Fear Assessment in Information Security Dialog Box based on Hybrid Kansei Engineering and KJ Method

Noor Afiza MAT RAZALI*, Nurjannatul Jannah Aqilah MD SAAD*, Muslihah WOOK*, Nor Asiakin HASBULLAH*, Normaizeerah MOHD NOOR* and Khairul Khalil ISHAK**

* National Defence University of Malaysia, Kuala Lumpur, Malaysia
** Management and Science University, Shah Alam, Malaysia

Abstract: Emotion is one of the predetermined aspects that lead to non-compliance behaviour by a user in the Information Security (IS) domain. Four prominent emotions have been recognized in IS, which are fear, stress, trust, and rage. In this study, fear will be highlighted as the scope to explain fear in IS through design concept. This paper discusses how to characterize fear as stimuli for user emotional assessment in IS through the design concept of information security dialog user interface design (UID). Recent research made by other researchers shows that too low and too high levels of fear lead to user reluctance and resistance behaviour. Thus, it is essential to conduct a study to suggest methodology and procedural details in measuring fear and propose the relationship between the level of fear and user compliance behaviour toward IS procedures and policies. This study adopted part of Kansei Engineering, and KJ Method in measuring fear towards IS dialog box UID as the artefact. This study characterizes fear emotion in the IS domain based on users’ compliance response towards the artefacts. Findings from this study will give a new perspective on emotion, particularly for fear toward design in the IS domain and serve as the foundation of emotion in the IS field concerning Kansei and Affective Sciences.

Keywords: Information security, Emotion, Kansei, KJ method, Affective, Fear

1. INTRODUCTION

Leaked information can convey severe loss towards an organization and data or information stored in organizations have the risk of being affected by security incidents such as information breached and espionage [1-3]. This is due to various threats present externally or internally. According to Jouini et al. [4], external threats could be classified as an outer factor that could compromise an organization’s security in the event of a natural and artificial disaster such as flood, hurricane, landslide, terrorism, etc. Meanwhile, internal threats come directly from the organizations’ staff or workers that have authority in accessing the organization’s critical system. Hence, the Information security (IS) policy role is crucial in governing employees’ actions according to organizations’ rules, standards and procedures [5]. However, despite having a well-constructed policy and procedure, employees of an organization tend to perform non-compliance action, either unintentionally or intentionally, that will result in a security breach [6, 7]. A study also shows that non-compliance behaviour against security procedure also being influenced by emotions [8]. Previous studies suggest that prominent human emotional traits in IS realm are rage, trust, fear, and stress [9-15]. In this study, we choose fear as the scope of study due to the essential aspect of fear in keeping user compliance towards any security procedure [16]. Researchers are discussing and observing characteristics of design elements and its relationship with emotion [17-22]. However, the dimension of emotion is impulsive and measuring emotion is a huge challenge, especially in assimilating emotion with a design concept for the IS domain due to a lack of existing methodology.

This study investigates relationships between fear and IS dialog box user interface design (UID), which indirectly correlate to user IS procedure compliance. Hence, this study adopts Kansei Engineering (KE) methodology since KE has been established as a compatible method in understanding emotion and psychology in various fields through design. To further simplified the process, KJ method also is employed. This research contributes to the conceptualization of fear in the IS domain and Human-Computer Interaction field by explaining fear based on the design elements in IS dialog box UID and discussing the impact of fear in UID design that could be utilized in shaping user action towards IS policy compliance.
2. BACKGROUND AND RESEARCH MOTIVATION

2.1 Information Security (IS)

The IS well-known basic triage is confidentiality, integrity, and availability, or the CIA triad. Security of information that evolves inside an organization is critical as there might be any sensitive information and users’ affective behaviour being shared through [26].

There are several guidelines of IS procedures established for users to comply with the IS policy [9, 23-25, 27-29]. On the other hand, to cope with threats such as virus and malware, there are different technical security protection used. However, employees of the organization are the entity that seldom complies with the IS technical procedure or instruction that was given, which places the organization assets and information in great danger [30]. Study shows that the actual use and adaption of IS policy are still low among the users [31]. Generally, when formulating any IS policies or procedures, human factors are the most vital entity to consider because the non-compliance behaviours are influenced by emotions [32, 33].

2.2 Relationship of Fear and IS

Fear is a basic human emotion defined as any response taken towards a certain situation determined as risky as promoting precautionary motivation and self-protect action [34]. Individual users within an organization need to trust each other in safekeeping the information. Technical staff needs to trust users who access the information while obeying all the policies and safety requirements. Protection Motivation Theory (PMT) was used as a framework to understand the impact of fear appeals by findings crucial and important stimulus on fear appeal through earning information on perseveres of efficacy, expectancy behaviour of people upon exposure of the event and thus describe coping action of response [35-37]. PMT also captures fear traits on three elements which are (a) perceived severity, (b) perceived vulnerability, and (c) fear- arousal [38, 39]. Fear appeals have great potential for stimulating behavioural change if used correctly. Studies have shown that two types of employees’ adherence behaviours are compliance and deference [40, 41]. However, if an individual is exposed to a fear appeal that does not arouse a personally relevant perception of threat, then no appraisal of efficacy will occur [36-38].

