World Academy of Science, Engineering and Technology
International Journal of Humanities and Social Sciences
Vol:2, No:10, 2008

Use of Persuasive Technology to Change End-Users' IT Security Aware Behaviour: A Pilot Study

Ai Cheo Yeo, Md. Mahbubur Rahim, and Yin Ying Ren

***Abstract*—**Persuasive technology has been applied in marketing, health, environmental conservation, safety and other domains and is found to be quite effective in changing people's attitude and behaviours. This research extends the application domains of persuasive technology to information security awareness and uses a theory-driven approach to evaluate the effectiveness of a web-based program developed based on the principles of persuasive technology to improve the information security awareness of end users. The findings confirm the existence of a very strong effect of the web-based program in raising users' attitude towards information security aware behavior. This finding is useful to the IT researchers and practitioners in developing appropriate and effective education strategies for improving the information security attitudes for end-users.

***Keywords*—**Information security, persuasive technology, IT security-aware behaviour, theory of planned behaviour survey.

I. Introduction

AS the dependence on information processing and the interconnection of various information systems via the internet increase, so is the risk to information systems. As a result, organisations have increased their spending on information security technologies [1-3]. However, despite increased spending organisations still continue to experience electronic attacks. This is because inappropriate and destructive human behaviours involved in the use of information systems substantially inhibit the effectiveness of information security technology [1,4,5,6].

According to many IT gurus, appropriate and constructive human-computer behaviour represents the key to the success of information security. Human behaviour is however complex and multifaceted, and this complexity defies the expectations for control and predictability that IT developers routinely assume for technology [1]. Hence, it is not a great surprise that in the 2006 Australian Computer Crime and Security Survey, respondents cited "*changing user attitudes and behaviour regarding computer security practices*" to be the most challenging aspect of computer security management [7].

From time to time, social psychology researchers tried to test the assumption that human attitudes serve as their behavioural predispositions. Substantive research illuminated the strong relation between attitude and behaviour [8]. Therefore, a change in attitude is likely to result in a modification of behaviour [9]. In recent years, research has been carried out on using technology to persuade users to change their attitudes and behaviour. Fogg [10] labels this phenomenon as "persuasive technology". It is defined as a computing system, device, or application intentionally designed to change a person's attitudes or behaviour in a predetermined way [11]. Persuasive technology has been applied in marketing, health, environmental conservation, safety and other domains and is found to be quite effective in changing people's attitude and behaviours [12-14]. This research extends the application domains of persuasive technology to information security awareness in two specific manners: first, a web-based program based on persuasive technology was developed to improve the information security awareness of users; second, in order to measure the effectiveness of this web-based program, an instrument based on the Theory of Planned Behaviour (TPB) [15] was constructed and tested through a pilot study. The findings in broad terms offer support for the assertion that persuasive technology has the potential to bring a change in the attitude towards information security.

The rest of the paper is structured as follows. First, a brief but critical literature analysis is provided. Second, a seven-stage research design is described. Third, the development of a web-based program is explained. Next, the empirical results are presented and discussed. Finally, some concluding remarks are made and future directions of the research are suggested.

II. Literature Analysis

Literature analysis focuses on three specific aspects which are important to address the research concern: information security awareness, use of technology to change user attitudes, and theoretical framework to measure user attitudes. Each is briefly described below.

A. Information Security Awareness

Effective user security behaviours are vital to the success of information security. End user behaviours can be grouped into three categories: malicious, neutral and beneficial [1].

Authors are with Monash University, Australia (e-mail: mahbubur.rahim@infotech.monash.edu.au).

Information security researchers and practitioners recognised that user security behaviours, in particular, neutral and beneficial user security behaviours can be changed by increasing the information security awareness of users. Social psychology has been used successfully in changing the attitude and behaviour of people and this can be extended to make security awareness programs more effective. Thomson and von Solms [9] highlighted some of the social techniques that could be pertinent to an information security awareness program. Sipeon [16] explored the possibilities offered by motivation/behavioural theories in information security and presented a persuasion strategy aimed at increasing user's commitment to security guidelines.

