IBIMA Publishing
Journal of Internet and e-Business Studies
http://www.ibimapublishing.com/journals/JIEBS/jiebs.html
Vol. 2012 (2012), Article ID 936368, 10 pages
DOI: 10.5171/2012.936368

Investigating Email Users Behavior against Spam: A Proposed Theoretical Framework

Yanti Rosmunie Bujang and Husnayati Hussin

Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, Malaysia.

Abstract

Spam is the most common problem faced by email users today when they communicate via the Internet or mobile technology. Despite numerous efforts taken, the battle to contain this problem still goes on. This paper describes a proposed model which focuses on the behavior of email users in avoiding spam while using this popular channel of communication. Based on the Technology Threat Avoidance Theory (TTAT), the model is enhanced by incorporating the ethics perspectives. The enhanced research model is hoped to be able to explain the email users' behavior in avoiding the spam email as a threat. Several factors have been identified as possibly influencing the behavior of email users, including perceived severity, perceived susceptibility, safeguard effectiveness, safeguard cost, self-efficacy and IT ethics. Although yet to be tested, it is anticipated that a study adopting the proposed model will contribute towards providing the knowledge to the ISP or ESP, decision maker and individual user to handle the spam problem more effectively in addition to the existing approaches.

Keywords: spam, TTAT, email user and behavior.

Introduction

Spam is a well known problem in email communication. It not only exists in email but also in other channels of communication such as short messaging services, over telephone (spit) and blog (splog). Two acronyms that were related to spam definition are UCE (Unsolicited Commercial E-mail) (Spam Act, 2003) and UBE (Unsolicited Bulk E-mail). The rapid evolution of communication methods makes the spammer become more creative and innovative to spread the spam email. This makes the effort to control the spam email very challenging.

Recent statistics by MessageLabs (MessageLabs Intelligence, 2011) indicate that the global ratio of spam rate in email traffic is 79.3%, which means 1 spam in 1.26 emails. It seems the spam rate is almost similar to the legitimate email traffic; this could be because of the difficulties faced by the anti-spam technology to identify the spam characteristics due to the fast evolution of spam. In fact, the technology must be a step ahead of the spammer technology to ensure that spam can be eliminated successfully but today, this is still an ongoing battle.

This paper attempts to highlight another perspective on spam problem, which is often being overlooked by most researchers, that is the behavior of email users in handling spam email based on Technology Threat Avoidance Theory (TTAT). The proposed theory is used to understand the spam threat avoidance behaviors among email users personally. The

 Contact author: Yanti Rosmunie Bujang E-mail: yrosmunie@yahoo.com

findings would be useful in providing knowledge to improve and complement other approaches in handling spam problem.

Spam Problem

Emails are considered to be one of the popular channels for marketing products and services. Email is preferred more than regular mail because it has lower distribution costs, wider reach, convenience and faster responses (Martin, Van, Raulas, & Merisavo, 2003). Despite the benefits to the advertising campaigns, emails are not favorably received by the consumers, email providers and the organizations. Many users are angry and frustrated because they have to sift thousands of unsolicited commercial emails annually. Email providers struggle to maintain quality service in the face of increasing server load, storage requirements and security threats. Organizations are burdened with financial and intangible costs of spam and managers struggle to find solution to spam problem (Corbitt, 2004).

Aside from the commercial perspective, email as the most popular type of medium of communication on the Internet has a hidden threat to the email users. Through spam emails, virus and malware can converge to produce a sophisticated attack which might cause serious damage to private email users and to organizations.

Most researchers focused on the technology effectiveness to combat spam. However, the volume of spam email has continued to grow creating an enormous burden on email service providers (ESPs), organizations and end users. These anti-spam measures could not stop spam as expected. The main reason is the continuous advancement of spam. Thus, there are still other factors that need to be considered to combat spam successfully.

Anti-Spam Measures and Issues

There are many solutions that have been proposed and implemented to control the spam problem. These measures include technological solution, introducing legislation and development of e-policies by organizations.

