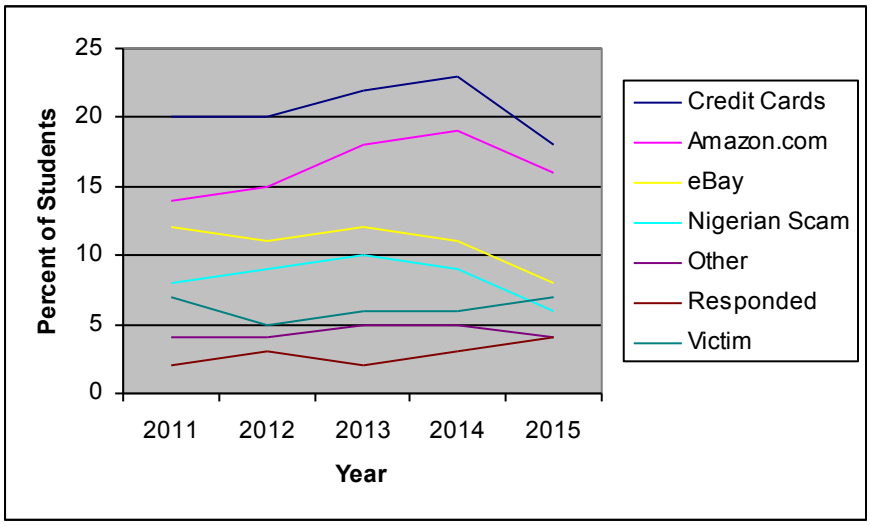
Variable	Correlation With Phishing Response
Gender	.060*
Academic Class	.000
Quantity of Phishing Email Received	.139**

* Correlation is significant at .05 level (2-tailed).
** Correlation is significant at .01 level (2-tailed).

CONCLUSIONS, IMPLICATIONS, AND LIMITATIONS

Results indicate that few students are receiving phishing email. Moreover, the percentage of students receiving credit card phishing email, eBay phishing email, and Nigerian scam phishing email decreased during the five-year study period. The most common types of phishing email for each year were credit card (18-23% of students per year) and Amazon.com (14-19% of students per year.) The least common types of phishing email were other (4-5% of students per year), Nigerian scam (6-10% of students per year), and eBay (8-12% per year). The only increase during the study period was Amazon.com phishing email, an increase from 14% of respondents in 2011 to 16% in 2015. Overall, the percentage of students receiving phishing email decreased from 29% to 21% of students. Chart 1 graphically illustrates the trends for each type of phishing email.

Chart 1. Phishing Email Type and Behavior Trends



In terms of the quantity of messages received per month, volumes decreased for each type of phishing email with the exception of Nigerian scam phishing email (an increase from 10.5 per month in 2011 to 14.9 per month in 2015). There was no discernable pattern with respect to the highest and lowest volume types across the study years. Overall, however, the volume decreased from 15.6 per month in 2011 to 14.9 per month in 2015 and the percent of phishing email as a percentage of all email received decreased from 7.4% in 2011 to 6.7% in 2015.

An examination of behavior finds that few students, 2-4% per year, indicate responding to phishing email. Moreover, most have not been a victim of identity theft with only 5-7% per year indicating that he or she has been victimized. Relative to businesses in general, in which 85% of firms were victimized in 2015, students appears to be considerably less of a target and less victimized (Wombat, 2016). However, a sizable percentage of students (32-36% per year) report personal knowledge of at least one other victim of identity theft. Finally, an examination of those who have responded to a phishing email finds that gender and quantity of phishing email received had

significant correlations with phishing response behavior. Males, for example, were more likely relative to females to respond to a phishing email.

Implications

There are two important implications as a result of these findings:

1. One implication is that given there has been a dramatic decrease in the percentage of students receiving phishing emails, university implemented technological solutions may be improving and becoming increasingly effective in the war against phishing. It is possible that spam filters have assisted in not only the 28% decrease (from 29% to 21%) of students receiving phishing email but also in the 9% decrease (from 7.5% to 6.7%) in the volume of phishing emails as a percent of total email received. The only increase in student percentage occurred with regard to Amazon.com phishing but this may be a result of the 2015 Amazon.com attack discovered by Maywarebytes (Umawing, 2015). Another reason for the decrease in student attacks could be that students may not be a major target of phishers, given students' relative lack of financial resources. This theory, however, would be difficult to confirm without intimate knowledge of phishers. Overall, findings suggest that continued vigilance with regard to technological solutions may provide dividends not only in the academic community but in the business world. This is especially important given the much high victimization level found with respect to businesses (Wombat, 2016). As a result, this gap implies that businesses may be lagging behind universities in the anti-phishing technology battle and that businesses may have technological opportunities.

2. A second implication is with regard to student behavior. Although a relatively small percentage of students responded to phishing email and have been a victim of identity theft, the 50% increase (from 2% to 4%) of students responding to phishing emails during the five-year study period is mildly troubling. It is also possible that response and identity theft levels are under-reported because of embarrassment. Moreover, because nearly 8 of 10 respondents did not indicate receiving a phishing email, it is not possible to evaluate his or her behavior when a phishing email is received. As a result, although students are receiving ant-phishing instruction, educational techniques with regard to positive computing behavior may need to be improved However, because the vast majority of student behavior has been positive, the results imply that although there is room for improvement, students are likely prepared to face the current phishing challenges when entering the business world upon graduation. Based upon these findings, it is also possible that businesses may find similar behavior by implementing anti-phishing instruction with current employees, new employees, and, especially executives, given the new spear-phishing attacks.

