Exploring Millennials' Malware Awareness and Intention to Comply with Information Security Policy

Review of Integrative Business & Economics Research

Kamphol Wipawayangkool*
College of Business Administration
Sam Houston State University

Eric Villafranca
College of Business Administration
Sam Houston State University

ABSTRACT

Despite the importance of security awareness, our understanding of its nature is limited, because its operationalization in extant research has mostly been too broad. This paper develops a construct of malware awareness, a specific aspect of security awareness, by focusing on the awareness of viruses, worms, Trojans, phishing, and spamming. This paper then explores the effects of the malware awareness along with security measure self-efficacy and attitude on intention to comply with information security policy. By using data collected from the millennials, or generation Y, who are about to enter the workforce, we found that only the phishing and spamming awareness and attitude toward security measures are significant predictors of intention to comply. Implications and future research directions are discussed.

Keywords: Information Security, Security Awareness, Malware, Millennials

1. INTRODUCTION

One of the crucial components in information security management is security awareness (Siponen 2000; von Solms 2001). According to the Information Security Forum (ISF) (2005), security awareness is defined as the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly. Both researchers and practitioners have come to acknowledge that security awareness is fundamental to effective and successful information security management and that investing in security awareness improvement rather than technology can be more cost effective (Jones 2007; Kelly 2006). Nonetheless, our understanding of the nature of security awareness is limited, because behavioral aspect of security awareness is being understudied and its conceptualization and operationalization in extant research have mostly been too broad (Siponen 2000). Another concern among information security managers is the arrival of the millennials or generation Y to the workforce and studies on their security-related perceptions and behaviors are lacking.

To fill such gaps, this paper proposes a specific aspect of security awareness, namely malware awareness by exclusively focusing on the awareness of viruses, worms, Trojans, phishing, and spamming. Using data collected from the millennials, this paper then explores the influence of their malware awareness along with security measure

ISSN: 2304-1013 (Online); 2304-1269 (CDROM)

self-efficacy and attitude on their intention to comply with information security policy. This paper is organized as follows. The next section provides background of malware, namely, viruses, worms, Trojans, phishing, and spamming. Methodology and analysis are then presented. Finally, the findings, limitations, and future research directions of the study are discussed.

2. MALWARE

2.1 Viruses

A computer virus is a program whose purpose is to cause damage, steal data, take control, and/or to spread to other software. Like biological ones, computer viruses enter a host through a carrier and then spread throughout the system by attaching to a file, or an executable one, and wait for the victim to launch the host program (Subramanya and Lakshminarasimhan, 2001). Originally, attackers attached viruses to floppy disks, which was slow and inefficient because it required users to spread it by sharing disks. Then, viruses become capable of attaching themselves to macros such as those to automate tasks in Microsoft Office. As macros can perform other actions outside of the program, an attacker can cause damage with code that runs in the background. The threat of macro viruses is still present, but with the Internet, downloadable viruses are an even greater threat (Heiser, 2004).

As the first line of defense, anti-virus software performs variety of detection techniques such as signature-based scanning, emulation, sandboxing, behavioral analysis, and check-sums. The most popular method is signature-based scanning, where the software scans the system searching for code unique to known viruses, also known as signatures (Dezfouli et al., 2013). Emulation method launches software in a virtual environment known as a sandbox where a virus cannot spread to the rest of the system. If it finds a virus, it will quarantine the carrier and then remove the malicious code (Chang et al., 2013). Behavioral analysis allows the user to accept or decline any changes that the software attempts to perform (Ahmadi et al., 2013), allowing the user to stop the virus from executing in real-time. This method reduces false positives, which is the quarantining of legitimate software because it resembles the signature of a virus. If the user recognizes the program as legitimate, they can accept it (Bontchev, 1997). Finally, a check sum scans system files and makes note of the number of bits that they contain. This data is stored, and then compared to new counts later. Any inconsistencies are indicative of the presence of a virus. Effective anti-virus software performs a combination of the techniques with little degradation of the system performance (Nance, 2010).

