

Symbolism in Computer Security Warnings: Signal Icons and Signal Words

Nur Farhana Samsudin, Zarul Fitri Zaaba*, Manmeet Mahinderjit Singh, Azman Samsudin

School of Computer Sciences,
Universiti Sains Malaysia, 11800 Minden,
Pulau Pinang, Malaysia

Abstract—Security warning is often encountered by the end users when they use their system. It is a form of communication to notify the users of possible consequences in the future. These threats have always been evolved with the advancement of technologies. The attacks threaten the end users with many harmful effects such as malware attacks. However, security warning keeps being ignored due to various reasons. One of the reasons is lack of attention towards warnings. The end users feels burden and treat security task as a secondary rather than primary task. To divert user's mind to read and comprehend the security warnings, it is important to capture the user's attention. Signal words and signal icons are important in the security warning as it is the elements that could help user to heed the warnings. A survey study has been conducted with 60 participants in regards to the perception towards attractiveness and understanding of the signal words and icons. It can be revealed that end users significantly feel that the icon with the exclamation marks is attractive and easy to understand. However, only one of three hypotheses is proven to be significant.

Keywords—security; signal icons; signal words; usable security; usability; warning

I. INTRODUCTION

Home computer users are more susceptible to security threats such as viruses, worms and phishing attacks with the advancement of Internet and technologies. These threats could lead to possible harm to the computer users and their system in the future such as interruption (i.e. an assets becomes destroyed or unavailable), interception (i.e. an illegitimate party have access to an asset), modification (i.e. the content of an assets is altered) and fabrication (i.e. an illegitimate party inserts a fake objects into the system) [1]. In computer system, the security warning acts as a defense mechanism to resist our system from being harmed. It takes of various forms such as the dialog box, balloon, in-place, banners and notifications [2]. It is usually presented with signal words such as “warning”, “harm” and “danger”. In addition, the signal words are usually being accompanied with signal icons such as a warning icon, an error icon, an information icon and a help icon [2]. These icons have their own meaning and it is utilised based on their respective significance. The signal icon and signal words are some of the important elements in security warnings. Studies revealed that humans process visual data better than text [3]. They claimed that the human brain could process images 60,000 times faster than text. This shows that the visual representations in security warnings could aid the end users in comprehend the security warning faster.

However, security warnings is often being ignored by the users because of various reasons such as they do not understand the messages [4,5], they are unaware of the risk, too much technical words [5,6] and users have an incorrect mental model of risk [6,7]. Users are more focused on their primary task and consider the computer security as secondary tasks [8]. Users also feel like complying with computer security is a burden to them. These problems lead to the lack of usability in computer systems. End users are not able to perform security tasks effectively and the risk communications are not conveyed correctly. In addition, the level of protection offered by the web browsers towards phishing url or malicious site are also very limited [9]. Hence, end-users need to be more alert of the security of their system so that less harm would be experienced.

This paper is organised as follows: Section 2 explores the related work and literature studies; Section 3 describes the methodology implemented in this studies, Section 4 explains the hypotheses used within this study; Section 5 describes the study results and findings, Section 6 presents a brief discussion and finally Section 7 ends with the conclusion highlighting the limitation and current progress of this study.

II. RELATED RESEARCH

Warning is a form of risk communication that is utilised as a message to convey possible consequences of an action [10]. It notifies people about the risk so that possible harm could be avoided. [11] claimed that warning is anything that could interrupts an individual's focus towards possible danger. The warnings in computer context applied the same principle. It is some representations that could prevents the end users from losing several assets such as financial assets and critical data, system access, privacy and valuable time (i.e. user's time) [2].

On the other hand, the end users are still encounter problems with security warnings. [5] have listed six classifications of problems in warnings namely attention towards warnings, understanding of warnings, use of technical wordings, evaluation of risks from warnings, users' motivation towards heeding warnings and users' assessments of the implication of warnings.