The most common approach today is by using the technological solution. As usual, every anti-spam technology company would claim their technology or tools are more effective than the others. This battle will never end since this is a kind of business competition. These companies must compete with one another, the best of which will gain better trust from email users. The existence of spam is caused by people, therefore only people can solve the problem by changing the technology or the email users' behavior. Due to the increasing number of cyber crime recently, the behavior of email user must change to fit with the security requirements accordingly.

The second approach is by introducing laws and regulations in the country. The main issue with enforcing the anti-spam legislation is the jurisdiction where the spammers can evade. If they are banned by a specific country, they will move to another country which does not have any spam laws. The other issue is that, not all countries have spam laws and even if they have, sometimes it is not comprehensive to cover all the spammer activities because spammers are very creative and they have high motivation to pursue their goals.

Due to this problem, researchers now focus more on the human aspect as an alternative solution to the technology security problem. Many researchers have realized that they have to find an alternative solution rather than focus on the technology solution only. Therefore, they have changed their direction of technology security to the human aspect (Anderson & Agarwal, 2006; Ng, Kankanhalli, & Xu, 2009; Woon, Tan, & Low, 2005; Workman, Bommer, & Straub, 2008). However, the knowledge is yet far from complete (Liang & Xue, 2010). This paper attempts to highlight the user behavior's perspective as a complementary approach in handling spam problem, that is, by providing

some understanding of the email recipients' behavior on spam emails. The information will be helpful to develop anti-spam technological measures tailored to the need of the email users and useful for the decision maker to enforce any rules and regulations to protect the email users right on email usage.

Theoretical Perspectives

Two theories are considered in this paper as they are viewed as relevant to understanding users' behavior towards spam. These theories are Technology Threat Avoidance Theory and Coping Model of User Adaptation (CMUA) Theory, which are reviewed briefly in the following sub-sections.

Technology Threat Avoidance Theory (TTAT)

TTAT was introduced by Liang & Xue (2009) and still considered to be at an infancy stage. The theory was tested to the spyware problem among students. In general, TTAT provides a framework in explaining the cognitive processes people use to appraise threat, seek solutions and ultimately avoid IT threats by adopting safeguarding measures (Liang & Xue, 2009). The theory is able to explain individuals' behavior in avoiding the threat of malicious information technology. Spam emails, though some considered not malicious, are still considered unwanted emails and a nuisance to many people, hence will be investigated further based on the theory.

In TTAT, the difference between malicious and virtuous IT is based on the designer intention and user perception. The authors define malicious IT as computer programs designed to make system dysfunction or security and privacy breaches such as viruses, worms and spyware; whereas virtuous IT is a computer system designed to provide communicational, computational or decisional aids to users to increase their performance.

TTAT can be used to investigate the users' threat perceptions. In addition, adoption of safeguarding IT is only a part of the malicious IT avoidance behavior. In IT security practices the ultimate goal is to avoid threat rather than to adopt a specific safeguarding IT (Liang & Xue, 2009). Hence, this theory focuses on the avoidance behavior rather than technology acceptance. The author has articulated that avoidance and adoption are two qualitatively different phenomena and contend that technology acceptance theories provide a valuable, but incomplete understanding of the user. Therefore, to get a better understanding of the user, there is a need to consider avoidance behavior in this research model.

In this theory, there are two options to manage the threat which is defined as the coping process. According to Lazarus and Folkman (1984), there are two types of coping that can be performed to deal with the threat; namely, problem-focused and emotion-focused. Problem focused coping is using safeguarding measures in terms of effectiveness, costs and user self-efficacy. However, if malicious IT is still not reduced, then the user will perform emotion-focused coping (Liang & Xue, 2009).

Coping Model of User Adaptation (CMUA) Theory

In CMUA, user adaptation is triggered by a significant IT event that disrupts the users work environment. It begins when the user gains an awareness of the potential consequences of significant IT events (Beaudry & Pinsonneault, 2005). Then they evaluate them to be of personal and/or professional relevance, and to be important as an opportunity or a threat (Folkman, 1992; Griffith, 1999). They found that in a threatening IT event, individuals' choice of problem or emotion-focused coping depends on their perceived control over self, work and technology.

