Human Aspects of Information Security: An Empirical Study of Intentional versus Actual Behavior

A. Komatsu[1], D. Takagi[2] and T. Takemura[1,3]

[1] Security Economics Laboratory, Information-Technology Promotion Agency
Tokyo, Japan
[2]Graduate School of Humanities and Sociology, The University of Tokyo
Tokyo,Japan
[3] Research Institute for Socionetwork Strategies, Kansai University
Osaka, Japan
e-mail: a-koma@ipa.go.jp

Abstract

A significant amount of empirical research has been conducted on the socio-economic (sociological, psychological, economic) aspects of information security such asthe phenomena of individuals who are willing to take security measures, but often do not. There is a growing body of research relating to individual behaviour and decision-making. To promote effective information security measures, this paper refers to research on the psychology of persuasion from the field of social psychology. A survey was conducted into determinants for changing attitudes through persuasive messages, and the results were analysed. A questionnaire was used and the authors built a demonstrative experimental environment, which analysed in detail attitudinal changes in an individuals' behaviour.. As a result, the authors found differences in behaviour regarding the intent to implement measures discovered from the responses to the questionnaire as well as from actual conduct in the demonstrative experiment.

Keywords

Information Security, sProtection Motivation Theory, Elaborative Likelihood Model

1 Introduction

In Japan, according to the “Survey Report of Information Security Incidents” released every year by the Japan Network Security Association, 1032 security incidents happened in 2005, and theft and loss resulting from individual human error accounted for 42% of all incidents and was the largest category. In response to these types of situations, many products aimed at preventing information leaks have become available in the market and management practices, such as ISMS, have been implemented. However, in the 2009 survey, information leakage incidents had failed to decline, with the number reaching 1539 incidents. Although individual human error incidents had declined to 7.9%, incidents caused by administrative error had increased from 5.1% in 2005 to 50.9% (JNSA, 2010). Based on these statistics, new approaches for information security measures have arisen. One such approach is research focusing on the behaviour of individuals as standard practice and decision-making. In this paper, we analyze a survey on the behaviour of individuals who

implement information security measures. In particular, we refer to existing research on attitudinal change using persuasive communication from the field of persuasion psychology.

The structure of this paper is as follows. In Section 2, the background to the motivation of our research is discussed. In Section 3, related works and the models our research is based on are discussed. In Section 4, the outline of the questionnaire and the experiment we designed is explained. In Section 5 the results are given as well as an explanation of the analysis and a discussion. In Section 6, this paper is summarized.

2 Background

A Bot is a malware program which allows a malicious attacker (referred to simply as an 'attacker' hereinafter) to gain control of a computer for fraudulent purposes. Once a computer is infected with a Bot, the attacker remotely controls the computer externally. Therefore, the user can cause damage to the entire network without recognizing that their PC is infected. The Cyber Clean Center (CCC) (2011) is an organization supported by the Ministry of Economics, Trade, and Industry (METI), and the Ministry of Internal Affairs and Communications (MIC) with the collaboration of ISPs. With the help of ISPs, the CCC sends an attention-grabbing warning email to the users of Bot-infected computers (Figure 1).

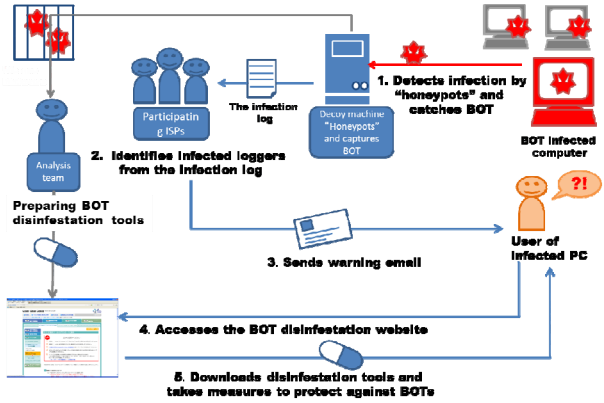

Figure 1: Activity by the Cyber Clean Center

CCC also provides a cleaning tool on its Website. People who are notified of an infection are expected to download the cleaning tool, install it on their PCs, and take necessary steps accordingly. This activity has proven to be effective, leading to the relatively low rate of Bot infections in Japan, compared to the rest of the world. However, among the users who received such an e-mail warning from the CCC, those who implemented the recommended measures (i.e., downloading the cleaning tool) account for only about 32.5 percent, thus underscoring the need to improve this rate. Despite being warned of the Bot-infection and urged to implement specific