This study focuses on the user's attention towards warning with the focus on signal icons and signal words. The attention towards warning is one of the most important aspects in the effort to improve the current implementation of security warnings. People's attention is the fundamental element to

This work is supported by a short term grant from the Universiti Sains Malaysia (USM) [304/PKOMP/6313287]. *Corresponding author

attract the users to read and comprehend the given security warnings. Studies by [12] revealed that there are four categories of reasons for ignoring warnings which are:

- 1) Failures in personal variables: Users do not have the knowledge or experience regarding the security warnings.
- 2) Failures in intention: Users were not motivated to responds to security dialogs.
- 3) Failures communication delivery: The security warnings fail to grabs user’s attention.
- 4) Failures in communication processing: Users do not understand the message being conveyed.

Studies by [13] revealed that the end users were not attentive towards warning as it is hard to comprehend. The participants of their experimental studies were asked to perform a task of purchasing an item online. It can be revealed that the lock icon in the web browsers are noticed however ignored, and the certificates are rarely used by the users. Users did not look at some indicator such as the certificate icon and even if they look at it (i.e. lock icon), they did not maintain their attention to it. Hence, it can be summarised that it is important to embed a better icon and signal words in order to grasp the user’s attention.

[2] suggests that there are four types of standard icons in Windows namely the error, warning, information and question mark icon. Figure 1 shows the standard icons in Windows. These icons have different usage and meaning as described below:

- 1) Error icon: The problem or error has occurred.
- 2) Warning icon: The condition might cause a possible harm in the future.
- 3) Information icon: Useful information is presented.
- 4) Question mark icon: Indicated a Help entry point.

The questions on icons understanding have also been questioned in previous studies [14]. From the studies it can be found that there are still some misconceptions towards icon understanding in security warning. It is important for warnings to convey the right information to the users in order to aid the users in making the right decision.



Fig. 1. Standard icons in Windows; from left to right; Error icon, Warning icon, Information icon, Question mark icon [2]

The usage of the standard icons takes consideration of the message type, severity of the issues and the context of the situation. It is important to present the appropriate signal icon and words in order to provide a better understanding and correct risk communication.

Studies by [15] revealed how the users of IT perceive the severity of hazard and detailed assessment of the signal icons and signal words. They claimed that by combining signal words and signal icon in a security warnings, the level of

hazard perceive by the end users are higher as shown in Table I. They also conduct an experiment of habituation effects in security warnings. By presenting the combination of signal words and signal icon with three different treatment condition, users became habituated only after a few exposures to the same message. Their study also revealed that the signal word and signal icon combination with higher perceived severity to that of the habituated edit request message have the highest hit rate with 39%.

TABLE I. MEAN VALUES (STANDARD DEVIATION) OF THE PERCEIVED SEVERITY OF SIGNAL WORDS AND SIGNAL ICON [15]

Word	Blank	i	?	!	x
Blank		2.00 (1.43)	2.18 (1.73)	3.74 (1.98)	5.30 (2.29)
Notice	2.23 (1.63)	2.64 (1.76)	2.52 (1.67)	3.89 (1.99)	5.19 (2.35)
Error	3.84 (2.19)	3.85 (1.90)	3.73 (1.92)	4.97 (2.20)	6.24 (2.37)
Warning	4.06 (2.10)	4.09 (2.03)	3.91 (1.96)	5.41 (2.08)	6.65 (2.20)
Urgent	4.09 (2.31)	4.15 (2.14)	3.97 (2.13)	5.34 (2.29)	6.54 (2.37)
Critical	5.11 (2.49)	4.82 (2.42)	4.74 (2.21)	6.01 (2.26)	7.38 (2.22)

On the other hand, a study on end-users’ awareness of security indicators have been conducted by [16]. They ask their participants to perform an online transaction in a simulated online banking platform. It can be revealed that none of their participants look at the website address indicator (i.e. lock icon and ‘https’ wording in address bar). These results are worrisome because the absence of security indicator in address bar might hints insecure connection. This study highlights that most of computer users are not attentive towards details such as the url and signal icons. It is important to draw users attention as soon as they load the page since they are performing task that might cause loss of valuable assets, privacy over confidential information and tricked into fraud [2].