In the coping process, two processes have been identified that continuously influence each other. The first process is individual evaluation on the potential consequences and event (appraisal). Secondly, individual performs different action to deal with the situation at hand (coping efforts). In worst cases, when the expected consequences are perceived as unavoidable, individuals might withdraw from the situation such as by asking for a transfer, quitting a job or retiring (Begley, 1998).

Proposed Research Model

TTAT is selected as the core research model because of its ability to explain voluntary security behavior in a non-work setting, where IT security is not mandated and is appropriate to investigate individual computer users' IT behavior (Liang & Xue, 2010). Each identified variable is discussed further according to the need of the study.

The basic concept of the study is email users' awareness of the threat caused by spam (experienced spam attack in the inbox), then how they react to the spam email: whether to perform problem-focused coping (adopt anti-spam measures) or emotion-focused coping (avoiding any anti-spam measures). The users will perform emotion-focused coping when their trust in the anti-spam measures is low which means they do not trust anti-spam technology to control spam entering their inbox. However, there are also several factors need to be considered which might influence the user's behavior.

Problem-Focused Coping

Problem-focused coping is chosen when email users feel they can avoid spam email and control the situation, which means they believe they can reduce the number of spam email entering their inbox. It could include the following actions:

- Install anti-spam software on their personal computers – There are many options of anti-spam software which sometimes come in package with other anti-virus software. For an individual user, this is quite difficult to invest. This option becomes more unattractive if they believe spam filtering by ESP is good enough to control the spam.

- Activate their spam filtering for their email account – Usually this application is provided by ESP by default, such as commercial email or email account provided by the organization.

- Move identified spam email to the spam folder – Most ESPs have provided spam filtering to each email user account. The email users are encouraged to move any spam emails to this folder because in future the emails will be quarantined automatically. However, the email users are encouraged to check this folder sometimes in case false positive happens when the legitimate email is classified as spam email. The possibilities of losing important emails might happen if they ignore the spam folder.

- Report spam cases to the ESP/ISP or related agencies – However, it is a fact that most email users do not know how to lodge a report on spam. This is the case in Malaysia, for example, where only 7.7% of email users reported spam cases (Bujang & Hussin, 2010). This is despite the fact that in Malaysia, there is a Cyber 999 hotline provided by MyCERT (Malaysia Computer Emergency Response Team) a unit under NISER (National ICT Security and Emergency Response Centre) to handle spam cases.

- More cautious to publish email address on the Internet – As mentioned in past research papers, some spammers get the email address from any website that has published email address such as blogs and social networks. According to Emma Barnetta as reported in The Telegraph online (Barnetta, 2011), 67% of social networks users have been attacked by spam in 2010. In addition, the spammers

switch to the social networks because people less aware on spam email find that it is sent from 'friend' in social networks, such as Facebook.

- Prefer to delete spam email manually – This option normally will be the choice of those who have no trust in the technology. The risk entailed is email users might accidentally delete the legitimate email which is known as false positive (Leung, 2003) and it causes more problem if it was an important email.

- Apply more ethical manners in using email – Ethically, a user should not easily forward any email to all contacts listed in their address book without considering whether the recipients have an interest in the content. Unfortunately, according to Leung (2003) this method also has been abused by some spammers: by responding to the email, thus inferring the email account is active and the users will become a victim in the future. Similar to the unsubscribe option for the email recipients, when they reply with unsubscribe request it shows their account is active and those email users have opened their spam email.

- More ethical while on the Internet – It depends on the users' trust in the Internet and the decision is various among Internet users. Some people do not mind publishing their email address on the Internet; others refrain from doing so. In fact, some marketers harvest email address from the websites, newsgroups and chat rooms (Leung, 2003), and social networks: the most popular recently. Thus, limiting the publication of email address on the Internet might help in reducing the spam problem.

The above list is not exhaustive. As long as the effort done is to control spam emails, it could be considered as part of problem-focused coping.