B. Use of Technology to Change User Attitudes

In recent years, technology has been used to persuade users to change their attitudes and behaviour. This field of research has been termed "Captology". Fogg [10] defined captology as design, research, and analysis of interactive computing products created for the purpose of changing people's attitude or behavours. Persuasion has been viewed as the major strategy for influencing people. Since computing technology is pervasive, it allows persuasion messages through technology to be interactive rather than one-way, that is, altering and adjusting the pattern of interaction based on the characteristics or actions of the persuaded party – the user's inputs, needs and context [17]. This application of persuasion strategy by means of computing technology is defined as persuasive technology.

TABLE I
PERSUASIVE TECHNOLOGY STRATEGIES

	Strategies
Computer as Persuasive Technology Tools	a) Reduction: Persuading through Simplifying b) Tunneling: Guided Persuasion c) Tailoring: Persuasion through customization d) Suggestion: Intervening at the Right Time e) Self-monitoring: Taking the Tedium Out of Tracking f) Surveillance: Persuasion through observation h) Conditioning: Reinforcing Target Behaviours
Computers as Persuasive Media (Simulation)	a) Simulated cause-and-effect scenarios: Offering Exploration and Insight b) Simulated environments: Creating Spaces for Persuasive Experiences c) Simulated Objects: Providing Experiences in Everyday Contexts
Computers as Persuasive Social Actors	a) Physical Attractiveness b) Similarity c) Influencing through language: Praise d) Reciprocity e) Authority

Fogg [10] developed a functional triad for captology, which neatly organised three different ways people respond to computer technology. Firstly, the computer as a tool persuade people by making some behaviour easier or more efficient to do, or leading people through a process or performing calculations or measurements that motivates. Secondly, the computer as a medium can persuade people by allowing people to explore cause-and-effect relationships, or providing people with vicarious experiences that motivate or helping people rehearse a behaviour. Thirdly, the computer as a social actor can persuade people by rewarding people with positive feedback, or modelling a target behaviour/attitude or providing social support. A summary of persuasive technology strategies are organised in Table I.

Captology can be applied in a variety of fields, including health, safety, environment, personal relationships, consumerism, education and community involvement. Empirical results have shown that persuasive technology can change people's attitude and behaviours to some extent [12-14]. This research extends the application of persuasive technology to information security awareness.

Although a range of programs have been reported in the literature to increase awareness toward information security, there have been few studies that evaluate the effectiveness of these programs. We developed an instrument based on the Theory of Planned Behaviour (TPB) which was used to measure the effectiveness of the information security awareness program.

C. Theory of Planned Behaviour

TPB is one of the most widely applied models in addressing the causation of diverse human behaviour. It also attracted the interests of many information systems scholars, and has been observed to be highly valid [18]-[19]. According to TPB [15] intention is the immediate determinant of the corresponding behaviour and that this intention is, in turn, a function of a person's attitude toward the behaviour, his/her subjective norms which reflects social influence and outside the individuals' control that may in turn affect his/her behaviour and intention. During the past decade, TPB has been applied to examine a wide variety of behaviours with considerable success. The behaviours include condom use [20-22], class attendance [23-24] leisure activities [25], participating in regular exercise [26,27]. The findings of these esearch conclude that the best single predictor of a person's behaviour is the intention to perform the behaviour.

The TPB can not only serve as a predictor of a person's behaviour, it can also be used to measure a person's belief change, attitude change and ultimately behaviour change [8]. For example, Valois and his co-researchers [28] used TPB to verify the effect of persuasive messages on nursing students' beliefs and attitudes regarding provision of care to people living with HIV/AIDS. Quine and his co-researchers [29] designed and evaluated an intervention based on the TPB to encourage the use of protective helmets in school-age cyclists.