In studies by [17], they revealed that the empirical evidence show that graphical cues such as icons, arrows and boxes attract users attention and the eyes get fixed on the headings first, followed by text blocks and graphics. Their results suggest that the use of visual metaphors aid the users to understand the message better. These finding shows that graphical representations such as icons is important elements in a warning. To access the end users perception of signal words and signal icons in security warning, a survey was conducted to better understand the issues of the current implementation of security warnings.

III. METHODOLOGY

We conduct a survey to discover the user perception and understanding of the security warning dialogs with the focus on signal words and icons.. Participants were recruited through word of mouth and e-mail. The participants were asked to provide a numerical rating on a seven-point Likert scale of

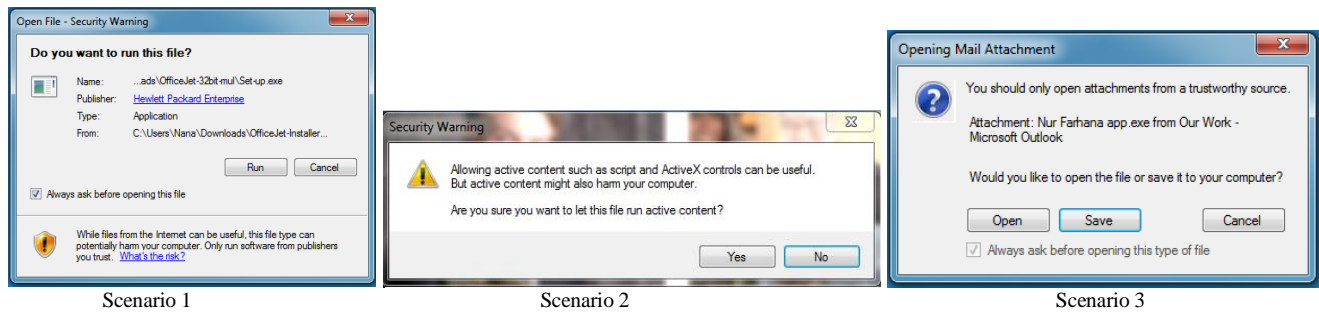


Fig. 2. The study background and computing skills of participants

given scenarios. They could choose the most preferred number where 1 indicate strongly disagree and 7 indicates strongly agree. Studies by [15,17] also conducted the similar survey method to access the end users insights of the current implementation of security warnings however different in scenario used. The Likert-scale is chosen because it is easy to construct, have a high probability of producing a dependable scale and it is easy to be comprehend by the participants [18].

IV. HYPOTHESES

In order to investigate the end users perception towards signal words and icons in security warnings, we proposed three hypotheses to test the significant difference. We would like to explore whether different groups of people have different understanding of security warnings [19]. We have identified two groups from the study which are the technical and non-technical groups. The technical and non-technical groups reflected the user’s background. The hypotheses are created based on the questionnaire in the interview sessions. The hypotheses are described in Table II.

TABLE II. SURVEY QUESTIONS AND THE RESPECTIVE HYPOTHESES

Survey Questions	Hypotheses
The use of visual / graphics (e.g. icons, colors, graphics) helps to draw my attention.	There is no difference between technical and non-technical participants in terms of “The use of visual / graphics (e.g. icons, colors, graphics) helps to draw my attention”. (H1)
The use of visual / graphics (e.g. icons, colors, graphics) helps me to understand the risk.	There is no difference between technical and non-technical participants in terms of “The use of visual / graphics (e.g. icons, colors, graphics) helps me to understand the risk”. (H2)
The words used in the warning is easy to understand.	There is no difference between technical and non-technical participants in terms of “The words used in the warning is easy to understand”. (H3)

To test the statistical differences between two groups, we used Chi-square test in order to look for the statistical difference. The purpose of Chi-square test is to evaluate the association between two categorical variables [20]. Studies by [21] revealed that a Chi-square test is utilised as a comparison of more than one group where the differences are related to the actual sample and another hypothetical data. It is considered as a statistical significant findings when $p < 0.05$. In this test, the Likert-scales values were grouped into three classifications with the range of 1 to 3 is equal to No, 4 is equal to Neutral and 5 to 7 is equal to Yes. This classifications have also been conducted by [14,19]. The results of the Chi-square test are explained further in the next section.