Persuasive messages can be embedded into security communication applications, such as warning box and pop-up dialog box [42]. Siponen suggested incorporating a persuasive message towards the user in generating behaviour that could contribute to security procedure compliance [43]. However, too high fear inducement could lead to a defensive act of user while too low fear inducement will have resulted in user neglection toward security procedure [44].

Thus, fear appeal had been generally found as an effective tool in attitude change. Applying fear appeals in the IS is highly needed as fear appeals provide educational and motivating information [45, 46]. A combination of interactivity and fear appeals is more effective compared to interactivity alone. The effectiveness on positive attitude change can be seen when a lower amount of fear was induced into a certain communication rather than applying a higher amount of fear [47]. The amount of fear could be described as the level of fear. A high level of fear is often ineffective as it contains too much on the specification and characterizing of harmful consequence alongside with recommendation process change of behaviour [48]. This resulted a defensive act of user by avoiding warning messages, minimizing the severity of threats, or even denying its relevance [42]. People have invulnerability illusions caused by fear, anxiety, and stress associated with perceived threats. People with higher vulnerability to any threats will be less likely to perform any security procedures than those who perceived lower vulnerability to any threats [46].

Based on previous studies, a user’s vulnerability assumption and illusion are proven to affect a user’s tendency to perform the designated security procedures and precautions. Fear manipulation to push the user in the direction of acting towards complying IS objectives could be implemented through IS UID. However, to meet this purpose, there is a need to find the ideal fear level induced by the user via the IS UID. Also, to reach that goal, fear measurement conceptualization significantly needs to be addressed.

2.3 Kansei and KJ Method

Measuring emotion through artefact has been widely implemented in KE to incorporate the emotional appeal in the product design, resulting in precise results regarding human emotion upon an artefact. The Kansei method frequently being used in expressing people’s emotions and feeling once they see a design. This method used an emotional descriptor or Kansei Word (KW) to reflect users’ emotions through self-reporting mechanisms. Besides, Kansei Word (KW) represents human emotion that triggered due to certain circumstance [49, 50]. Meanwhile, the KJ Method is a method introduced by Kawakita Jiro as a group process for establishing priorities for effective decision making [51] that also
Fear Assessment in Information Security Dialog Box based on Hybrid Kansei Engineering and KJ Method

Keen assessment is recognized as a key approach to measure fear level by instigating the IS dialog box. Sample of designs that are used as the specimens are numerous antivirus dialog box. The selection of the antivirus dialog box samples was made with the aim to measure emotions. The samples function is to capture user attention and give an alert to the users regarding the IS policy in the basic windows environment.

However, there is a gap in the methodology of determining the right level of fear inducement as too low inducement leads to neglect act while too high inducement resulted in reluctance act by the user. Past studies mainly emphasized the influence of fear emotion in the user compliance act, yet none in measuring the exact level of fear inducement needed. Based on the statement, this study adopted hybrid KE and KJ theory to characterize fear as stimuli for user emotional assessment in IS and propose the hybrid method of measuring fear using the design of an antivirus dialog box.

As compared to other methods, KE is a method that is specifically used in developing a new concept of product associate with consumer’s implicit needs on product design. However, the selection of Kansei Word (KW) using full KE methodology will result in the complexity of determining research samples due to a large number of design elements and selecting Kansei Word (KW) of fear emotion in IS domain. It would lead to difficulty in analyzing and interpreting data. Thus, in this study, KJ Method was adopted to choose one word that represents the KW for fear.

3. CHARACTERIZING FEAR AS STIMULI IN INFORMATION SECURITY DIALOG BOX

In characterizing fear as stimuli for user emotional assessment, the connection of user’s fear IS components need to be developed. Based on the literature reviews, we suggested that fear elements in the IS will need to be elaborated according to the level of fear that the users should consider during the IS implementation. This is vital for safeguarding the information and assets using IS security dialog box as the artefact. Hence, we propose that level of fear should be determined in this study by defining each fear level by adopting an appropriate quantitative method to explain any phenomenon or condition by analyzing numerical data using mathematical methods.