countermeasures, why do only 32.5 percent of users follow the recommendation? The answer might be that users think downloading and installing such a cleaning tool on their PCs might incur costs as well as cause further trouble. One survey in the field discusses the hypothesis that this phenomenon is a "Social Dilemma" and tries to verify the cognitive elements which are the feature of "Social Dilemma" (Komatsu et al., 2010). The results of the survey revealed that a users' attitude (based on stated preference) does not match that users' behaviour (based on revealed preference). For this reason, an analysis of the cause for this difference is necessary. Also, additional surveys and experiences need to be conducted. The authors found that the cognitive element that most affects a users' behaviour is a sense of crisis. Therefore, the authors refer to both Protection Motivation Theory (PMT), which can create the sense of a threat and the Elaboration Likelihood Model (ELM), which is a behavioural model using persuasibility in the decision-making process.

3 Related Research and Trends

Since 2001, a field of research called "Security Economics" has emerged with Ross Anderson at the forefront (2001). Far from being a Western-only interest, security economics has also garnered considerable interest in Asia (Sugiura et al., 2008). Also, Egelman et al., (2008) provide an insightful study that creates effective security indicators within the context of phishing. These indicators are clearly needed, as 97% of participants believed in phishing enough to visit the URLs. For the participants who saw the active warnings, 79% chose to heed them and close the phishing sites, whereas only 13% of those who saw the passive warnings obeyed them. Without the active warning indicators, it is likely that most participants would have entered personal information. However, the active indicators did not perform equally. In other words, this study has substantiated the effectiveness of the active warning alerts used in the experiments. A current and important result in terms of potential malware problems also exists. Christen et al., (2011) examined the cost for an attacker to pay users at home to execute arbitrary malware and then asked these users to download and run an executable program they wrote without being told what it did and without any way of knowing how it works .

3.1 Persuasion Psychology

Persuasive communication is a type of communication used for the adoption of certain beliefs in people.. Persuasion is defined as a socially effective process or a socially effective action that causes attitudinal or behavioural changes with a receivers' consent under a non-enforcing manner. This type of communication is mainly accomplished through language (Fukuda, 2002).

3.1.1 Protection Motivation Theory

Rogers (1983) discussed how communication that constructs threats is not a single communication, but several, which include three stimulus variables. The negative factors which define attitudinal change are "perceived severity", "probability of occurrence", and "cost". The positive factors include "response efficacy" and "self-

efficacy". When reflecting on information security measures with these kinds of factors in mind, it is evident that behaviours related to information security measures are not just conducted by individuals, but by multiple people. In other words, it is necessary to investigate collective behaviour in order to persuade people to adopt coping behaviours for information security measures. This type of protection motivation theory is proposed by Fukuda and Tozuka (2005), to explain the effect of threat persuasion, which requires a collective coping behaviour. The factors for collective coping behaviour are defined as "perceived responsibility", "perceived ratio of others "and "perceived social norms". The "perceived ratio of others" means recognition of the ratio of others implementing security countermeasures. Research concerning information security using PMT on state of individual cognition under threats of home wireless security already exists by Tam et al., (2005).

The present authors consider the intention to implement security measures as dependent upon the situation and include such factors such as the capability of coping , past experience regarding incidents of information security, and the literacy of the Internet environment. Because of these reasons, the discussion is extended to the Elaboration Likelihood Model.

3.1.2 Elaboration Likelihood Model

The Elaboration Likelihood Model (ELM) designed by Petty and Cacioppo (1986) is considered to be high in explanatory power among models dealing with attitudinal change caused by personal circumstances upon receiving a persuasive message. The model defines two processing routes for a persuasive message as follows:

a) Central route: A persuasive message is scrutinized, understood, and then a logical coping behaviour is adopted..

b) Peripheral route: The receiver of the message does not have sufficient ability to understand its content, and so is affected by factors not directly related to the message content, such as the level of trust in the sender of the message

When a person changes their attitude through the peripheral route, their attitude is relatively temporary and is generally influenced by other information. On the other hand, when an attitude change occurs through the central route, the attitude is relatively sustained, regardless of whether the coping behaviour is employed or not. We introduced central route factors such as "persuasiveness of message" and "level of comprehension", and as peripheral routes, "trust in sender" and "trust in message". We assume that these factors are influenced by individuals' IT-skills, knowledge, or intention in implementing security measures.