III. Research Propositions

The aim of this research is to test the effectiveness of a web-based program in order to change the attitudes of end-users towards information security awareness. Three important aspects of information security discussed in the IT literature were chosen: password management, e-mail management and virus protection. Each aspect is briefly described below:

Password security is essential to the security of information systems [30]. While the majority of organisational and home users rely heavily on user-generated passwords as a basic form of authentication to sensitive information and personal resources, the insecure creation of passwords and password usage could open the first door to a malicious attacker. In contrast, good password management behaviour can be a defense against intrusion into a computer system [31]-[33]. In their study, Zviran and Haga [34] investigated the core characteristics of user-generated passwords and associations among those characteristics. Their findings confirm that user-selected passwords are still being made up of the characteristics of personal details meaningful to the user, are relatively short, are comprised of alphanumeric characters, are rarely changed, and are usually written down. These findings indicated a need to raise the security consciousness of system users. Many organisations and practitioners provide guidelines on good password security practices which if adopted can help protect information resources from both external and internal attacks.

Another vital component of information security aware behaviour is email management. A key aspect of email management is concerned with spam emails. Spam email is unsolicited email that may consist of commercial advertising, pornography or get-rich-quick schemes [33]. The problems posed by spam have grown from simple annoyances to security issues such as virus attacks. The deluge of spam costs up to an estimated $20 billion each year in lost productivity [35]. Users can help limit the chances of being attacked by being security cautious and taking actions against spammers and by following a good email management practice [36]-[38].

Virus software, commonly known as 'malware" is a software inserted into an information system to cause harm to that system or other systems, or to subvert them for uses other than those intended by their owners [39]. Malware affects everyone: government, business and individual users. However, it is the individual home users who are more vulnerable because of their lack of awareness about the possible harmful effect of malware. Different types of malware are commonly observed including virus, worms, spyware among others. As the reliance of home users on the Internet increases so do the threat of malware. The lack of user awareness and their subsequent inaction contributes to the increasing prevalence of malware. The number of new viruses discovered every month continues to increase [40]. The Global Information Security Survey 2005 [41] found that virus attacks are the source of the greatest financial losses. Without any protection against viruses, users could become the unwitting vehicle for disrupting the information systems in the organisation. Good malware protection practices consist of installation of anti-virus software, keeping anti-virus software updated, use of firewall and installation of software patches among others.

Drawing upon the above mentioned security aspects, the following hypotheses were formulated which would be examined through a pilot study:

H1: There is no significant difference between pre-program post-program attitudes toward password management.
H2: There is no significant difference between pre-program post-program attitudes toward virus protection.
H3: There is no significant difference between pre-program post-program attitudes toward e-mail management.

IV. Research Design

This research follows a seven stage research approach: literature review; approval of ethics application, interviews with IT security experts, development of web-based program; design of instrument; pilot study and analysis of results. Stage 1 involved a literature review of information security, persuasive technology and TPB. The literature review identified information security topics and persuasive strategies to be used in designing the web-based program aimed at increasing the information security awareness of users. In stage 2, a formal ethics application was lodged with the researchers' educational institution in order to ensure that national and university imposed guidelines relating to privacy and data collection were faithfully adhered to.

In stage 3, two semi-structured interviews were conducted with IT executives from a leading tertiary educational institution. The goal of interviews was to gain insights into the security behaviour of students. These executives have good first-hand knowledge of the information security behaviours of students and staff.

In stage 4, a web-based program was then developed using two persuasive strategies: tunneling and influencing through language. The aim of the web-based program was to change the attitudes of students toward information security in the password management, virus protection and e-mail management.

In stage 5, to measure the effectiveness of the web-based program, an instrument was developed based on TPB [15]. In stage 6, a pilot study was conducted with 30 students from the Arts Faculty (15 females and 15 males) who acted as end-users. The students' attitudes toward information security awareness were measured before and after they had used the web-based program in a computer laboratory.

In stage 7, paired t-tests were used to compare the mean difference between pre-program and post-program attitudes (the higher the better). If there is a significant difference between the means of pre-program attitudes and post-test attitudes, we can conclude that this persuasive web-based program is effective in changing students' attitudes toward

security awareness.