Figure 1 shows our research design on characterizing fear as stimuli for user emotional assessment in IS dialog box. In this research, we discuss how the emotion assessment in IS can be conceptualized by utilizing the proposed methodology to achieve the research objectives within our research scope. In this research design, we suggested that fear elements in the IS must be conceptualized according to the different levels of fear that the users should concern about the IS implementation objectives for safeguarding the information and assets. Figure 1 shows that the design elements comprise computer security dialog box characteristic including box colours, icons, box characteristics, and contents. The level of fear proposed to be determined by analyzing respondents’ responses to numerous physical traits (design element characteristics) set as the samples in this study. Meanwhile, the KE methodology adopted to define KW with the list of potential KW extracted from PANAS-X, DEQ and Brisque Emotion. In the research design, we also expressed that the quantitative analysis method was employed.

In this research, we determine that is vital to observe how the artefacts that we set according to the items and category of the design will affect the user’s fear. We assume that the right level of fear in a dialog box design will be able to catalyse user compliance towards IS policy implementation. Finding the right amount of fear that needed to be injected in the IS dialogue box design need to be determined based on the analysis data.

4. RESEARCH METHODS

The hybrid method of KE and KJ method is adopted as the emotion measurement method. We performed user emotional assessment in IS based on our hypotheses below:
1) The fear assessment could be done by measuring fear through the artefacts using hybrid KE and KJ methods
2) Design elements characteristics in IS Dialog Box UID has a significant relationship with fear and could be proven through quantitative data analysis
In characterizing fear as the Kansei stimuli, the experimental process flow is shown in Figure 2. The research process includes instrument preparation steps, preparation for emotion measurements by preparing the specimens, and KW. Then, after the data gathering process was completed, the emotion conceptualization process was delivered. Based on the data, a summary of the guide list was completed. A total of 75 students participated in the evaluations. The students are those who know about Information Security as they are from the Security Course of Faculty of Defence Science and Technology, National Defence University of Malaysia (UPNM). Figure 2 shows the flow and research scope of this study. In this study, the Independent Variable (IV) in this study is the Design Element of the information security dialog box, while the Dependent Variable (DV) is the emotion (fear). The intended result of this study is to propose a guide list of IS dialog box design requirements that embeds the respective level of fear emotion.

4.1 Research Instrument Preparation
Research instrument of this study consisting phases of Preparation of Specimens and Kansei Checklist Development. Both phases in this study are done by adopting Kansei Design Model (KDM) [50].

4.1.1 Preparation of Specimens
The specimen in this research refers to IS dialog box selected from the existing antivirus software application and based on the criterion of UID elements. The extraction of UID of IS dialog box is done through literature review regarding antivirus dialog box UID. Each criterion of the specimen’s design element was then analysed to investigate the possible visible elements to the user’s eye. This is parallel to the second process of Investigation of Design Elements.

In this process, KE Type 1 or known as the KE Pack technique, was adopted. KE Type 1 technique involves different samples collecting and classification according to Item, which is the element’s design.

In this study, color, type, size, box position, the content of the message, font size, and font style are set as the Item. Meanwhile, the design element category that functions as the attribute of each specified item is set accordingly, as shown in Table 1. This process is the third process of Classify Design Elements.

The process of Classifying Design Element was carried out by finalizing specimens through the matrix box of specimens and design elements. The process began with checking design value that makes up the appearance of IS dialog box. If a specimen matched the investigated design element, thus the matrix box was checked. However, if there are more than two specimens are checked for the same design elements. Thus, the specimens were invalid and not selected. As an example, Specimen A, Specimen B and Specimen C have the same colour ‘Red’ for Box Color and, Specimen A and Specimen B have the same Icon Type ‘Warning.’ Thus, all three specimens are invalid since they cross-checked the same design with each other.

The process was tested repeatedly throughout the 40 specimens. The extracted design elements determined to be the final specimens for this study are shown in Table 1, with only 12 specimens based on four items.

| Design Element Characteristic | Item | Category |
|------------------------------|------|----------|
| Box Color                    | Color| Red, Orange, Yellow, Blue, Black |
| Icon                         | Type | Warning (!), Danger (X), Other |
| Box Characteristic           | Color| Red, Yellow, White |
| In Screen Position           | Size | Big, Small, Average |
| Content                      | Message| Generic and specific message |
| Font Size                    | Font Size| Small (8pt,10pt), Medium (12pt,14pt) |
| Font Style                   | Font Style| Italic, Bold, Normal |
4.1.2 Kansei Checklist Development

The checklist in this research referred to the measurement tool in investigating the user’s emotional response towards information security dialog box UID. A complete checklist will consist of target emotional words or known as Kansei Word (KW), with a self-reporting system scale. The selection of Kansei Word (KW) is made by adopting the KJ method.

As this research focuses only on the fear emotion dimension, we conducted one activity to pinpoint one word that represents the user fear in the IS domain. We employ the suggestion from an expert in a language field to find the most suitable word that represents fear in the IS domain. Multiple wording representing the fear word (synonym) will result in an inaccurate analysis of data as this research only focused on one dimension of emotion. Thus, to attain only one fear word that can represent fear in the IS domain accurately, we executed a polling or voting procedure. The fear words were extracted from the PANAS-X scale [60], DEQ scale [61], and Basque Emotion Lexicon scale [62], as shown in Figure 3.