4 Survey and Demonstration Experiment

4.1 Preparations and questionnaire

To analyse the difference in actual behaviour and implementation intention, observation of the behaviour of people who are pressured to take actual measures when they received a persuasive message is needed. More specifically, factors for a persuasive message that needs to be satisfied become clear by clarifying the process that leads to an actual behaviour and the cognitive factors that trigger such attitudinal changes.. Therefore, we first conduct a preliminary survey on the implementation of intention, then link this survey with a demonstration experiment, and analyze each individual's behaviour and its linkage with the questionnaire. Below, we summarize the issues:

a) Regardless of whether or not there is an intention to implement measures, what are the circumstances of individuals who do not implement them?

b) What kind of persuasive message will give rise to attitudinal changes?

According to the ELM, to effect attitudinal changes from a warning alert email, the factors which will cause attitudinal change will depend on whether or not the individual has the ability to deeply comprehend the content of the warning alert mail. Therefore, it could be inferred that the attitudinal change will depend to some degree on the difference in IT skills and the degree of the user's involvement in security incidents. The procedure of the questionnaire was as follows: Subjects were presented with an explanatory text about Bots, followed by an warning alert mail, and then given a download method for a Bot-removal tool as a countermeasure. Subsequently, the demonstration experiment was conducted after selecting the participants from the respondents that answered the questionnaire. Furthermore, to elicit accurate intentions, the true purpose of the questionnaire was not disclosed. Also, the contents of the questionnaire varied widely so that the participants could not deduce the overall purpose of the questionnaire.

4.2 Experimental set-up

An experimental system was developed and constructed in the laboratory with a LAN connected to the Internet. One hundred participants were extracted from respondents of the questionnaire and were composed so that the number of participants who have experienced a computer virus infection was equal to the number of participants who did not. The experiment was conducted in three anechoic rooms with PCs set up so that there was no external influence (Figure 2). Also, monitoring PCs were prepared so that the authors could observe the PC screen used by each test participant (Figure3).

4.3 Ethical considerations

The experiment was conducted based on the Japanese Psychological Association "Code of Ethics" in regard to conducting a psychological experiment (JPA, 2011). The participants were told that the name of the experiment was, "A psychological experiment about a game environment that uses collective knowledge".

5 Findings and Discussion

The survey was conducted over the Internet using a Web survey environment from Cross Marketing Ltd. (2012). The reason we adopted an Internet survey was because the topic of this survey was Bot viruses, and people that used the Internet had to be selected effectively. The survey period was from 9 March 2010 to 10 March 2010, and the total number of respondents was 2254. Table 1 shows the number of respondents per gender and in each age group.

age	Male	Female
20-29	280	266
30-39	287	276
40-49	284	275
50-59	293	293
total	1144	1110

Table1: Gender and Age Composition of the Respondents of the Questionnaire

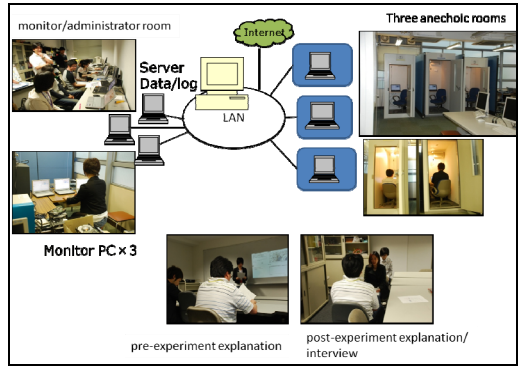

Figure 2: Overview of Experimental Environment

From 17 April 2010 to 29 May 2010, we conducted the experiment with three participants at one time, for a total of 35 times. We interviewed the participants about their behaviour in the game after the experiment. As a result, 93 samples were available because 7participants claimed that they did not take the indicated countermeasures because the PC was not their own. Table 2 shows the results of whether or not participants implemented the measures during the experiment with respect to having the intention for implementation in the questionnaire. Thirty-four participants in the questionnaire responded that they intended to implement the

measures, whereas of these, thirteen actually implemented the measure and twenty-one failed to do so.

5.1 Findings from result of the questionnaire

Variables related to IT-skill level had 11 question items; "degree of involvement" had 3 items. For each respectively, we executed a principal component analysis with the median of the first principal component as the dividing line. PMT cognition factors with values of 1-4 indicate the level of cognition in descending order. According to multinomial logistic regression, "response efficacy" was the element within the collective PMT that was shown to significantly influence the implementation intention the most ($p<0.05$). As for factors in ELM, "trust in sender" influenced the intention of those in the low IT-skilled group the most. The statistics tool "stata11" was used because of its overall reliability in various areas of research.