Emotion-Focused Coping

Emotion-focused coping will be performed when individuals feel that they could neither avoid nor control the situation. This includes self-deception and avoidance (Beaudry & Pinsonneault, 2005) when using the technology. The tendency is more towards those who have no knowledge about the technology to fight spam, ultimately they will decide to just let it happen as it is. Some options they might choose are as follows:

- Terminate their existing email account and register a new email account – This is for those who have no idea about what to do to reduce spam emails and give up on hundreds of spam emails in their inbox. This method is easy for those who find no significance in email communication, but impossible for individuals, who depend on email application for official purposes. This is a temporary solution only because the new email account also has a great opportunity to be spammed as well.

- Avoid using email frequently – This option is also for email users who do not consider email a significant channel of communication. This makes sense for short-distance communication but not for long-distance because of the high cost of telephone charges.

- Do not lodge a report for any spam cases – The email users believe although they report spam email, this would not reduce them in their inbox. They feel there will be no action taken by the responsible party. It is worse if there is no legislation to protect them from spam attack.

- Do nothing with the spam email – Obviously, this option means the email users do not have any knowledge about the hazard of spam email and they might respond to the spam email.

The study also attempts to investigate the factors that influence each coping method. The following sub section discusses the proposed factors that are postulated to influence the spam email coping behavior.

Factors Influencing Coping Behaviour

Several factors are included in the proposed model, which include perceived threat and perceived avoidability. Perceived avoidability is included to test whether it mediates users' appraisal of all aspects of the safeguarding measures. Two antecedents for perceived threat are perceived severity and perceived susceptibility, and three antecedents for perceived avoidability are safeguard effectiveness, safeguard cost and self-efficacy.

Perceived severity is defined as the extent to which an individual perceives that negative consequences caused by malicious IT are severe (Liang & Xue, 2009). When the users believe that they will be attacked by malicious IT and the consequences of being attacked is serious, then they will perceive it as a threat. If the user fails to consider either one, it may lead to a misunderstanding of the threat perception. According to Gurung et al. (2009), perceived severity refers to the individual's perception regarding the magnitude of the consequences. In the past research of IT security, perceived severity has shown consistent results. Perceived severity does predict whether individuals will enable their home wireless network security (Woon et al., 2005), adoption of anti-spyware tools (Gurung et al., 2009), spyware threat (Liang & Xue, 2010; Workman et al., 2008) and information security behavior (Workman et al., 2008).

In TTAT, perceived avoidability is more towards the characteristics of the anti-spam measures. It refers to the effectiveness of the anti-spam measures in controlling spam, the cost of anti-spam measures and the usability of the anti-spam measures.

The model also include IT ethics as a possible factor that influence problem-focused coping. This is because some deemed spam as caused by unethical use of email and Internet technology, either for purely personal interest or excessive commercial gains. In information society, interest of public should be given priority over personal interest which means interest of the society comes before the interests of individuals. IT ethics and morality is the issues of inappropriate, illegal and unethical use of computers (Lee & Kozar, 2008). However, only little attention has been given to empirical studies on computer ethics and moral issues associated with IT (Conger & Loch, 1995) . Hence, more work is required to help explain and minimize unethical IT behavior (Lee & Kozar, 2008).

Research Propositions

For the research context, if the email users become aware of the negative effect of spam, they will perceive it as a threat. Thus, the awareness of the consequences of spam email is very important to determining how the email users view it. Different individuals have different perceptions of those consequences among different malicious IT. Hence, perceived severity of being attacked by spam email positively affects perceived threat.

Proposition 1*: The users who perceive spam email as severe to them will perceive spam email as a threat.*

According to Liang and Xue (2009), perceived susceptibility is an individual's subjective probability that a malicious IT will negatively affect him or her. Past research has indicated the inconsistent result of perceived susceptibility. In a study on email security behavior, perceived susceptibility does not determine individuals will enable their wireless network security (Woon et al., 2005) and adoption of anti-spyware threat (Gurung et al., 2009). However, it does have an effect on other studies of IT security user behavior (Liang & Xue, 2010; Workman et al., 2008). Although different studies have different findings, the users' evaluation on

susceptibility of negative consequences would determine their perception of IT threat (Liang & Xue, 2009).