The result from the procedure indicated ‘Jittery’ was most participants choose with nine votes, and it is shown that word was most reflecting the fear and was selected to be used in Checklist afterwards. Other’s word gets less vote from participant such as ‘Scared’ (7 votes), ‘Afraid’ (6 votes), ‘Worry,’ ‘Nervous,’ ‘Alarm (5 votes),’ Frightened’ (4 votes), ‘Uneasiness’ (3 votes) and Shaky (1 vote).

4.2 Evaluation Process

The Kansei evaluation process of this research is carried out in a controlled environment of two sessions. There are 20 students for the first session and 30 students for the second session. The activities session was divided into two sessions due to a reason to perform the evaluation process work smoothly and get stable communication between instructors and participants. The evaluation starts with a simple overview of research for better understanding and a simple briefing on consents and instructions. A Kansei checklist given to participants to evaluate IS dialog box samples of software application UID is shown through the projector. Participants were needed to evaluate a 5-point of Semantic Differential (SD) scale concerning their fear feeling after watching each sample of IS dialog box UID specimens shown by the instructor. An example of IS dialog box UID specimens shown to participants is as in Figure 4.

5. RESULT AND DISCUSSION

SPSS software was used to identify the relationship between fear emotion and the specific design of the IS dialog box category that is referred to as the artefacts. The design was characterized by items and for each item, relevant categories being established. The artefacts are expected to assist in the fear measurement toward the artefact. In developing the Checklist, a reliability test called Cronbach Alpha was employed to measure the checklist result’s reliability. Alpha Cronbach’s average value was to be exceeded or equal to 0.7 and Alpha Cronbach’s value for this experiment was 0.938, which is higher than the value obtained in our research shows high internal consistency of the Checklist. The Kansei participant’s procedure responses were then computed to determine the mean, minimum and maximum value. Analysis of the results is continued with Factor Analysis (FA).

FA was conducted to find the significant factor of design that embeds target emotion (fear) for IS dialog box. FA is performed through Principal Axis Factoring with Varimax rotation in SPSS v21. FA resulted that Component 1 has the highest Eigenvalues of 18.312 compared to other components. Figure 5 shows the plotted graph of Factor Loadings in ascending order. The plotted graph in ascending order is to provide better visualization of factor loadings values which fear emotion embeds in each design element held.
Hence, from the result, it can be said that design element characteristics from 0.81 to 0.877 could be defined as design elements that generate a high level of fear. Meanwhile, design element characteristics from 0.425 to 0.73 could be defined as design elements that generating a low level of fear. Based on our results, we concluded that design element characteristics from 0.749 until 0.778 could be defined as design elements that generate a medium level of fear.

In Table 2, we summarize the factor loadings of IS dialog box design elements characteristics based on the generated level of fear from the FA results. For box characteristics, from the 12 specimens that were used in this study, all the specimens did not specify any fear characteristics differences. Nevertheless, design elements characteristic with items Content, [Font Size: ‘8pt’ and ‘2pt’; Font Style: ‘Normal,’ ‘Bold’; Icon Type ‘Danger’; Icon and Box Color: ‘White,’ ‘Yellow’] fall under design element characteristic that generates a high level of fear. Design elements characteristic with items Content, [Font Size: ‘10pt’, ‘14pt’; Font Style: ‘Italic’; Box Color: Orange] fall under design element characteristic that generates a medium level of fear. However, the message’s content in the IS dialog box specimen that shows a medium level of fear was not able to be observed. Meanwhile, Design elements characteristic with items Content, [Content IS Dialog Box: Generic Message; Box Color: Red, Black, Blue] fall under design element characteristic that generates a low level of fear. However, ‘Font Size’ and ‘Font Style’ that specifically generate a low level of fear could not be observed.

IS dialog box UID that mapped to a specific level of fear, as shown in Table 2 can be used as a foundation to IS dialog box UID design that could induce fear emotion. Based on the previous research discussed, the fear appeal had been generally found as an effective tool in influencing users’ attitudes and behaviour. The level of fear emotion for users could relate to user IS policy compliance. Designs of IS dialog box UID could be utilized to induce fear in users. By manipulating fear, the users could be catalysed to complying with the IS policies set by an organization. This study provides the finding that shows the design characteristic that could inject a low, medium, and high level of fear based on the data that we collected in our study. Figure 6 and Figure 7 show the IS dialog box UID that was corresponding to the low and high level of fear respectively.