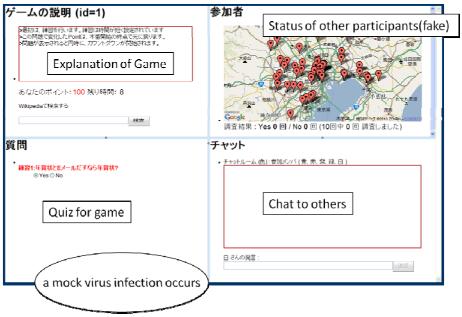

Figure 3: Snapshot of Participant's PC Screens

Questionnaire (number of respondents)		Measured in Experiment (number of participants)	
Intention	34	Implemented	13
		Not implemented	21
No intention	59	Implemented	24
		Not implemented	35
Total	93		93

Table2: Implementation Intention in the Questionnaire and Actual Implementation Results in the Experiment

5.2 Analysis of participants whose intentions and actual implementations were different

Since the total sample number is only 93, sample numbers for each four cases divided by intention/no-intention and behaviour (implement/not implement) were too small to run statistical analysis. Therefore, the authors introduced a multiplicative dummy with intention and cognitive elements defined by PMT and ELM Next, a stepwise multinomial logit regression was used to extract significant elements efficiently. The criteria for stepwise regression is $p<0.15$. The result of the stepwise analysis is shown in Table 3. Multiplicative dummies are indicated using the prefix

"in_" with the original elements. The elements which affect actual behaviour without intention include "ITskill(+)" and "self-efficacy"(-). With intention, the elements include "perceived cost"(-), "perceived response efficacy"(-), "perceived social dilemma"(-), "persuasiveness of message"(-), "social norm"(+), "perceived severity"(+), " level of involvement"(-), and "responsibility"(+). Therefore, these positive elements affect the promotion of actual behaviour while cost, perceived response efficacy, perceived social dilemma, persuasiveness of message and level of involvement prevent actual behaviour.

Behaviour	Coef.	Std.Err	Z	P>|z|
IT-skill	1.546	0.924	1.67	0.094
in_ Perceived Cost	-2.708	1.237	-2.19	0.029
Level of comprehension	1.007	0.347	2.91	0.004
In_Perceived response efficacy	-4.688	2.177	-2.15	0.031
Trust in sender	-1.512	0.624	-2.42	0.015
In_Trust in sender	4.749	1.712	2.77	0.006
In_Perceived social dilemma	-6.264	2.641	-2.37	0.018
In_Perceived ratio of others	-4.778	1.715	-2.79	0.005
In_Persuasiveness of message	-2.083	1.407	-1.48	0.139
In_Perceived norm	1.764	1.000	1.76	0.078
Perceived self-efficacy	-1.080	0.513	-2.10	0.035
In_Perceived severity	5.844	2.499	2.34	0.019
Perceived ratio of others	1.030	0.516	2.00	0.046
In_ involvement	-2.062	1.067	-1.98	0.053
In_level of comprehension	-2.779	1.039	-2.67	0.007
In_responsibility	5.514	2.158	2.56	0.011
_cons	-4.569	3.237	-1.41	0.158

n=93,, Pseudo R2 = 0.354

Table 3: Result of stepwise logit analysis

A coefficient for the multiplicative dummy (e.g. in_the Perceived ratio of others) represents the impact of an element under intention and for a corresponding non-multiplicative dummy (e.g. Perceived ratio of others under no intention). Using the sign of the estimated coefficients for these items, the estimation results can be interpreted as follows:

- Level of comprehension is positive, but comprehension level with intention is negative: Comprehension promotes actual behaviour under non-intention, but prevents actual behaviour under intention.

- Trust in sender is negative, but in-trust is positive: Trust in sender prevents actual behaviour under non-intention, but promotes actual behaviour under intention.

- The perceived ratio of others is positive, but the in-perceived ratio of others is negative: Perceived ratio of others promotes actual behaviour under non-intention, but prevents actual behaviour under intention.

The above results seem to suggest that intention affects the actual behaviour of participants not directly but indirectly via cognitive elements. To be precise, we think that intention affects the elements and, then, subsequently, influences actual behaviour.

In the case where an Internet user trusts a sender, the former is unlikely to take measures if she/he has no intention, whereas the opposite is likely to hold true otherwise. In the case where the level of comprehension is high, an Internet user is unlikely to take measures if she/he has intention. Here, she/he observes a surrounding experimental environment carefully, understands the situation well, and, then concludes that she does not have to take measures. That is, she/he does not take measures unless she/he *really* thinks it is necessary. A similar argument applies to the case for the perceived ratio of others.