V. Design of Web-Based Program

For each of the information security aspects (discussed in Section III), a list of good information security practices were identified. A web-based program was developed to educate users on good information security practices. Two of the persuasive strategies that were used to develop the web-based program are tunneling and influencing through language

Tunneling technology is defined as using computing technology to guide users through a process or experience providing opportunities to persuade the users along the way. For users, tunneling makes it easier to go through a process. For designers, tunneling controls what the user experiences - the content, possible pathways, and the nature of the activities [10]. It is a strategy in which an interaction sequence is carefully laid out to provide maximal exposure to persuasive strategies. Plous [42] argued that once people are committed to an idea or a process, most people tend to stick with it, even in the face of contrary evidence. Examples of effective tunneling technology applications are software installation, registration on web site, and dieting web site [10].

The tunneling technology approach was used to develop the information security awareness web-based program. The web-based program sequentially displays the items one by one to produce an interaction tunnel. Each web page presents only one information security practice. On each page, the user is presented with one multiple-choice question. The question assesses the user's awareness of a particular information security practice. If the user answers correctly, he/she would be praised; otherwise he/she would be informed of the correct practice.

The user can then navigate to the next question. For example the user is asked "How many characters do you have in your password?" If the user select the correct answer "8 characters or more", he/she would be praised. However, if he/she answers incorrectly, he/she would be told "Your password is too short! Hackers can guess your password instantly! Your password should have at least 8 characters!". After the user has answered all the questions relating to password management, a summary of good security practices for the topic is presented to reinforce the information to ensure that they are more likely to be remembered.

Computing products can use written or spoken language in an attempt to convey social presence and to persuade people. By offering praise, via words, images, symbols, or sounds, computing technology can lead users to be more open to persuasion. This persuasive strategy is praise. Prior research has shown that people who received computer praise, responded significantly more positively than did people who received no evaluation [10]. Language is used in the web-based program to promote good IT security behaviours and leverage the power of relationships. In our web-based program, when the user chooses the correct answer to a question, positive feedback is provided to praise the user.

VI. Instrument Design

To evaluate the effectiveness of the web-based program in influencing students' attitudes in information security, a research instrument based on TPB was developed. TPB can be used to measure a person's belief change, attitude change and ultimately behaviour change [8]. According to TPB, a person's behaviour is immediately determined by his/her intention and that this intention is, in turn, a function of his/her attitude toward the behaviour, his/her subjective norms which reflects social influence and outside the individuals' control that may in turn affect his/her behaviour and intention. Since the web site is aimed at changing the attitudes of users toward information security, the construct that is relevant in this research is the "attitudes toward behaviour". "Attitudes toward the behaviour" refers to the degree to which the person has a favorable or unfavorable evaluation of the behaviour in question.

Guidelines from TPB [43] were used to construct the instrument for measuring users' attitudes toward password management; virus protection and e-mail management. The instrument consists of twenty one items. The strength of attitudes toward behaviour was measured on a 5-piont Likert scale from extremely worthless to extremely useful or extremely harmful to extremely beneficial. The items were arranged so that the stems are a mix of positive and negative statements. Items that have negative stems are recorded in the data analysis, so that lower rating for a negative stem reflects a positive attitude toward target behaviour.

VII. Analysis of Results

The participants were required to attend an information security awareness program which is based on persuasive technology. To evaluate the effectiveness of the persuasive web site program in changing students' attitude toward information security awareness, the participants were asked to complete the instrument developed based on TPB before and after attending the information security awareness program. Thirty students from the Arts Faculty participated in the pilot study.

The means and standard deviations for password management, virus protection and e-mail management are shown in Table II, Table III and Table IV respectively. As we can see from the tables, the means for all the items are higher after participants have attended the information security awareness program.