**Table 2**: IS dialog box UID characteristics and the level of fear

| Design Element Characteristic   | Category               | Low    | Medium | High   |
|--------------------------------|------------------------|--------|--------|--------|
| **Box Size**                    | Big, Medium, Small    | N/A    | N/A    | N/A    |
| **Position**                    | Center, Upper Left, Upper Right, Bottom Left | Bottom Right, | N/A    |
| **Font Size**                   | N/A                   | 10pt, 14pt | 8pt, 12pt |
| **Font Style**                  | N/A                   | Italic | Normal, Bold |
| **Message**                     | N/A                   | Specific Message |
| **Color**                       | Red                   | N/A    | White, Yellow |
| **Type**                        | N/A                   | Other, Warning | Danger |
| **Box Color**                   | Red, Black, Blue      | Orange | White, Yellow |
Fear Assessment in Information Security Dialog Box based on Hybrid Kansei Engineering and KJ Method

6. CONCLUSION AND FUTURE WORKS

This study shows the conceptualization of fear emotion in the IS domain based on users’ compliance response towards the artefacts. The artefacts include design components that were constructed based on IS dialog box UID. Our quantitative data gathering has proven our hypothesis that there is a significant relationship between fear emotion and IS dialog box UID design characteristic.

We obtained results through quantitative analysis to proven that the design and fear relationship could be measured clearly by utilizing KE and KJ methods. However, in this study, the specimens that were limited give limitations to the overall results. In our future work, the specimen will be further enhanced with more diversity to represent broader design characteristics to obtain more comprehensive results.

Based on our findings, we suggest the characterization of IS dialog box UID that embeds a different level of fear can influence users’ attitudes and behaviour. On the other hand, the right amount of fear that could influence user behaviour towards IS policy compliance is subjective. The right amount of fear could be illustrated as the level of fear that impacts the user’s compliance towards IS policy. Our finding characterizes the design of IS dialog box UID and the relationship with fear. However, finding the right amount of fear that gives the optimum impact on IS policy compliance is the next field that need to be explored comprehensively. Inducement of fear through IS dialog box UID that has an optimum impact on the user’s attitude and behaviour and guarantees user’s compliance towards IS policy is the ultimate goal that could benefit the IS realm.

ACKNOWLEDGEMENTS

This research was supported by the Malaysia Ministry of Higher Education, under the grant of FRGS FRGS/1/2017/ICT04/UPNM/03/1