2.2 Worms

Unlike a computer virus, a worm does not require a host file and can spread itself (Ochieng et al., 2014, Qing and Wen, 2004). Passive worms spread by infecting shared files such as those in P2P networks. Unsuspecting users download these shared files and infect their local system. The worm will then duplicate itself into the shared folder of the new victim, awaiting another download. Passive worms propagate very slowly but are dangerously stealthy because they avoid traditional virus signature detection (Wang et al., 2009). On the other hand, active worms infect systems by exploiting vulnerabilities using discovery techniques. The worm scans a range of addresses to find

ISSN: 2304-1013 (Online); 2304-1269 (CDROM)

a vulnerable host and then copy itself to it, allowing it to spread rapidly, or uses a pre-generated list, or "hit list" input by the worm's creator. It can also develop an internal hit list by searching victim systems for addresses and relationships with their communication partners, which usually share the same vulnerabilities. Some worms perform all of these discovery techniques, making them very intelligent and very hard to stop (Fan and Xiang, 2010).

One of the first known worms, named Charisma, infected computers in 1987; as victims opened the email to see a Christmas tree picture, the worm resent itself to every person in the victims' contact list, causing slowness in connectivity due to the amount of traffic that it generated (Heiser, 2004). In 2003, a worm known as SQLSlammer was able to double the number of infected systems every 8.5 seconds. Within 10 minutes of the first infection, over 90% of systems that had a certain SQL vulnerability on Windows systems were infected. It was extremely hard to eliminate the worm, because not all systems were online at the same time and all it took was one infected system to re-infect all the others (Panko, 2003).

As worms have the properties of viruses, with the additional capability of self-propagation, anti-virus software can be a first line of defense (Ochieng et al., 2014). Anti-virus software combined with a firewall on both the local system and the network is a better protection (Rehman et al., 2011). While too many layers can produce false positives, or the filtering of legitimate network traffic, the risk is worth the repercussions. Honeypots are also a good protection against worms. Honeypots try to discover worms by luring them in a secure environment. They minimize false positives by adding to the knowledge base of anti-virus software (Shyamasundar, 2015).

2.3 Trojans

Similar to the Trojan horse in Greek mythology, a computer Trojan disguises itself as a legitimate program but in fact carries a harmful payload. Anti-virus software does not automatically detect Trojans because they may also perform legitimate functions (Emm, 2006). There are several types of Trojans. Remote Access Trojans provide the attacker full administrative control over the victim's system. Data Sending Trojans look for sensitive information on the victim's system, or even install Keyloggers that can capture passwords or sensitive information. Destructive Trojans delete files like a virus, but they go undetected and do not spread to other systems like viruses. File Transport Protocol (FTP) Trojans open port 21 (FTP port) on the victim system and allows the attacker to store and retrieve illegal software. Finally, Security Software Disabler Trojans disable the victim's anti-virus software and allow other malware to infect the system (Saini et al., 2011).

Early Trojans propagated slowly because they infected other systems by chance when clueless victims passed them around on floppy disks. The Internet brought the development of Trojans that steal passwords and other confidential information online. Attackers hid Trojans in freeware and waited for victims to download it from their website. Hackers also target specific systems that they know contain information that will lead to financial gain or chaos (Kello, 2013, Manky, 2013, Sunner, 2007).

Trojans are evasive but are not immune to detection. Once a system is infected, the anti-virus software finds the culprit and saves the Trojan's signature. Therefore, a good defense is to keep the anti-virus software's signature database up to date. In addition, users should only download software from trusted websites. New anti-virus software

ISSN: 2304-1013 (Online); 2304-1269 (CDROM)

also use honeypots to launch Trojans in a virtual environment where it will not harm the system (Shyamasundar, 2015).