The limitations of this study are primarily a function of the sample, sample distribution, and type of research. The use of additional universities and more equal distribution among academic class and gender would increase the robustness of results. Another limitation relates to the self-reported nature of the survey. Future research is needed to explore how gender affects behavior and to explore which measures in the education process may be most effective in promoting positive student email behavior. Overall, however, the study provides rich insight into the current state of academic phishing and potential benefits to industry.

REFERENCES

Alsharnouby, M. Alaca, F., & Chiasson S. (2015). Why Phishing Still Works: User Strategies for Combating Phishing Attacks. *International Journal of Human-Computer Studies*, October, 82, 69-82.

Associated Press. (2014). IRS: Identity Theft Prosecutions Doubled in 2013. *cnbc.com*, January 8. Available: http://www.cnbc.com/2014/01/08/irs-identity-theft-prosecutions-double-in-2013.html

Auby, K. (2010). How We Work: Communications Trends of Business Professionals. *Plantronics.com*¸ September. Available: https://www.plantronics.com/us/howwework/

Bickerton, M. (2015). Email: It's About Respect. Email Marketing White Paper 2015. *Raven5.agency*, March 14, 1-14. Available: http://www.raven5.agency/blog/email-its-about-respect

Case, C. J. & King, D. L. (2008). Phishing for Undergraduate Students. *Research in Higher Education Journal*, 1, 100-106.

Conover, W. J. (1999). *Practical Nonparametric Statistics*. Hoboken, NJ: Wiley.

Daily Mail Reporter (2012). How Smartphones and Tablets Are Adding Two Hours to Our Working Day. *The Daily Mail*, October 30. Available: http://www.dailymail.co.uk/sciencetech/article-2225325/Smartphones-tablets-add-TWO-HOURS-working-day.html

Huang, E. Y. & Lin, S. W. (2009). Do Knowledge Works Use E-Mail Wisely? *Journal of Computer Information Systems*, 50(1), Fall, 65-73.

IBM. (2013). The Future of Email and Applications Is Social. *idgconnect.com*, February 13, 1-12. Available: http://www.idgconnect.com/view_abstract/24320/the-future-of-email-and-applications-is-social

King, D. L. & Case, C. J. (2012). The Student's Decision Of Whether Or Not To Go Phishing. *Business Research Yearbook, Global Business Perspectives*, 19(1), 72-79.

Krebs, B. (2015). Massive 46M Dollar Cyberheist. *CyberheistNews*, August 12, 5(32), 1-6. Available: http://securenation.net/massive-46m-dollar-cyberheist

Kroll. (2016). Global Fraud Report 2015-2016. *kroll.com*, January, 1-86. Available: http://www.kroll.com/global-fraud-report

Lubold, G. & Paletta, D. (2015). Pentagon Sizing Up Email Hack of Its Brass. *The Wall Street Journal*, August 7. Available: http://www.wsj.com/articles/pentagon-sizing-up-email-hack-of-its-brass-1438989404

Mohammad, R. M., Thabtah, F. & McCluskey L. (2015). Tutorial and Critical Analysis of Phishing Websites Methods. *Computer Science Review*, August, 17, 1-24.

Murphy, C. (2013). Goodbye IT, Hello Digital Business. *Informationweek.com*, March 18, 1360, 14-25 Available: http://informationweek.com/1360/digital/

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The Design of Phishing Studies: Challenges for Researchers. *Computers & Security*, March 9. Available: http://www.sciencedirect.com/science/article/pii/S0167404815000231

Radicati, S. (2014). Email Statistics Report, 2014-2018. *radicati.com*, April, 1-5. Available: http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf

Sjouwerman, S. (2015).BitPay Losses 1.8 Million in Phishing Attack. *Knowbe4.com*, September 19. Available: https://blog.knowbe4.com/bitpay-loses-1.8-million-in-phishing-attack

Swapan, P. (2012.) Phishing Counter Measures and Their Effectiveness – Literature Review. *Information Management & Computer Security*, 20(5), 382 – 420.

Symantec. (2015).Web Security Threat Report Part 2 2015. *Symantec.com*, October 1, 1-35. Available: https://www.symantec.com/content/en/us/enterprise/white_papers/symantec-web-security-threat-report-2-en-us.pdf

Umawing, J. (2015). Fake Amazon UK Mail Asks You to Verify Account Number After "Breach.", *malwarebytes.org*, September 16. Available: https://blog.malwarebytes.org/fraud-scam/2015/09/fake-amazon-uk-mail-asks-you-to-verify-your-account-after-breach/

Webster, M. (2016). Phishing. *merriam-webster.com* .Available: http://www.merriam-webster.com/dictionary/phishing

Wombat. (2016). 2016 State of the Phish. *Wombatsecurity.com*, January. Available: http://info.wombatsecurity.com/hubfs/WombatThreatSim-StateofPhish2016_final_web.pdf?submissionGuid=fdf007cc-8a1e-40c0-8fc6-3ec167906965

Wombat. (2016). The Cost of Phishing and the Value of Employee Training. *informationweek.com*, January 7. Available: http://www.informationweek.com/whitepaper/risk-management-security/security-monitoring/ponemon-cost-of-phishing-and-value-of-employee-training/372083?gset=yes&