Literature Studies on Security Warnings Development

Zarul Fitri Zaaba[1], Steven M. Furnell[2,3] and Paul S. Dowland[2]
1School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
2Centre for Security, Communications and Network Research, Plymouth University, United Kingdom
3School of Computer and Security Sciences Edith Cowan University Perth, Western Australia
zarulfitri@usm.my, info@cscan.org

Abstract— Security warnings are intended to alert users about the possibility of events that may compromise their protection. They encounter security warnings on daily basis in many situations when dealing with their computer. However, prior studies have shown that users often have difficulty in understanding the warnings, which can pose a particular risk in cases where they are required to make a decision. Well gathered information is needed to help the researchers and other people to further understand this area. This paper describes an overview of studies on security warnings. It covers problems that end users encounter with security warnings, possible solutions and approaches of security warnings and useful classification of security warnings studies. It is expected that this paper will benefit the academicians, research community or general public to understand the problems and possible solutions in improving security warnings.

Keywords— Security, Warning, Interface, Usability, Usable security, Human Computer Interaction,

I. Introduction

In view of increasing threats in computer usage, today's users need to be familiar with the use of security tools and how to interact with related system functionality. However, in many cases a major challenge is about the usability of the technologies because users can face difficulties in understanding them correctly and utilizing them effectively. One area that needs focus is the issue of interaction with these tools, particularly when users are presented with a warning to inform or to remind them that something untoward is happening or is going to happen.

It is not at all uncommon for users to encounter warnings in which they are presented with more than one option and there are no specific features to support them in making a decision. Often, the decision that they have to make may have significant consequences (i.e. users do not realise the impact of the decision on the security and protection of the computer). Therefore, this could jeopardize the fundamental goal of computer security (i.e. confidentiality, integrity and availability). This paper provides an overview of security warnings studies based on a review of user interactions with security tools and technologies

II. RELATED WORKS

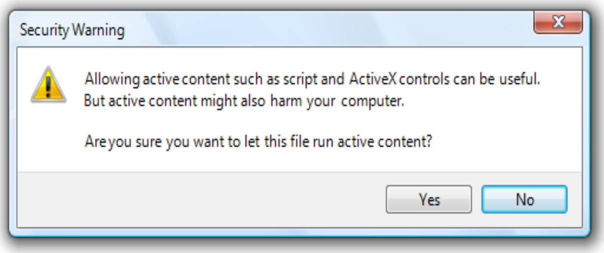
Warnings can be defined as safety communications that are used to inform people about hazards to protect them from any harm [1]. Warnings can also be defined as anything that can alert an individual's attention towards potentially dangerous circumstances [2]. Therefore, in general a warning is a method to inform about the occurrence of risks or problems in the future and it can help to protect the users from harm. A similar concept can be applied to computer warnings, as all applications (e.g. web browsers) inform users using warnings representation based on its contexts and the level of severity (e.g. dialogue box, balloons, banners, and notifications).

As a medium of communication to inform users about possible issues in computer systems, warning functions must be presentable. A user should be able to comprehend the current problems they are facing and later be guided to make better decisions. The new concept of HCI-S was introduced to make the interfaces better in regards to security [36]. Based on our investigation, many issues have been raised in relation to security warnings. However, not much focus has been given on classification approaches to improve security warnings and its architecture. This paper intends to provide some useful information to clarify these issues.

The outline of this paper is as follows: section II will explain the related work; section III with an overview of issues in security warning studies such as the problems, solutions and approaches; section IV highlights discussions on security warnings related issues; Section V explains the future works; finally, section VI ends with the conclusions.

III. OVERVIEW OF ISSUES IN SECURITY WARNINGS

Many observations and user studies have looked at various domains such as virus alerts and active browser warnings [3], online banking context [4] and privacy and policy [5]. Microsoft had taken steps to improve previous warning dialogues (i.e. defaults buttons, labels, primary text, footnote area and assistance text) [6].



Allowing active content such as script and ActiveX controls can be useful. But active content might also harm your computer.