2.4 Phishing

Phishing is attackers' attempt to steal data or redirect users to a malicious website by imitating a legitimate identity. It gets its name from the activity of fishing, in which a person casts a baited line into water and waits for a fish to bite before reeling it in. In this case, the line is the internet and the bait is a spoofed email message or website (Luo et al., 2012, Orman, 2013).

In a phishing attack, hackers will create a fake website that imitates a legitimate one and then send the users an email that appears to be from a legitimate source. The email then uses the concept of social engineering to make the victim click on a link that takes them to the fake website to enter the username and password that they use on the legitimate site and/or ask the victim to update their information such as bank account number and social security number. The attackers will use this data to steal the victim's identity, or they will sell the data on illegal underground markets. The latter method allows the attacker to mitigate their risk because the data is now out of their hands (Banday, and Qadri, 2007).

It can be difficult to discern a faked email and website from the actual ones. The user could call to verify the email with the legitimate company. The user could also just exit the email application and visit the company website through a known and trusted Uniform Resource Locator (URL). Another method is to hover the mouse pointer over the links in these phishing emails as doing so will show where the link will actually take the user (Orman, 2013).

2.5 Spamming

Spam is unsolicited bulk emails along with their undesirable online communication. Attackers normally send them to victims with other forms of malware such as botnets (Rao and Reiley, 2012). Spam gets its name from the canned meat product of the same name manufactured by Hormel Corp. A comedy sketch called Monty Python's Flying Circus came out in 1970 that featured Spam. As the sketch progressed, the actors used the word Spam more often, and it soon became so pervasive that it was essentially the only spoken and written word remaining. This same concept applies to email spam as it is so overbearing the victim will end up with a mailbox full of spam and nothing else (Steyerl, 2011).

The first known person to send out spam is Gary Thuerk of Arpanet, who sent out a mass email to invite people to an Arpanet presentation in 1978. Two attorneys, Laurence Canter and Martha Siegel developed modern spamming in 1994 by hiring programmers to send out mass email advertisements to help immigrants receive green cards. By 2003, spam traffic had reached a staggering 85% of all email traffic and caused over 500 million dollars in damage (Rafiee et al., 2012).

In 2003, the United States passed The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) into law, which requires several things for an unsolicited advertising email to be legal. First, it must have a valid return address. Then, it must offer an opt-out option. Finally, it must identify itself as advertising explicitly in the subject line of the email. There is no evidence that this law has any impact on the amount of Spam, but it is a step in the right direction. In addition,

ISSN: 2304-1013 (Online); 2304-1269 (CDROM)

researchers have begun suggesting that legislation make it illegal for banks to process transactions made by spammers, making it harder for them to make a profit and reducing the amount of Spam traffic (Arutyunov, 2013).

3. METHOD

The survey was announced and administered online to undergraduate students in a course at a public university in the southwest U.S. Students who chose to participated received extra credit in the course. 78 out of 122 requests were completed without any missing data, yielding a response rate of 64%. Male students accounted for 70% of the respondents, while female students 30%. Approximately 14% of the respondents were 20 years old and below, 83% were between 21 and 30, and 3% were between 31 and 40. About 32% had high school diploma, 53% associate's degrees, and 13% bachelor's degree, and 3% others. The age demographics data show that the sample was indeed the millennials which were the target group of the study.

The survey items for malware awareness were newly developed in this study (10 items), while those for intention to comply (3 items) and attitude toward security measures (3 items) were adapted from Bulgurcu et al. (2010), and those for security measure self-efficacy (4 items) were adapted from Anderson and Agarwal (2010). All the items were seven-point Likert-type scales anchored from strongly disagree (1) to strongly agree (7). All Cronbach's alphas exceeded 0.8, exhibiting reliability of all the measures (Nunnally, 1978). Control variables included gender, age, highest education obtained, and academic classification. Table 1 showed descriptive statistics, reliability, and correlations.