TABLE II
ATTITUDES TOWARD PASSWORD MANAGEMENT

Password Management	Pre-program M	Pre-program SD	Post-program M	Post-program SD
Participants (n=30)				
Length of password	3.67	0.99	4.33	0.76
Composition of password	3.83	0.75	4.20	0.89
Selection method of a password	4.03	0.96	4.23	0.90
Usage of password	2.97	1.03	3.57	0.94
Memorization of password	3.43	1.01	3.70	0.99
Sharing a password	3.93	0.69	4.10	0.48
Frequency of password change	2.97	0.85	3.63	0.89

*M=Mean; SD=Standard Deviation

TABLE III
ATTITUDES TOWARD VIRUS PROTECTION

Virus Protection	Pre-program M	Pre-program SD	Post-program M	Post-program SD
Participants (n=30)				
Installation of anti-virus software	4.30	1.02	4.53	0.73
Keep anti-virus software updated	4.30	0.88	4.53	0.68
Automatic update	4.10	1.03	4.33	0.71
Frequency of update	3.40	0.97	4.03	0.96
Configuration of anti-virus software	3.60	0.77	4.17	0.79
Use of firewall	3.73	1.08	4.20	0.81
Installation of software patches	3.43	0.86	3.83	0.99
Students' behavior when encountered with IT incident	3.17	0.79	3.93	0.87

*M=Mean; SD=Standard Deviation

TABLE IV
ATTITUDES TOWARD E-MAIL MANAGEMENT

E-mail management	Pre-program M	Pre-program SD	Post-program M	Post-program SD
Participants (n=30)				
Use anti-virus software to scan e-mail attachment	4.03	0.67	4.23	0.63
Delete e-mails from people you do not know	3.77	0.73	4.10	0.66
Check with friends with unexpected e-mails from them	2.97	0.89	3.70	0.84
Do not send personal details with e-mails	3.40	1.04	4.17	0.87
Use of spam filter	3.77	0.77	4.10	0.71
Use of phishing filter	3.53	0.73	3.97	0.56

*M=Mean; SD=Standard Deviation

Before performing student t-tests to determine whether significant differences exist between student attitudes prior and after the conduct of the web-based program, it is important to verify whether the attitude data follows a normal distribution. This was achieved using the Shapiro-Wilk normality test for both pre-progarm and post-program attitude data. The Shapiro-Wilk values for pre and post-presentation attitude responses were far greater than 0.05; hence the distribution of student responses can be assumed to follow a normal distribution.

In order to find out whether there exists a statistically significant difference in the overall attitude of students prior and after the web-based program attendance, a paired-sample t-test (2-tailed) was conducted with a 95% confidence interval. The results of the paired-sample t-test, which are shown in Table V, indicate the existence of a significant difference in student attitudes towards each of the three security aspects (i.e. e-mail management, password management and virus protection) confirming the existence of a very strong effect of the web-based program in raising student attitudes towards information security aware behavior.

TABLE V
RESULTS OF STUDENT T-TESTS

Security Aspect	Pre-program M	Pre-program SD	Post-program M	Post-program SD	t-value	p-value
Password management	3.55	0.9	3.97	0.8	-6.2	.000
E-mail management	3.58	0.8	4.04	0.7	-7.2	.000
Virus protection	3.75	1.0	4.20	0.8	-7.9	.000

VIII. Conclusion and Limitations

This research has used a theory-driven approach to evaluate the effectiveness of the use of persuasive technology in improving the information security awareness of end users. A web-based program based on the principles of persuasive technology was prepared and an instrument to measure its effectiveness was also developed by referring to TPB. A pilot study involving 30 students (who acted as end-users) participated in an experiment in which they were required to complete the same instrument prior and after attending the web-based program presentation. The findings indicate the existence of a significant difference in student attitudes towards each of the three security aspects (i.e. e-mail management, password management and virus protection) confirming the existence of a very strong effect of the web-based program in raising student attitudes towards information security aware behavior. This finding is useful to the IT researchers and practitioners in developing appropriate and effective education strategies for improving the information security attitudes for end-users.

This finding however needs to be treated with caution because the participants of this research were confined to students from the Arts Faculty only. Hence, this research could be extended to students from other disciplines, academics and administrative staff of the University. Gender difference in attitudes toward information security awareness could also be investigated. Only three information security awareness topics were included in the study. Other security topics could be included in future research.