Proposition 2*: The users who perceive spam email susceptible to them will perceive spam email as a threat*

Susceptibility and severity is necessary in order to evaluate people's appraisal of malicious IT (Liang & Xue, 2009). Different individuals have different perceptions of these different malicious IT. Hence, perceived susceptibility and perceived severity of being attacked by spam positively affects perceived threat.

Naturally, when email users are aware of the threat caused by spam emails, they are motivated to take actions to protect themselves. If they are avoiding any safeguard to control spam, there must be a reason why they are disabling the options that they have.

Safeguard effectiveness is defined as the subjective assessment of a safeguarding measure regarding how effectively it can be applied to avoid the IT threat (Liang & Xue, 2009). It has some similarities with perceived usefulness in TAM (Davis, 1989). In TAM, perceived usefulness is intended to measure how the technology increases the user job performance. In UTAUT the intention is particularly pronounced as performance expectancy (Venkatesh, Morris, Davis, & Davis, 2003). In TTAT effectiveness is perceived to measure the usefulness of the safeguard in terms of its ability to objectively avoid the threat of malicious IT (Liang & Xue, 2009).

Proposition 3*: The users believe if they adopt effective anti-spam tools, spam email can be avoided.*

Other than effectiveness, other criteria need to be considered, such as include cost of the safeguard. The costs refer to an individual's physical and cognitive efforts that are needed to use the safeguarding measures, such as time, money, inconvenience and comprehension (Weinstein, 1993). Previous studies consistently suggested that cost negatively influence IT security behavior. It was stated that costs negatively influence users' appraisal of the safeguard avoidability (Liang & Xue, 2009) and perceived behavioral control to determine adoption intention and actual adoption of anti-spyware software adoption (Lee & Kozar, 2008).

If the awareness of the impact of spam is low, impossible for the email users willing to invest their money in adopting anti-spam software. In Malaysia, 69.3% of email users admit that they have low awareness of the spam issue (Bujang & Hussin, 2010). Furthermore, they did not realize the impact of spam email due to the fact that most of them choose a neutral answer (neither agree nor disagree) when asked about these issues. From the same study, it was found that 73.5% of email users did not adopt anti-spam software except those provided for free by the ESP or employer (Bujang & Hussin, 2010). Thus, the study attempts to seek whether cost has a significant effect on them to adopt anti-spam measures.

Proposition 4*: The users believe if the cost of anti-spam measure is reduced, spam email can be avoided.*

Bandura (1997) stated the reason the role of self-efficacy beliefs in human is functioning is that "people's level motivation, affective states, and actions are based more on what they believe than on what is objectively true" (p2). It is more about the individual's belief in his/her capabilities and not about how capable the individual is. Graham and Weiner (1996) concluded that particularly in psychology and education, self-efficacy has proven to be a more consistent predictor of behavioral outcomes than any other motivational constructs. For this study, self-efficacy is defined as a user's confidence in taking anti-spam measure and as an important determinant of avoidance motivation.

Self efficacy has been highlighted by the numerous studies in the IS literature and its relationship with intention to IT adoption is well established. According to Compeau, Higgins, & Huff (1999), self efficacy and outcome expectations can predict the behavioral reactions in information technology. This is consistent with the results of other researches which demonstrate that users are more motivated to perform IT security behaviors as the level of their self-efficacy increases (Ng et al., 2009).

Proposition 5*: The users believe when they are confident in taking anti-spam measure, spam email can be avoided.*

Normally, people will avoid any harm situation because they realize how harmful the effect is to them. How they avoid the situation depends on how serious the harm is perceived. Once the user is conscious of the serious consequences of threat, their intention to avoid it will increase.

Proposition 6*: The users who perceive spam email consequences as a serious threat, their motivation to employ anti-spam will be stronger.*

According to Liang and Xue (2009), emotion-focused coping is performed when the safeguard could not reduce the threat sufficiently. As posited in coping theory, individuals are inclined to adopt the emotion-focused coping when they feel that they have limited control over the situation.