Table 1. Descriptive statistics, reliability, and correlations

	Mean (SD)	Alpha	VWT	PHSP	ATT	SE	COM
VWT	4.38 (1.68)	0.93	1				
PHSP	5.65 (1.21)	0.95	.691**	1			
ATT	6.46 (0.91)	0.93	.291**	.467**	1		
SE	5.62 (1.15)	0.88	.675**	.580**	.613**	1	
COM	6.01 (0.99)	0.97	.412**	.561**	.586**	.552**	1

Notes. N = 78. ** Significant at the 0.01 level (2-tailed). SD = Standard Deviation, Alpha = Cronbach's Alpha, VWT = Virus, Worm, and Trojan Awareness, PHSP = Phishing and Spamming Awareness, ATT = Attitude toward Security Measures, SE = Security Measure Self-Efficacy, COM = Intention to Comply.

Multiple regression analysis was then performed to determine whether the virus, worm, Trojan awareness, the phishing and spamming awareness, security measure self-efficacy, and attitude toward security measures were significantly associated with intention to comply with information security policy. Control variables were first entered and only age was found to be significant ($b = 0.62$, $p < 0.05$). Subsequently, the overall model that included all the proposed independent variables significantly explained about 41% of the variance in intention to comply ($F = 13.32$, $p < 0.05$). The phishing and spamming awareness ($b = 0.26$, $p < 0.05$) and attitude toward security measures ($b = 0.37$, $p < 0.05$) were found to be the only significant predictors of intention to comply.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM)

4. DISCUSSION

The findings expectedly suggest that the millennials are more likely to comply with information security policy of the organization as they get older and have positive attitude toward security measures. Interestingly, they are likely to comply if they are more aware of the concepts of phishing and spamming, not those of viruses, worms, and Trojans. This implies that while knowing the nature of the more relatively technical types of malware such as viruses, worms, and Trojans does not lead to the millennials' intention to comply, the awareness of the phishing and spamming does. To that end, it could be interpreted that rather than bombarding the millennials with technicalities of malware, managers should provide security training with the focus of a more social-engineering, practical side of malware such as phishing and spamming in order to ensure their compliance to the security policy. The result also hinted that improving the millennials' attitude toward security measures may even be a more slightly effective approach.

Due to the exploratory nature of this study, the findings should be interpreted with caveats and further studies are warranted. Particularly, studies with a larger sample size and a confirmatory set of hypotheses are crucial to ensure the validity of the analysis results in this study. Common method variance is also needed to be mitigated through either statistical techniques or research design or both. The classification of malware in this study could also be subject to change depending on the theory of future research. Future researchers could expand our research model by including more constructs such as tendency to violate information security policy.

APPENDIX

Table A. Survey Items

Virus, Worm, and Trojan Awareness
I know how viruses, worms, and Trojans are different and the damages they can cause.
I can recognize different symptoms of viruses, worms, and Trojans.
I can identify whether a system is infected with either viruses, worms, or Trojans
I have sufficient knowledge of the potential threats and negative consequences of viruses, worms, and Trojans.
Phishing and Spamming Awareness
I know what phishing is and the damages it can cause.
I know what spamming is and the damages it can cause.
I can tell if an email or a web site is a phishing one.
I can tell if an email or an advertisement is a spamming one.
I have sufficient knowledge of the potential threats and negative consequences of phishing emails and web sites.
I have sufficient knowledge of the potential threats and negative consequences of spamming emails and advertisements.
*Attitude toward Security Measures **
To me, security measures are necessary.
Taking security measures to protect my personal computer is important.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM)

I like the idea of taking security measures to secure my personal computer.
*Security Measure Self-Efficacy **
I feel comfortable taking security measures to secure my primary personal computer.
I have the resources and the knowledge to take the necessary security measures.
Taking the necessary security measures is easy to me.
Taking the necessary security measures is entirely under my control.
*Intention to Comply ***
I intend to comply with the requirements of the information security policy of my organization in the future.
I intend to protect IT resources according to the information security policy of my organization in the future.
I intend to follow the information security policy of my organization in the future.