V. RESULTS AND FINDINGS

A total of 60 participants were gathered for the survey. The majority of the participants between the age range of 18 – 25 years old and equally distributed between male and female. Since the interview is promoted well in the university, most of the participants are predominantly from the Universiti Sains Malaysia, Penang, Malaysia.

From the overall responses, the gender of our participants is divided almost equally where it comprises of 45% male and 55% female. Majority of the participants’ are in the range of age of 18-25 years old (95%) and the rest of them were in the range of 26-35 years old. This indicates that they were most likely to grow up in the era of information technology. In addition, the result suggests that the respondents were familiar with the computer and latest technology. Previous studies were also conducted within the university background and majority of the participants were in the range of age between 18-30 years old [8,19]. In addition, most of our participants have high educational background (i.e. postgraduate (8%) and undergraduate (92%)). Figure 3 depicted the study background and computing skills of the study participants.

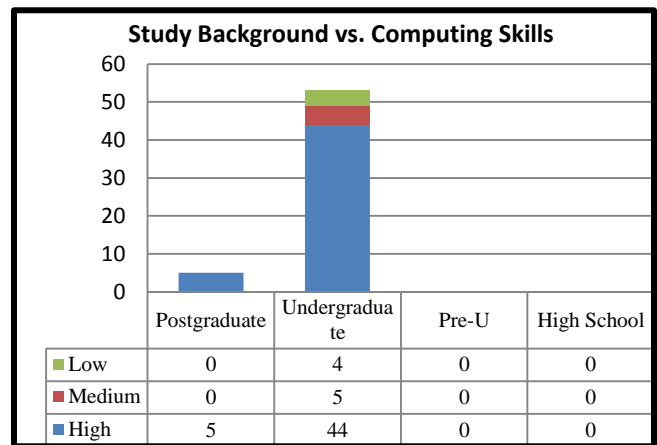





Fig. 3. The study background and computing skills of participants

To classify and determine our study participants skills in computer security, four basic questions were asked in the demographic forms. The questions derived from this section are based on the six tasks from the “Security Center” of Windows Vista [22]. The method of accessing users knowledge by asking a few security questions is also conducted by [23]. The security questions involve knowledge of installing updates, scan for malwares, delete browser’s

cookies and setup password. The categorisation was high, medium and low. For high level expertise, the participants were able to perform advanced task such as installing updates and patches (i.e. could perform all task). For medium level, the participants were unable to perform one of the tasks given while for the low level, the participants could not performed more than one task.

In the questionnaire, we have included three security warnings example (i.e. in a form of image) to explore the end users understanding and perception of the icons and signal words used in the warnings. Figure 2 shows the security warnings shown to the users. The three security warnings have also been discussed in studies by [4,6,14]. The association of signal words and signal icon used in the three scenarios are depicted in Table III.

TABLE III. SIGNAL WORDS AND SIGNAL ICONS USED IN EACH SCENARIOS

Scenario	Signal words	Signal icons	Background colour	Meaning of icons
1	Warning, harm,		Orange	Warning
2	Warning, harm		Yellow	Warning
3	Unavailable		Blue	Help

It can be noted that for scenario 1 and scenario 2, both utilise “warning” and “harm” as a signal words that indicates the possible bad consequences to the system. The icons used are similar which are the exclamation mark icon which means warning. With regards to scenario 3, it can be noted that there is “no signal words” that are available to cues the end users of a possible harm. As for the signal icon, the question mark icon is presented. Generally this icon is a help icon where it will lead users to a guidance page.

A. Scenario 1

Table IV indicates H1 that among those who were from non-technical group, 23 of them found that the icon was more attractive. Despite more non-technical participants found that the icon was attractive, the difference for both version was not statically significant (p = 0.431). The icons used in the warning were referring to the exclamation mark icon with the shape of a shield. It can be assumed that most of the participants (43/60) were attracted to the exclamation mark icon. When the user is attracted to the security warning, it can help in providing the users with better understanding of the message in the warning dialogs.