Preposition 7*: The users who perceive spam email consequences as serious threats but have no knowledge of anti-spam measure, will likely to perform emotion-focused coping.*

As discussed in the previous section, avoidable perception is influenced by safeguard effectiveness, safeguard cost and self-efficacy. These factors will determine whether spam email can be avoided and when they feel spam email is avoidable, the motivation to adopt the anti-spam software will increase. Thus, user level of confidence determining their willingness and motivation to use anti-spam will increase.

Proposition 8*: The users who see spam email consequences as avoidable will have a stronger motivation to employ anti-spam.*

The email users who have no idea what to do with spam email have a tendency to perform emotion-focused coping. There are also possibilities for those who perform problem-focused coping at first will turn to emotion-focused coping later due to their inability to avoid spam. At this stage, they are considered to perform both problem and emotion-focused coping.

Proposition 9*: The users who perceive spam email consequences as unavoidable will likely perform emotion-focused coping.*

According to a study undertaken by Lee and Kozar (2008), two variables of IT ethics have been added to their model; namely, moral obligation and denial of responsibility. Moral obligation is defined as an individual's perception of the moral correctness of performing behavior (Corner & Armitage, 1998), whereas Denial of Responsibility is defined as an individual's tendency to ascribe responsibility to himself/ herself or to diffuse and depersonalize it to others (Gattiker & Kelley, 1999; Harrington, 1996) . IT ethics is similar to rationalizing the consequences of one's behavior and was developed by Schwartz (Lee & Kozar, 2008). In the present study the combination of both variables is identified as IT Ethics. IT Ethics does not influence the emotion-focused coping because it does not involve any behavior in avoiding spam email. Therefore, the proposition made is as follows:

Proposition 10*: If the users are more ethical in using email application, it will increase the motivation to adopt anti-spam measure.*

In TTAT model, avoidance motivation can be represented by the behavioral intention to use the safeguard (Liang & Xue, 2010). This is similar to the argument of Venkatesh (2003)

in his theory of IT adoption, Unified Theory of Acceptance and Use of Technology (UTAUT). Furthermore, in the cognitive theory by Ajzen (1991), behavioral intention is a strong predictor of actual behavior no matter what the final result is. The aim is not to measure how successful the users are on employing anti-spam measure; but the aim is to investigate how they deal with the spam email. The final proposition is expressed as below:

Proposition 11*: The users' avoidance motivation will influence the avoidance behavior which is to adopt anti-spam measure.*

Conclusions

The proposed model is yet to be tested. However, it is anticipated that a study based on the proposed model will bring many benefits either towards personal user, company or decision maker. Each one of these stakeholders can improve the effectiveness of spam control measures based on their understanding of how the users perceive spam as a threat.

The findings are more useful to the software developing companies such as ESP, ISP or security-technology based companies. Once the behavior of email users is known, the software developer can develop tools based on the user requirements or needs in order to make it more user-friendly. For the company, the more users use the technology, the more profit it they gains from the higher demand.

For the personal email user, they will know their weaknesses in using email technology. Awareness of lack of knowledge or skill in certain application will make them more cautious in the technology. It is hoped they will practice secure transaction using internet, especially email technologies.

To the top level management either in a company or any organization or country, the group of decision makers can develop and adopt more effective and comprehensive rules and policies to control spam problem by focusing on the behavioral aspects of mail users. They could provide better guidelines for personal email users to use the email technology more responsibly.

References

Anderson, C. L. & Agarwal, R. (2006). 'Practicing Safe Computing: Message Framing, Self View, and Home Computer user Security Behavior Intentions,' *Paper presented at the International Conference on Information Systems*, Milwaukee, WI.

Bandura, A. (1997). 'Self-efficacy: The Exercise of Control,' *New York: Freeman*.

Barnetta, E. (2011). "Spam Attacks on Social Networks 'Rise Dramatically'" [Electronic Version]. *The Telegraph*, 19 January 2011,

Beaudry, A. & Pinsonneault, A. (2005). "Understanding Use Responses to Information Technology: A Coping Model of User Adaptation," *MIS Quarterly*, 29(3), 493-524.