REFERENCES

1. Burns, A. J., Posey, C., Roberts, T. L., and Lowry, P. B.; Examining the relationship of organizational insiders’ psychological capital with information security threat and coping appraisals, Computers in Human Behavior, 68, pp.190-209, 2017, doi: 10.1016/j.chb.2016.11.018.
2. Gundu, T., and Flowerday, S. V.; Ignorance to awareness: Towards an information security awareness process, SAIEE Africa Research Journal, 104(2), pp.69-79, 2013.
3. Ö˘ütçü, G., Testik, Ö. M., and Chouseinoglou, O.; Analysis of personal information security behavior and awareness, Computers & Security, 56, pp.83-93, 2016, doi: 10.1016/j.cose.2015.10.002.
4. Jouini, M., Rabai, L. B. A., and Aissa, A. B.; Classification of security threats in information systems, Procedia Computer Science, 32, pp.489-496, 2014, doi: 10.1016/J.PROCS.2014.05.452.
5. Siponen, M., and Vance, A.; Neutralization: New insights into the problem of employee information systems security policy violations, MIS Quarterly, 34(3), pp.487-502, 2010, doi: 10.2307/25750688.
6. Johnston, A. C., Warkentin, M., and Siponen, M.; An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric, MIS Quarterly, 39(1), pp.113-134, 2015, doi: 10.25300/MISQ/2015/39.1.06.
7. Shropshire, J., Warkentin, M., and Sharma, S.; Personality, attitudes, and intentions: Predicting initial adoption of information security behavior, Computers & Security, 49, pp.177-191, 2015, doi: 10.1016/j.cose.2015.01.002.
8. Wrigley, C., Gomez, R., and Popovic, V.; The evaluation of qualitative methods selection in the field of design and emotion, Proceedings of the 7th International Conference on Design and Emotion, 2010.
9. Warkentin, M., and Willison, R.; Behavioral and policy issues in information systems security: The insider
threat, European Journal of Information Systems, 18(2), pp.101-105, 2009, doi: 10.1057/ejis.2009.12.
10. Son, J.; Information & management out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies, Information & Management, 48(7), pp.296-302, 2011, doi: 10.1016/j.im.2011.07.002.
11. D’Arcy, J., Herath, T., and Shoss, M. K.; Understanding employee responses to stressful information security requirements: A coping perspective, Journal of Management Information Systems, 31(2), pp.285-318, 2014, doi: 10.2753/MIS0742-1222310210.
12. Henshel, D., Cains, M. G., Hoffman, B., and Kelley, T.; Trust as a human factor in holistic cyber security risk assessment, Procedia Manufacturing, 3, pp.1117-1124, 2015, doi: 10.1016/j.promfg.2015.07.186.
13. Ishak, K. K., Razali, N. A. M., Lokman, A. M., and Kinoshita, T.; Kansei Information Security Assessment (KISA): Characterizing trust as stimuli for user emotional assessment in information security, Indian Journal of Science and Technology, 9(S1), pp.1-6, 2016, doi: 10.17485/ijst/2016/v9is1/106846.
14. Bansal, G., Zahedi, F. M., and Gefen, D.; Do context and personality matter? Trust and privacy concerns in disclosing private information online, Information & Management, 53(1), pp.1-21, 2016, doi: 10.1016/j.im.2012.04.002.
15. Saad, N. J., Afiza, M. R., Ishak, K. K., Hasbullah, N. A., Zainudin, N., Ramli, S., Wahab, N., and Amran, M. F.; Fear as emotion assessment in information security using Kansei engineering methodology, Proceedings of the 7th International Conference on Kansei Engineering and Emotion Research, pp.654-663, 2018.
16. Vance, A., Siponen, M., and Pahnila, S.; Motivating IS security compliance: Insights from habit and protection motivation theory, Information & Management, 49(3-4), pp.190-198, 2012, doi: 10.1016/j.im.2012.04.002.
17. Demirbilek, O., and Sener, B.; Product design, semantics and emotional response, Ergonomics, 46(13-14), pp.1346-1360, 2003, doi: 10.1080/00140130310001610874.
18. Ou, L. C., Luo, M. R., Woodcock, A., and Wright, A.; A study of colour emotion and colour preference, Part III: Colour preference modeling, Color Research and Application, 29(5), pp.381-389, 2004, doi: 10.1002/col.20047.
19. Ürgen, C.; The use and importance of emotional design in contemporary design practice, Thesis (Master), Izmir Institute of Technology, 2006.
20. Desmet, P. M. A., Porcelijn, R., and Van Dijk, M. B.; Emotional design; Application of a research-based design approach, Knowledge, Technology & Policy, 20(3), pp.141-155, 2007, doi: 10.1007/s12130-007-9018-4.
21. Ho, A. G., and Siu, K. W. M.; Emotionalise design, emotional design, emotion design: A new perspective to understand their relationships, Proceedings of the International Association of Societies of Design Research (IASDR) Conference, 2009.
22. Khodaddeh, Y., and Rostamkhani, S.; Emotional design: Study of the colour preferences of Iranian users, Proceedings of the 11th Engineering and Product Design Education Conference-Creating a Better World, pp.244-250, 2009.
23. Bulgurcu, B., Cavusoglu, H., and Benbasat, I.; Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, MIS Quarterly, 34(3), pp.523-548, 2010, doi: 10.2307/25750690.
24. Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J.; Analysis of end user security behaviors, Computers and Security, 24(2). pp.124-33, 2005, doi: 10.1016/j.cose.2004.07.001.
25. Vroom, C., and Von Solms, R.; Towards information security behavioural compliance, Computers & Security, 23(3), pp.191-198, 2004, doi: 10.1016/j.cose.2004.01.012.
26. Pahnila, S., Siponen, M., and Mahmood, A.; Which factors explain employees’ adherence to information security policies? An empirical study, Proceedings of the Pacific Asia Conference on Information Systems, PACIS 2007, pp.438-439, 2007, doi: 10.1007/978-0-387-72367-9_12.
27. Herath, T., and Rao, H. R.; Protection motivation and deterrence: A framework for security policy compliance in organisations, European Journal of Information Systems 18(2), pp.106-125, 2009, doi: 10.1057/ejis.2009.6.
28. Kabay, M. E., Robertson, B., Akella, M., and Lang, D. T.; Using social psychology to implement security policies, Bosworth, S., Kabay, M. E., and Whyne, E. (eds), Computer security handbook, 50, 2012.
29. Kraemer, S., Carayon, P., and Clem, J.; Human and organizational factors in computer and information security: Pathways to vulnerabilities, Computers & Security, 28(7), pp.509-520, 2009, doi: 10.1016/j.cose.2009.04.006.
30. Pahnila, S., Siponen, M., and Mahmood, A.; Employees’ behavior towards IS security policy
Fear Assessment in Information Security Dialog Box based on Hybrid Kansei Engineering and KJ Method

31. Wang, P.A.; Information security knowledge and behavior: An adapted model of technology acceptance, Proceedings of the 2nd International Conference on Education Technology and Computer, vol.2, pp.364-367, 2010, doi: 10.1109/ICETC.2010.5529366.

32. Harley, J.M., Bouchet, F., Hussain, M.S., Azevedo, R., and Calvo, R.; A multi-componential analysis of emotions during complex learning with an intelligent multi-agent system, Computers in Human Behavior, 48, pp.615-625, 2015, doi: 10.1016/j.chb.2015.02.013.