5.3 Requirements on a Persuasion Message

We summarize the requirements for a persuasive message. The results showed that in order to form the implementation of intention, it is necessary to communicate in a simpler manner "what kind of effect" an information security measure has on an individual, and to send a message which appeals to the low IT-skills group's trust in the sender. Also, the fact that these groups will process the message through a peripheral route is assumed, and therefore, presenting information that is intuitively satisfying is believed to be more effective than the accuracy of the message.

The results of the analysis between intention and actual behavior are more complicated than previously thought. The message should be sent by a trusted entity. While existing research shows that many people have an intention to heed the email warning, effective elements of an intention include social norms, the degree of severity of the message of persuasion, and a sense of responsibility, which are not always considered as well. If a user has the intention to heed an email warning and carry out the measures needed, then this intention will be effective for conducting actual behavior because the user will trust the sender. When a user has the intention of measuring implementation, the other users enforcement of the notification is not needed, and when a user's own degree of comprehension is high, it does not necessarily effect actual behavior.

5.4 Future Topics

Previously we believed that cognitive elements affected actual behavior through intention. However, the result shows the possibility that intention affects cognitive elements. We would like to consider the relationship among intention, actual behavior, and cognitive elements.

6 Conclusion

We conducted this psychology experiment to observe an actual, individual behavior after the questionnaire. The difference in intention and actual behavior was revealed.

Several cognitive elements related to PMT and ELM were effective in promoting the implementation of security measures. We will apply the results to activities that promote information security measures. However, the relationship between complex structures remains when considering intention, actual behaviour, and cognitive elements.

7 Acknowledgments

The authors wish to thank Professor Nicolas Christin of Carnegie Melon University for his valuable comments. We also wish to thank Professor A.Yoshikai of Nihon University, Associate Professor A.Inomata of the Nara Institute of Science and Technology, Assistant Professor M.Ueda of the National Institute of Informatics, and Dr. H.Numata of Excellead Technology Inc., for carrying out the survey and experiment.

References

Anderson, R. (2001). Why Information Security is Hard- An Economic Perspective, ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference, 2001, IEEE Computer Society, Washington, DC.

CCC: Cyber Clean Center in Japan. (2011), "Achievements of the Cyber Clean Center", https://www.ccc.go.jp/en_report/201101/index.html

Christin, N., Egelman, S., Vidas,T, and Grossklags, J. (2011) "It's All About The Benjamins: An empirical study on incentivizing users to ignore security advice," Financial Cryptography & Data Security.

Cross Marketing Ltd., Web Site(2012), http://global.cross-m.co.jp/(Accessed 25 April 2012)

Egelman, S, Cranor, L, and Hong, J. (2008) "You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings." CHI '08: Proceedings of the SIGCHI conference on Human Factors in Computing Systems.

Fukada, H.(2002) "Handbook for Persuasion Psychology", Kita-ohji Publishing(in Japanese), 2002.

JNSA Japan Network Security Association. (2010). "Survey report for the information security incident in 2009" (in Japanese), http://www.jnsa.org/result/incident/2009.html.

JPA: The Japanese Psychological Association, "JPA code of ethics," http://www.psych.or.jp/members/rinri.html

Komatsu, A., Takagi, D., and Matsumoto, T., (2010) "Empirical study on cognitive structures and personal gain in information security countermeasure", Journal of IPSJ, (in Japanese), Vol.51, pp.1711-1725.

Tozuka, T., Fukada, H., (2005) "Study of the collective protection model for Threat appeal persuasion," The Japanese Journal of Experimental Social Psychology, Vol.44, No.1, pp.54-61.

Petty, E.,Rechard, Cacioppo, J.,.(1986), "The Elaboration Likelihood Model of persuasion," Advances in Experimental Social Psychology, Vol.19, 1986.

Rogers, R.W.,(1983), Cognitive and Physiological process in fear appeals and attitude change," A revised theory of protection motivation theory, Social Psychophysiology. Press,pp.153-176, New York.

Sugiura, T., Komatsu, A., Ueda, M., and Yamada,Y., (2008) "Challenge to Information Security Economics," Proc. of Computer Security Symposium 2008 (in Japanese), pp.725-730.

Woon, I., Tan, G.-W., and Low, R.(2005) "A Protection Motivation Theory Approach to Home Wireless Security," International Conference on Information Systems, Proc. of ICIS2005, Paper31.