It can be noted that in standard version, 5 participants from the technical groups did not understand the risk while 1 participant from the non-technical version claimed that the icon used did not convey risk. Surprisingly, the number of participants who understand the risk from the technical group was lesser than the non-technical group and the difference was also not statistically significant (p = 0.181).

TABLE IV. THERE IS NO DIFFERENCE BETWEEN TECHNICAL AND NON-TECHNICAL PARTICIPANTS IN TERMS OF “THE USE OF VISUAL/GRAPHICS (E.G. ICONS, COLORS, GRAPHICS) HELPS TO DRAW MY ATTENTION” (H1) BASED ON SCENARIO 1

Icon Attractiveness	Yes	No	Neutral
Technical	20	1	9
Non-Technical	23	2	5
$\chi^2 = 1.685, p = 0.431, df = 2$			

Even though the results were not statistically significant, majority of our participants agree that the visual in scenario 1 helps them to understand the risk better. With better understanding of the meaning and purposes of the elements in security warning dialogs, the risk communication could better be conveyed.

TABLE V. THERE IS NO DIFFERENCE BETWEEN TECHNICAL AND NON-TECHNICAL PARTICIPANTS IN TERMS OF “THE USE OF VISUAL / GRAPHICS (E.G. ICONS, COLORS, GRAPHICS) HELPS ME TO UNDERSTAND THE RISK” (H2) BASED ON SCENARIO 1

Icon Understanding	Yes	No	Neutral
Technical	23	5	2
Non-Technical	25	1	4
$\chi^2 = 3.417, p = 0.181, df = 2$			

Table VI shows that for the standard version, the result was statistically significant (p = 0.049). It can be found that the 26 participants with technical background able to understand the words used easily rather than only 18 participants from the non-technical background. The words used in the standard version were name, from, type, publisher and .exe. It can be noted that there was a difference between the technical and non-technical participants in understanding the words used in the security warning dialogs. These results suggest that the security warnings should minimise the technical jargons in the text blocks.

TABLE VI. THERE IS NO DIFFERENCE BETWEEN TECHNICAL AND NON-TECHNICAL PARTICIPANTS IN TERMS OF “THE WORDS USED IN THE WARNING IS EASY TO UNDERSTAND” (H3) BASED ON SCENARIO 1

Words Understanding	Yes	No	Neutral
Technical	26	1	3
Non-Technical	18	6	6
$\chi^2 = 6.026, p = 0.049, df = 2$			

B. Scenario 2

Table VII indicates H1 that among those who were from non-technical group, 20 of them found that the icon was more attractive. Despite more non-technical participants found that the icon was attractive, the difference for both version was not statically significant (p = 0.791). However, we learnt that majority of the users (65%) were attracted to the icons and colors in scenario 2. The icon used in the warning was referring to the exclamation mark icon.

TABLE VII. THERE IS NO DIFFERENCE BETWEEN TECHNICAL AND NON-TECHNICAL PARTICIPANTS IN TERMS OF “THE USE OF VISUAL/GRAPHICS (E.G. ICONS, COLORS, GRAPHICS) HELPS TO DRAW MY ATTENTION” (H1) BASED ON SCENARIO 2

Icon Attractiveness	Yes	No	Neutral
Technical	19	4	7
Non-Technical	20	5	5
$\chi^2 = 0.470, p = 0.791, df = 2$			

It can be noted that in scenario 2, 2 participants from the technical groups did not understand the risk while 4 participants from the non-technical participants claimed that the icon used did not convey risk. The results revealed that the number of participants who comprehended the risk from the technical group and non-technical group were similar with a total of 21 participants from each group. It can be noted that there was no significance difference between both groups as $p = 0.607$. These results indicated that for scenario 2, the use of icon did not help the users in comprehending the risk. This might be resulted from the highly technical message provided in the scenario 2 as it contains words such as “active content”, “ActiveX” and “script”. Studies by [14] revealed that 40% of their participants rated that they were having problems with those technical words. The users might be demotivated because when they read the words and look at the icon, they unable to comprehend the meaning and relate it to the given cues.