33. Aytes, K., Conolly, T., and Connolly, T.; A research model for investigating human behavior related to computer security, Proceedings of the 9th Americas Conference on Information Systems, pp.2027-2031, 2003, [Online]. Available: http://aisel.aisnet.org/amcis2003/260/0A.

34. Ortony, A., and Turner, T.J.; What’s basic about basic emotions?, Psychological Review, 97(3), pp.315-331, 1990, doi: 10.1037/0033-295X.97.3.315.

35. Mwagwabi, F., McGill, T., and Dixon, M.; Short-term and long-term effects of fear appeals in improving compliance with password guidelines, Communications of the Association for Information Systems, 42(1), pp.147-182, 2018, doi: 10.17705/ICAIS.04207.

36. Rogers, R.W.; A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), pp.93-114, 1975, doi: 10.1080/00223980.1975.9915803.

37. Maddux, J.E., and Rogers, R.W.; Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change, Journal of Experimental Social Psychology, 19(5), pp.469-479, 1983, doi: 10.1016/0022-1031(83)90023-9.

38. Skotnes, R. Ø.; Persuading end users to act cautiously online: A fear appeals study on phishing, Information and Computer Security, 23(3), pp.302-316, 2015, doi: http://dx.doi.org/10.1108/ICS-01-2015-0001.

39. Milne, S., Sheeran, P., and Orbell, S.; Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory, Journal of Applied Social Psychology, 30(1), pp.106-143, 2000, doi: 10.1111/j.1559-1816.2000.tb02308.x.

40. Witte, K.; Putting the fear back into fear appeals: The extended parallel process model, Communication Monographs, 59(4), pp.329-349, 1992, doi: 10.1080/03637759209376276.

41. Son, J., and Rhee, H.-S.; Out of fear or desire: Why do employees follow information systems security policies?, Proceedings of the 13th Americas Conference on Information Systems, pp.1-6, 2007.

42. Du, H., Xu, H., Rosson, M.B., and Carroll, J.M.; Effects of fear appeals and point of reference on the persuasiveness of IT security communications, Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics, pp.82-84, 2013, doi: 10.1109/ISI.2013.6578791.

43. Siponen, M.T.; A conceptual foundation for organizational information security awareness, Information Management & Computer Security, 8(1), pp.31-41, 2000.

44. Xu, H., Rosson, M., and Carroll, J.; Increasing the persuasiveness of IT security communication: Effects of fear appeals and self-view, In Workshop on Usable IT Security Management, Symposium on Usable Privacy and Security (SOUPS), pp.1-4, 2007.

45. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A.; What levels of moral reasoning and values explain adherence to information security rules? An empirical study, European Journal of Information Systems, 18(2), pp.126-139, 2009, doi: 10.1057/ejis.2009.10.

46. Workman, M., Bommer, W.H., and Straub, D.; Security lapses and the omission of information security measures: A threat control model and empirical test, Computers in Human Behavior, 24(6), pp.2799-2816, 2008, doi: 10.1016/j.chb.2008.04.005.

47. Janis, I. L., and Feshbach, S.; Effects of fear-arousing communications, The Journal of Abnormal and Social Psychology, 48(1), pp.78-92, 1953, doi: 10.1037/h0060732.

48. Keller, P.A., and Block, L.G.; Increasing the Persuasiveness of fear appeals: The effect of arousal and elaboration, Journal of Consumer Research, 22(4), pp.448-459, 1996, doi: 10.1086/209461.

49. Lokman, A.M., and Kamaruddin, K.A.; Kansei affinity cluster for affective product design, 2010 International Conference on User Science and Engineering (iUSEr), pp.38-43, 2010, doi: 10.1109/IUSER.2010.5716719.

50. Lokman, A.M.; KE as affective design methodology, Proceedings of the 2013 International Conference on Computer, Control, Informatics and Its Applications (IC3INA), pp.7-13, 2013.

51. Scupin, R.; The KJ method: A technique for analyzing data derived from Japanese ethnology, Human Organization, 56(2), pp.233-237, 1997, doi: 10.17730/humo.562.x335923511444655.

52. Krol, K., Moroz, M., and Sasse, M.A.; Don’t work.
Can’t work? Why it’s time to rethink security warnings. Proceedings of the 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), pp.1-8, 2012, doi: 10.1109/CRISIS.2012.6378951.

53. Bravo-Lillo, C. C., Cranor, L. F., Downs, J., Komanduri, S., Reeder, R.W., and Schechter, S.; Your attention please: Designing security-decision UIs to make genuine risks harder to ignore, SOUPS ‘13: Proceedings of the Ninth Symposium on Usable Privacy and Security, pp.1-18, 2013, doi: 10.1145/2501604.2501610.