Notes. * Items preceded by "For the following statements, the term "security measures" refers to individual actions such as running and updating security software, keeping passwords secure, running a firewall, enabling encryption for home wireless network, etc."

** Items preceded by "For the following statements, the term "organization" refers to the university you currently attend. Typical information in a security policy includes: Do not use someone else's computer account, Do not share your computer account and password, Do not attempt to access any data or programs for which you have no authorization, Do not make unauthorized copies of copyrighted material, and Do not access, create, store, or transmit offensive or indecent material."

REFERENCES

[1] Ahmadi, M., Ashkan, S., Rahimi, H., Yadegari, B. (2013), "Malware Detection by Behavioural Sequential Patterns", *Computer Fraud & Security*, 8, 11-19.

[2] Arutyunov, V. (2013), "Spam: Its Past, Present, and Future", *Scientific and Technical Information Processing*, 40(4), 205-211.

[3] Banday, M., Qadri, J. (2007), "Phishing- A Growing Threat to E-Commerce", *The Business Review*, 12(2), 76-83.

[4] Bontchev, V. (1997), "Future Trends in Virus Writing", *International Review of Law Computers & Technology*, 11(1), 129-146.

[5] Chang, J., Venkatasubramanian, K., West, A., Lee, I. (2013), "Analyzing and Defending Against Web-Based Malware", *ACM Computing Surveys*, 45(4), Article 49.

[6] Corrons, L., Hoskins, D. (2008), "Exploring MBR Rootkits", *Network Security*, 3, 7-9.

[7] Dezfouli, F., Dehghantanha, A., Mahmood, R., Binti, N., Sani, M., Shamsuddin, S., Daryabar, F. (2013), "A Survey on Malware Analysis and Detection Techniques", *International Journal of Advancements in Computing Technology*, 5(14), 42-51.

[8] Eisenberg, T., Gries, D., Hartmanis, J., Holcomb, D., Lynn, M., Santoro, T. (1989), "The Cornell Commission: On Morris and the Worm", *Communications of the ACM*, 32(6), 706-710.

[9] Emm, D. (2006), "Focus on Trojans- Holding Data to Ransom", *Network Security*, 6, 4-7.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM)