TABLE VIII. THERE IS NO DIFFERENCE BETWEEN TECHNICAL AND NON-TECHNICAL PARTICIPANTS IN TERMS OF “THE USE OF VISUAL / GRAPHICS (E.G. ICONS, COLORS, GRAPHICS) HELPS ME TO UNDERSTAND THE RISK” (H2) BASED ON SCENARIO 2

Icon Understanding	Yes	No	Neutral
Technical	21	2	7
Non-Technical	21	4	5
$\chi^2 = 1.000, p = 0.607, df = 2$			

Table IX shows that for the scenario 2, the result was not statistically significant ($p=0.468$). It can be found that 21 participants with technical background can understand the words used easily rather than only 18 participants from the non-technical background. The message given in the security warning is “Allowing active content such as script and ActiveX controls can be useful. But active content might also harm your computer”. It can be noted that there were 11 participants from the non-technical background who could not understand the words in the dialogs.

TABLE IX. THERE IS NO DIFFERENCE BETWEEN TECHNICAL AND NON-TECHNICAL PARTICIPANTS IN TERMS OF “THE WORDS USED IN THE WARNING IS EASY TO UNDERSTAND” (H3) BASED ON SCENARIO 2

Words Understanding	Yes	No	Neutral
Technical	21	5	4
Non-Technical	18	9	3
$\chi^2 = 1.516, p = 0.468, df = 2$			

This result indicated that the non-technical groups were having problems in terms of understanding the technical jargons in computer. Studies by [6] also highlighted the same issues where their participants were having difficulties with the technical words.

C. Scenario 3

Table X indicates H1 that among those who were from non-technical group, 17 of them found that the icon was more attractive. Even though more non-technical participants found that the icon was attractive, the difference was not statically significant ($p = 0.670$). The differences between technical and non-technical users who choose “Yes”, “No” and “Neutral” were not that extensive. The icons used in the standard warning are the question mark icon. It can be noted that scenario 3 receives the lowest “Yes” score between the three scenarios presented to the users. It can be noted that the question mark icon was not an appropriate icon to be used in a critical message such as an email attachment dialogs. It is supposed to be a warning icon rather than question mark icon. When such problems occurs, users’ mental model will shift or learn that “?” icon means warning rather than help (i.e. incorrect mental model). This is not a good signal and it might lead to bad consequences.

TABLE X. THERE IS NO DIFFERENCE BETWEEN TECHNICAL AND NON-TECHNICAL PARTICIPANTS IN TERMS OF “THE ICONS USED ATTRACT MY ATTENTION” (H1) BASED ON SCENARIO 3

Icon Attractiveness	Yes	No	Neutral
Technical	15	9	6
Non-Technical	17	6	7
$\chi^2 = 0.802, p = 0.670, df = 2$			

It can be noted that in scenario 3, 10 participants from the technical groups did not understand the risk while 9 participants from the non-technical version claimed that the icon used did not convey risk. Surprisingly, the number of participants who understood the risk from the non-technical group was larger than the technical group however the difference was also not statistically significant ($p=0.866$). These results also had the least “Yes” choice as compared to other scenarios. It can be assumed that the question marks icon did not convey the risk communication in a good manner. Users might not realised the importance of responding correctly to the email attachment dialogs since the signal words and icons are not properly utilised.

TABLE XI. THERE IS NO DIFFERENCE BETWEEN TECHNICAL AND NON-TECHNICAL PARTICIPANTS IN TERMS OF “THE USE OF VISUAL / GRAPHICS (E.G. ICONS, COLORS, GRAPHICS) HELPS ME TO UNDERSTAND THE RISK” (H2) BASED ON SCENARIO 3

Icon Understanding	Yes	No	Neutral
Technical	15	10	5
Non-Technical	17	9	4
$\chi^2 = 0.289, p = 0.866, df = 2$			

Table XII shows that the result was not statistically significant ($p=0.936$). It can be found that 22 participants with technical background can understand the words used easily rather than 23 participants from the non-technical background. The words used in the security warnings were trustworthy and .exe. It can be noted that majority of the participants (75%) able to understand the words easily. This might be resulted from the text message that contains the less or minimal technical words. Hence, both groups of users could better comprehend the message in the dialog.