Furthermore, other persuasive strategies like simulated cause-and-effect and similarity strategies were not used in the web site design. These strategies could be explored in the next version of the web site. Finally, the evaluation of the information security awareness program was carried out immediately after the implementation of the program. The long-term effectiveness of persuasive technology is still unknown. These and related issues need to be addressed in longitudinal studies.

References

[1] Stanton, J. M., Kathryn R.S., Indira G. & Cavinda C., "Examining the linkage between organizational commitment and information security"', in IEEE International Conference on Systems, Man and Cybernetics. pp: 2501-2506, 2003.

[2] Deloitte, '2005 Global security survey', Deloitte, available at: http://www.deloitte.com/dtt/cda/doc/content/2005%20Global%20Security%20Survey%281%29.pdf, 2005

[3] CIO, "CIO research reports", CIO, available at: http://www2.cio.com/research/surveyreport.cfm?id=93, 2005

[4] Straub D. W., "Effective IS security: an empirical study"', Information System Research, Vol.1, No.2, pp:255-277, 1990.

[5] Straub, D. W. and Welke, R. J., "Coping with systems risk: Security planning models for management decision making", MIS Q, Vol.22, No. 4, pp: 441-469, 1998.

[6] Leach, J., "Improving user security behaviour", Computers and Security. Vol.22, No.8, pp: 685-692, 2003.

[7] AUSCERT, "2006 Australian Computer Crime and Security Survey", Available at: www.auscert.org.au, 2006

[8] Ajzen, I., and Fishbein, M. Understanding attitudes and predicting social behaviour, Englewood Cliffs, NJ: Prentic-Hall, 1980.

[9] Thomson, M. and R. von Solms, 1998, 'Information security awareness: educating your users effectively', Information Management and computer security, Vol.6, No.4, pp: 167-173.

[10] Fogg B.J., Persuasive Technology: using computers to change what we think and do, Morgan Kaufmann Publishers, CA, 2003

[11] Fogg B.J., 'Persuasive Computers: Perspectives and Research Directions', CHI98 Conference of ACM (CA: ACM Press, 1998), pp: 225-232.

[12] Fogg B.J. and Clifford Nass, 'How users reciprocate to computers: an experiment that demonstrates behaviour change', in Extended Abstracts of the CHI97 Conference of the ACM/SIGCHI (New York: ACM Press, 1997), pp: 331-332.

[13] Lapolla, N.A. and Salvucci, A., 'Evaluation of a Youth Driving Simulator Program', available at: http://apha.confex.com/apha/128am/techprogram/paper_13286.htm, 2000.

[14] Lenert L, Muñoz RF, Stoddard J, Delucchi K, Bansod A, Skoczen S, Pérez-Stable EJ., 'Design and Pilot Evaluation of an Internet smoking cessation program', J AM Med Inform Assoc., 10 (1), pp:16-20, 2003.

[15] Ajzen, I., 'The theory of planned behaviour', Organizational Behaviour and Human Decision Processes, 50, 179–211, 1991.

[16] Siponen, M. T., 'A conceptual foundation for organizational information security awareness', Information Management and Computer Security, Vol.8, No.1, pp: 31-41, 2000.

[17] IJsselsteijn, W.A., de Kort, Y.A.W., Midden, C., Eggen, B., and van den Hoven, E., 'Persuasive technology for human well-being: setting the scene', Persuasive 06 Eindhoven: Springer, 2006

[18] Chau, P., 'An empirical assessment of a modified technology acceptance model', Journal of Management Information Systems, Vol.13 No. 2, pp: 185-205, 1996.

[19] Mathieson, K., 'Predicting user intentions: comparing the technology acceptance model with the theory of planned behaviour', Information System Research, Vol. 3, No. 2, pp: 173-191, 1991.

[20] Chan, D.K.-S., and Fishbein, M. , 1993, 'Determinants of college women's intentions to tell their partners to use condoms', Journal of Applied Social Psychology, 23, pp: 1445-1470.

[21] Libbus, K., 'Women's beliefs concerning condom acquisition and use', Public Health Nursing, 12, pp: 341-347, 1995.