[10] Fan, X., Xiang, Y. (2010), "Defending Against the Propagation of Active Worms", *Journal of Supercomputing*, 51, 167-200.
[11] Gunasekhar, T., Rao, K., Saikiran, P., Laksmi, P. (2014), "A Survey on Denial of Service Attacks", *International Journal of Computer Science and Information Technologies*, 5(2), 2373-2376.
[12] Heasman, J. (2006), "Rootkit Threats", *Network Security*, 1, 18-19.
[13] Heiser, J. (2004), "Understanding Today's Malware", *Information Security Technical Report*, 9(2), 47-64.
[14] Johnston, A., Schmidt, M., Arnett, K., Thomas J. (2007), "Getting to the Root of the Problem", *Journal of Internet Commerce*, 6(1), 1-12.
[15] Jones, D. (2007), "Low Cost Security Tools: Employee Awareness", *Security*, November, 90-91.
[16] Karim, A., Salleh, R., Shiraz, M., Shah, S., Awan, I., Anuar, N. (2014), "Review: Botnet Detection Techniques: Review, Future Trends, and Issues", *Journal of Zheijang University- SCIENCE C (Computers & Electronics)*, 15(11), 943-983.
[17] Kello, L. (2013), "The Meaning of the Cyber Revolution- Perils to Theory and Statecraft", *International Security*, 38(2), 7-40.
[18] Kelly, C.J. (2006), "Awareness Trumps New Security Toys", *Computerworld*, October, 44.
[19] Land, M. (2009), "The Methods of Windows Rootkits", *Journal of Applied Security Research*, 4, 389-426.
[20] Lerner, Z. (2014), "Microsoft the Bot Hunter: The Role of Public-Private Partnerships in Mitigating Botnets", *Harvard Journal of Law & Technology*, 28(1), 237-261.
[21] Levin, J., Grizzard, L., Owen, H. (2006), "Detecting and Categorizing Kernel-Level Rootkits to Aid Future Detection", *IEEE Security & Privacy*, 4(1), 24-32.
[22] Luo, X., Zhang, W., Burd, S., Seazzu, A. (2012), "Investigating Phishing Victimization with the Heuristic-Systematic Model: A Theoretical Framework and an Exploration", *Computers & Security*, 38, 28-38.
[23] Manky, D. (2013), "Cybercrime as a Service: A Very Modern Business", *Computer Fraud & Security*, 6, 9-13.
[24] Nance, B. (2010), "How to Fight Malware", *NetworkWorld Asia*, 6(1), 38-41.
[25] Nunnally, JC. (1978), Psychometric Theory. McGraw-Hill, New York.
[26] Orman, H. (2013), "The Compleat Story of Phish", *IEEE Internet Computing*, 17(1), 87-91.
[27] Panko, R. (2003), "Slammer: The First Blitz Worm", *Communications of the Association for Information Systems*, 11, 207-218
[28] Ochieng, N., Mwangi, W., Ateya, I. (2014), "A Tour of the Computer Worm Detection Space", *International Journal of Computer Applications*, 104(1), 29-33.
[29] Qing, S., Wen, W. (2004), "A Survey and Trends on Internet Worms", *Computers & Security*, 24, 334-346.
[30] Rafiee, H., Von Lowis, M., Meinel, C. (2012), "IPv6 Deployment and Spam Challenges", *IEEE Internet Computing*, 16(6), 22-29.
[31] Rao, J., Reiley, D. (2012), "The Economics of Spam", *Journal of Economic Perspectives*, 26(3), 87-110.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM)

[32] Rehman, R., Hazarika, G.C., Chetia, G. (2011), "Malware Threats and Mitigation Strategies: A Survey", *Journal of Theoretical and Applied Information Technology*, 29(2), 69-73.
[33] Ring, S., Cole E. (2004), "Taking a Lesson from Stealthy Rootkits", *IEEE Security and Privacy*, 2(4), 38-45.
[34] Saini, H., Mishra, S., Sahoo, P. (2011), "Defense Against Trojans Using Honeypots", *IUP Journal of Science and Technology*, 7(3), 49-61.
[35] Shyamasundar, L. (2015), "An Autoconfigured Hybrid Honeypot for Improving Security in Computer Systems", *International Journal of Computer Science and Information Technologies*, 6(1), 84-88.
[36] Silva, S., Silva, R., Pinto, R., Salles, R. (2012), "Botnets: A Survey", *Computer Networks*, 57, 378-403.
[37] Siponen, M.T. (2000), "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, 8(1), 31-41.
[38] Spafford, E. (1989), "Crisis and Aftermath", *Communications of the ACM*, 32(6), 678-687.
[39] Steyerl, H. (2011), "Digital Debris: Spam and Scam", *October*, 138, 71-80.
[40] Subramanya, S.R., Lakshminarasimhan, N. (2001), "Computer Viruses", *Potentials, IEEE*, 20(4), 16-19.
[41] Sunner, M. (2007), "Targeted Malware: The Rise of Targeted Trojans", *Network Security*, 12, 4-7.
[42] Von Solms, B. (2001), "Information Security – A Multidimensional Discipline", *Computer & Security*, 20, 504-508.
[43] Wang, F., Zhang, Y., Ma, J. (2009), "Defending Passive Worms in Unstructured P2P Networks Based on Healthy File Dissemination", *Computers & Security*, 28(7), 628-636.

ISSN: 2304-1013 (Online); 2304-1269 (CDROM)