TABLE XII. THERE IS NO DIFFERENCE BETWEEN TECHNICAL AND NON-TECHNICAL PARTICIPANTS IN TERMS OF “THE WORDS USED IN THE WARNING IS EASY TO UNDERSTAND” (H3) BASED ON SCENARIO 3

Words Understanding	Yes	No	Neutral
Technical	22	5	3
Non-Technical	23	4	3
$\chi^2 = 0.133, p = 0.936, df = 2$			

VI. DISCUSSION

One of the main elements that contributed to the attention of users towards warnings is the signal icons and signal words. With the focus of signal words and signal icons, three hypotheses have been constructed to test the usability of the security warning dialogs. It can be revealed that from the three hypotheses for each scenario, only one hypothesis is significant which is H3 for scenario 1 ($p=0.049$). Although most of the scenarios hypotheses are not statistically significant, but it give some indication and basis on how within small sample of participants perceive security cues (i.e. icons an words). The results shows that in terms of icon attractiveness and words understanding, majority of the participants chose scale of (5-7) which reflects their high preference (i.e. Yes) regardless of their study background or major. This result also indicates that the icons and signal words do attracts both groups and there is no significance difference between the two groups in perceiving the signal icon and signal words in general. In addition, it can be noted that in terms of risk understanding of security warnings, more users have better awareness when the exclamation mark icon is presented. Since precaution from possible malwares attacks is important, security warnings should presents an icon that presents caution in more explicit manner (i.e. rather than using question mark icons which is meant for help). One of the notable findings from the study is within scenario 1. It can be found that the non-technical people have the difficulties in understanding the words (i.e. technical jargons) in the warning. This results shows that it is important to have simpler words that can be understood by users. The similar findings are discovered by [6,14] where they claimed that technical words in warning dialogs should be easy to comprehend. Hence it can be summarised that security warnings should exhibit precise icons with more user-friendly word that could cater for both technical and non-technical users.

VII. CONCLUSION

Security warning is a form of communication that would always be encountered by the end users in order to protect their

computer system from being harmed. The hypotheses results revealed that there is no difference between the technical and no-technical participants in perceiving the signal icons and signal words in most of the scenarios. Although the outcome of the Chi-square test did not produce a statistically significant results (i.e. except in one scenario case), the frequency of participants who opt for scale (i.e. point 5-7 – “Yes”) are consistently high. It is believed that given the bigger sample size and different range of end-users’ background might give different impact in regards to the experiments conducted (i.e. testing the hypotheses). Having said that, it can be ascertained that the direction of this research can be expanded further in order to improve the risk communication. On the other hand, it can be noted that the total of participants in this survey is quite low. Given bigger sample size, the results might be different. In addition to that, the effects of habituation in security warnings (i.e. with the usage of signal icons and signal words) potentially can be experimented to find the cause for failure in attention towards warning. In conclusion, this research has shown that the signal words and icons in warnings via symbolism are essential elements in security warnings presentation. Hence the usability of security warning can be further improved for a better risk communication.

ACKNOWLEDGMENT

Token of appreciation to those participate directly or indirectly in this work. This work is supported by a short term grant from the Universiti Sains Malaysia (USM) [304/PKOMP/6313287].