[22] Reinecke, J., Schmidt, P., and Ajzen, I., 'Application of the theory of planned behaviour to adolescents' condom use: A panel study', Journal of Applied Social Psychology, 26, pp: 749-772, 1996.

[23] Ajzen, I.,and Madden, T. J., 'Prediction of goal-directed behaviour: Attitudes, intentions, and perceived behavioural control', Journal of Experimental Social Psychology, 22, pp: 453-474, 1986.

[24] Prislin, R.,andKovrlija, N., 'Predicting behaviour of high and lowself-monitors: an application of the theory of planned behaviour', Psychological Reports, 70, pp:1131-1138, 1992.

[25] Ajzen, I., and Driver, B. E., 'Application of the theory of planned behaviour to leisure choice', Journal of Leisure Research, 24, pp:207-224, 1992

[26] Godin, G.,Valois, P. and Lepage, L., 'The pattern of influence of perceived behavioural control upon exercising behaviour: an application of Ajzen's theory of planned behaviour', Journal of Behavioural Medicine, 16, pp: 81-102, 1993.

[27] Theodorakis, Y., 'Planned behaviour, attitude strength, role identity, and the prediction of exercise behaviour', The Sport Psychologist, 8, pp:149-165, 1994

[28] Valois, P., Turgeon, H., Godin, G., Blondeau, D., and Cote, F., 'Influence of a persuasive strategy on nursing students' beliefs and attitudes toward provision of care to people living with HIV/AIDS', Journal of Nursing Education, 40, pp: 354-358, 2001.

[29] Quine, L., Rutter D. R. and Arnold L., 'Persuading school-age cyclists to use safety helmets: effectiveness of an intervention based on the theory of planned behaviour', British Journal of Health Psychology, 6, pp: 327-345, 2001.

[30] Gehringer, E.F. "Choosing Passwords: Security and Human Factors", International Symposium on Technology and Society, ISTAS'02, pp 369-373, 2002.

[31] Microsoft 2006. "Strong Passwords: How to Create and Use Them." Retrieved 29 August, 2006 from http://www.microsoft.com/athome/security/privacy/ password.mspx

[32] Monash University "Unwanted/Unsolicited Email or Spam." Retrieved 25 August, 2006 from http://www.its.monash.edu.au/staff/email/spam/, 2006a
[33] Monash University 2006b. "Beware of Malicious Emails and Web Pages." Retrieved 25 August, 2006 from http://www.its.monash.edu.au/staff/security/staff-only/home/emails.html
[34] Zviran, M., and Haga, W.J. "Password Security: An Empirical Study,", Journal of Management Information Systems, (15:4), pp 161-185, 1999.
[35] Lyman J. "Spam Costs $20 Billion Each Year in Lost Productivity", Retrieved 3 November, 2006 from http://www.linuxinsider.com/story/32478.html, 2003.
[36] CERT "Email Bombing and Spamming." Retrieved 6 November, 2006, from http://www.cert.org/tech_tips/email_bombing_spamming.html, 2002.
[37] O' Reilly, D. "10-step Security." Retrieved 29 August, 2006 from http://www.pcworld.com/article/id,122500-page,1/article.html, 2005.
[38] University of California. "Email Safety Tips." Retrieved 11 June, 2008 from http://www.security.uci.edu/email/, 2006.
[39] OECD Report "Malicious Software (Malware): A security threat to the internet economy", Ministerial Background Report, Seoul, Korea, 17-18 June., 2008.
[40] CAIDA "CAIDA Analysis of Code-Red." Retrieved 25 October, 2006, from http://www.caida.org/analysis/security/code-red/, 2006
[41] CSI 2005. "2005 CSI/FBI Computer Crime and Security Survey." Retrieved 3 December, 2006 from http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf
[42] Plous S., The Psychology of Judgment and Decision Making, McGraw-Hill, New York, 1993.
[43] Ajzen, I, 'Constructing a TPB Questionnaire: conceptual and methodological considerations', available at: http://people.umass.edu/aizen/pdf/tpb.measurement.pdf, 2002.