Begley, T. M. (1998). "Coping Strategies as Predictors of Employee Distress and Turnover after an Organizational Consolidation: A Longitudinal Analysis," *Journal of Occupational and Organizational Psychology*(71), 305-329.

Bujang, Y. R. & Hussin, H. (2010, 14-16 July 2010). "Spam E-mail: How Malaysian E-mail Users Deal With It?," Paper presented at the International Conference on Innovation, Community and Technology (ICICT 2010), Bali, Indonesia.

Compeau, D. R., Higgins, C. A. & Huff, S. (1999). "Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study," *MIS Quarterly*, 23(2), 145-158.

Conger, S. & Loch, K. D. (1995). "Ethics and Computer Use," *Communications of the ACM*, 38(12), 30-32.

Corbitt, T. (2004). "Are You Suffering from Spam," *Management Services*, 48, 22-23.

Corner, M. & Armitage, C. J. (1998). "Extending the Theory of of Planned Behavior: A Review and Avenues for Future Research," *Journal of Applied Social Psychology*, 28(15), 1429-1464.

Davis, F. D. (1989). "Perceived Usefullness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, 13(3), 319-338.

Folkman, S. (1992). "Making the Case for Coping," Praeger, *Westport, CT*.

Gattiker, U. E. & Kelley, H. (1999). "Morality and Computers: Attitudes and Differences in Moral Judgements," *Information System Research*, 10(3), 233-254.

Graham, S. & Weiner, B. (1996). Theories and Principles of Motivation, In D. C. Berliner & R. C. Calfee (Eds.), Handbook of educational psychology (pp. 63-84). *New York: Simon & Schuster Macmillan*.

Griffith, T. L. (1999). "Technology Features as Triggers for Sensemaking," *Academy of Management Review* (24:3), 472-488.

Gurung, A., Luo, X. & Liao, Q. (2009). "Consumer Motivations in Taking Action against Spyware: An Empirical Investigation," *Information Management & Computer Security*, 17(3), 276-289.

Harrington, S. J. (1996). "The Effect of Codes Of Ethics and Personal Denial of Responsibility on Computer Abuse Judgement and Intentions," *MIS Quarterly*, 20(3), 257-278.

Lazarus, R. & Folkman, S. (1984). 'Stress, Coping, and Adaptation,' *New York: Springer-Verlag*.

Lee, Y. & Kozar, K. A. (2008). "An Empirical Investigation of anti-Spyware Software Adoption: A Multitheoretical Perspective," *Science Direct, Information and Management*, 45, 109-119.

Leung, A. (2003). 'SPAM The Current State,' *Telus Corporationo*.

Liang, H. & Xue, Y. (2009). "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly*, 33(1), 71-90.

Liang, H. & Xue, Y. (2010). "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems*, 11(7), 394-413.

Martin, B. A. S., Van, D. J., Raulas, M. & Merisavo, M. (2003). "Email Advertising: Exploratory Insights from Finland," *Journal of Advertising Research*, 43, 293-300.

MessageLabs Intelligence. (2011). "Global Spam Drops by One Third as Rustock Botnet is Dismantled; MessageLabs Intelligence's First Review of Spam-sending Botnets in 2011," [Electronic Version]. March 2011 Intelligence Report. Retrieved 4th April 2011,

Ng, B. Y., Kankanhalli, A. & Xu, Y. C. (2009). "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems*, 46(4), 815-825.

Venkatesh, V., Morris, M. G., Davis, G. B & Davis, F. B. (2003). "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, 27(3), 425-478.

Weinstein, N. D. (1993). "Testing Four Competing Theories of Health Protective Behavior," *Health Psychology*, 12(4), 324-333.

Woon, I., Tan, G. W. & Low, R. (2005). 'A Protection Motivation Theory Approach to Home Wireless Security,' *Paper presented at the International Conference on Information Systems*.

Workman, M., Bommer, W. H. & Straub, D. (2008). "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior*, 24(6), 2799-2816.