REFERENCES

- [1] B. Jung, I. Han, and S. Lee, “Security threats to Internet: a Korean multi-industry investigation.” *Information & Management*. 38, 8, 2001 pp. 487-498.
- [2] Microsoft, “Warning Messages.” [Online]. Available at: <https://msdn.microsoft.com/en-us/library/dn742473.aspx>, 2015.
- [3] Thermopylae, “Human process visual data better.” [Online]. Available at: <http://www.t-sciences.com/news/humans-process-visual-data-better>, 2014.
- [4] S. M. Furnell, A. Jusoh, D. Katsabas and P. S. Dowland, “Considering the usability of end-user security software”, Proceedings of 21st IFIP International Information Security Conference (IFIP SEC 2006). Karlstad, Sweden, 2006, pp. 307-316.
- [5] Z. F. Zaaba, S. M. Furnell, and P. S. Dowland, “A study on improving security warnings.” In proceedings of the Fifth International Conference on Information and Communication Technology for The Muslim World (ICT4M). Kuching, Malaysia, 2014, pp. 1-5.
- [6] C. Bravo-Lillo, L. F. Cranor, J. S. Downs, S. Komanduri and M. Sleeper, “Improving computer security dialogs.” *Human-Computer Interaction – INTERACT 2011*, 6949, 2011, pp. 18-35.
- [7] S. Egelman, L. F. Cranor and J. Hong, “You’ve been warned: an empirical study of the effectiveness of web browser phishing warnings.” In proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems. Florence, Italy, 2008, pp. 1065-1074.
- [8] S. Chiasson, M. Modi and R. Biddle, “Auction hero: The design of a game to learn and teach about computer security.” In World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, 2011, pp. 2201–2206.
- [9] N. Virvilis, A. Mylonas, N. Tsalis, and D. Gritzalis, “Security Busters: Web browser security vs. rogue sites” *Computers & Security*, 52, 2015, pp. 90-105.
- [10] M. S. Wogalter, “Purposes and scope of warnings.” *Handbook of Warnings*, USA: Lawrence Erlbaum Associate, ISBN 0-8058-4724-3, 2006, pp. 3-9.

- [11] W. A. Rogers, N. Lamson, and G. K. Rousseau, "Warning research: An integrative perspective." *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 42, 1, 2000, pp. 102-139.
- [12] C. Bravo-Lillo, "Improving computer security dialogs: An exploration of attention and habituation." Phd Thesis. Carnegie Mellon University, 2014.
- [13] T. Whalen and K. M. Inkpen, "Gathering evidence: use of visual security cues in web browsers." *Graphics Interface*, 2005, pp. 137-144.
- [14] Z. F. Zaaba and K. B. Teo, "Examination on usability issues of security warning dialogs". *Journal of Multidisciplinary Engineering Science and Technology*, 2, 6, 2015, pp. 1337-1345.
- [15] T. S. Amer, and J. B. Maris, "Signal words and signal icons in application control and information technology exception messages – hazard matching and habituation effects." *Journal of Information Systems*, 21, 2, 2007, pp. 1-22.
- [16] M. M. Althobaiti and P. Mayhew, "Users' awareness of visible security design flaws" *International Journal of Innovation, Management and Technology*, 7, 3, 2016, pp. 96-100.
- [17] L. Zhang-Kennedy, "Improving mental models of computer security through information graphics." Msc. Thesis, Carleton University, 2013.
- [18] D. Betram, "Likert Scales." Topic Report, The Faculty of Mathematics University of Belgrad, 2009.
- [19] K. Krol, M., Moroz and M. A. Sasse, "Don't work. Can't work? Why it's time to rethink security warnings." In proceedings of the Seventh International Conference on Risks and Security of Internet and Systems (CRiSIS). Cork, Ireland, 2012, pp. 1-8.
- [20] C. Albrecht, "Contingency Tables and the Chi Square Statistic." [Online]. Available at: <https://extension.usu.edu/evaluation/files/uploads/Start%20Your%20Engi/Study%20the%20Route/Analyze%20the%20Data/Interpreting%20Chi%20Square.pdf>, n.d.
- [21] E. McCrum-Gardner, "Which is the correct statistical test to use?" *British Journal of Oral and Maxillofacial Surgery*, 46, 1, 2008, pp. 38-41.
- [22] Windows Security, "Using Windows Security Center." [Online]. Available at: <http://windows.microsoft.com/en-ca/windows-vista/using-windows-security-center>, 2010.
- [23] F. Raja, K. Hawkey, S. Hsu, K. L. C. Wang, and K. Beznosov, "A brick wall, a locked door, and a bandit: A physical security metaphor for firewall warnings", Proceedings of the Seventh Symposium on Usable Privacy and Security. Pittsburgh, USA, 2011, pp. 1-20.