54. Zaaba, Z. F., Furnell, S. M., and Dowland, P. S.; A study on improving security warnings, Proceedings of the 5th International Conference on Information and Communication Technology for the Muslim World, (ICT4M), pp.1-5, 2014, doi: 10.1109/ICT4M.2014.7020633.

55. Mei, Y., and Lebin, J.; Study on Kansei engineering and its application to product design, Proceedings of the Second International Symposium on Computational Intelligence and Design. Vol.2, pp.525-528, 2009, doi: 10.1109/ISCID.2009.277.

56. Nagamachi, M.; Kansei engineering: A new ergonomic consumer-oriented technology for product development, International Journal of Industrial Ergonomics, 15(1), pp.3-11, 1995, doi: 10.1016/0169-8141(94)00052-5.

57. Lokman, A. M.; Design & emotion: The kansei engineering methodology, Malaysian Journal of Computing, 1(1), pp.1-11, 2010.

58. Awang, Z.; Research methodology and data analysis, Universiti Teknologi MARA Press, pp.1-321, 2012.

59. Venkatesh, V., Brown, S.A., and Bala, H.; Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems, MIS Quarterly, 37(1), pp.21-54, 2013, doi: 10.1080/14767430.2018.1454705.

60. Watson, D., and Clark, L. A.; The PANAS-X: Manual for the positive and negative affect schedule - expanded form, University of Iowa, p.24, 1994, doi: 10.17077/48vt-m4t2.

61. Blatt, S. J., D’Afflitti, J. P., and Quinlan, D. M.; Experiences of depression in normal young adults, Journal of Abnormal Psychology, 85(4), pp.383-389, 1976, doi: 10.1002/0021-843X.85.4.383.

62. Alonso-Arbiol, I., Shaver, P. R., Fraley, R. C., Oronoz, B., Unzurrunzaga, E., and Urizar, R.; Structure of the Basque emotion lexicon, Cognition and Emotion, 20(6), pp.836-865, 2006, doi: 10.1080/02699930500405469.

Noor Afiza MAT RAZALI (Non-Member)
Noor Afiza holds a bachelor’s degree in Computer and Information Engineering, Master of Science and PhD. of Science in Computer Science from Japanese Universities. Noor Afiza is an Associate Professor at the Defence Science and Technology Faculty in National Defence University of Malaysia. Her research and expertise are in the area of Cybersecurity, Disaster Management, Kansei Engineering, Human Computer Interaction, Big Data Analytics, Artificial Intelligence and Blockchain Technology. Noor Afiza also a professional technologist, a recognition given by Malaysia Board of Technologist.

Nurjannatul Jannah Aqilah MD SAAD (Non-Member)
Nurjannatul Jannah Aqilah Md Saad obtained the Master in 2020 and working in the industry after the graduation. Her research interest includes human interaction design, data mining and systems development.

Muslihah WOOK (Non-Member)
Muslihah Wook received her PhD in Information Science from Universiti Kebangsaan Malaysia in 2017, Master of Computer Science from Universiti Putra Malaysia in 2004, and Bachelor of Information Technology (Hons) from Universiti Utara Malaysia in 2001. Her research interests include data mining applications in various domain particularly in education, security and defence. Currently she is working as a senior lecturer at Department of Computer Science, Faculty of Defence Science and Technology, National Defence University of Malaysia. She has become members of International Association of Computer Science and Information Technology (IACSIT) and Institute of Research Engineers and Doctors (IRED) since 2011 and 2013 respectively. Recently, she has been appointed as a technical reviewer of Education and Information Technologies—Springer’s journal indexed by Scopus (Q2).

Nor Asiakin HASBULLAH (Non-Member)
Nor Asiakin Hashbullah received her PhD in Information Technology and quantitative sciences from MARA University of Technology Malaysia in 2017 and have done three months’ attachment in Glasgow Caledonian University of Glasgow under Privacy research in 2012. She holds a Master of Science in Information Technology from MARA University of Technology Malaysia in 2006, and bachelor of information technology (hons) from ‘University Kebangsaan’ in 2003. Currently she is a senior lecturer in the Department of Computer Science, National Defence University of Malaysia (UPNM). Her research interests are in the field of privacy, data protection, information security and ethics in ICT.

Normaizeerah MOHD NOOR (Non-Member)
Normaizeerah Mohd Noor obtained the Degree in Computer Science in 2020. She is a Research Assistant at National Defence University Malaysia. Her research interest includes human interaction design and systems analysis.

Khairul Khalil ISHAK (Non-Member)
Khairul Khalil Iskak, holds a bachelor’s degree in Engineering from Waseda University and a master’s degree from Universiti Teknologi MARA Malaysia. He is a professional in Information Technology and Engineering fields with wide experience in multiple multinational companies. Khairul is an appointed Research Fellow at the Management and Science University with research interest includes Cybersecurity, Big Data Analytics, Artificial Intelligence, Robotics, Blockchain Technology and Kansei Engineering.