Are you sure you want to let this file run active content?

Fig. 1 Examples of security warnings

Fig. 1 shows example of security warning which has been presented to the end-users. Based on the depicted warning, it can be noted the usage of technical jargons such as “script”, “ActiveX” and “active content” are used. A similar scenario occurs earlier in Pretty Good Privacy (PGP) 5.0 where the tool has been evaluated as not sufficiently usable [37]. The results indicate that one third of participants unable to sign and encrypt the e-mail and another one quarter exposed the secret key (i.e. breach of confidentiality and integrity).

In other context, [38] found out that usability problems still exist in the third party authentication. [39] On the other hand highlight the same problems in regards to configuration of firewall to selectively filter traffic. The implication of all these problems might lead to catastrophic outcomes (i.e. changes from secure to unsecure system). The next section determine to highlight further investigation in relation of security warning problems, challenges and approaches in improving security warnings.

A. *Further Investigation on Security Warnings Problems*

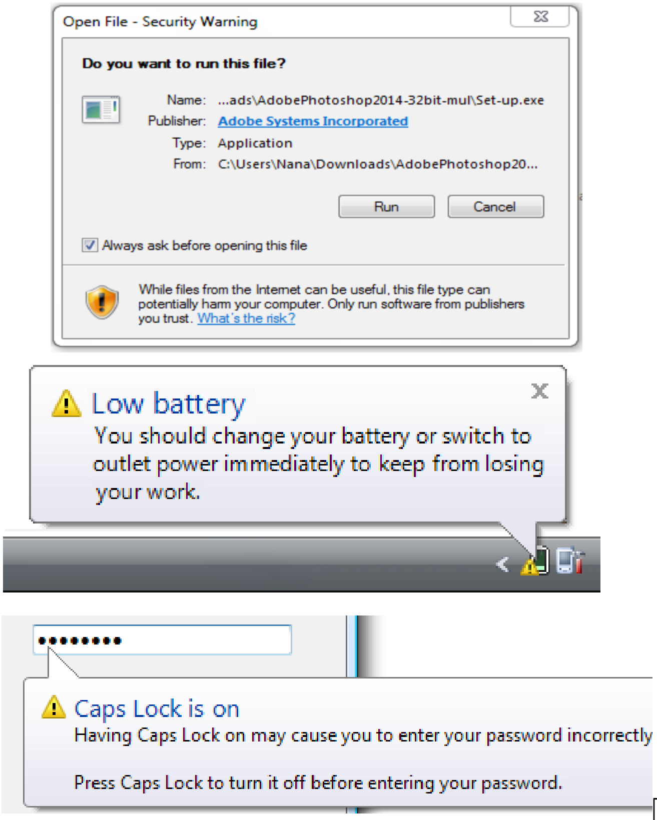
Security warnings in computer context can be classified to five different types shown in Table I [7]. Each user interface contexts works with a specified situation and Microsoft already had their own standard to implement it. Microsoft had been chosen due to its popularity and widely used by end users.

TABLE I. FIVE DIFFERENT USER INTERFACE CONTEXTS [7]

User Interface Contexts	**Suitable Usage**
Dialogue Box	Used for critical warnings that includes confirmation. Users must respond to the warning instantly (Modal dialogue box)
In-Place	Used to provide information that possibly prevents a problem. It is useful when users are making choices
Notifications	Used with significant circumstances or status that can be safely ignored by users (at least temporary)
Balloons	Used as a control in a situation that affects the input. This state is likely to be unintended and users may not realize that the input is affected.
Banners	Used to provide information that may prevent a problem. It is useful for users in completing a task

Security warnings in computer can be described as a representation of warning that diverts user’s attention to alert and notify the user on the possible consequences of an action in advance [14, 21).

Computer security warnings might be encountered while trying to open an attachment, running an application that is downloaded from the Internet or low battery level. These warning usually pop up instantly and needs immediate action. Fig. 2 shows the examples of security warning interface that user encounter while using the computer.



Open File - Security Warning

Do you want to run this file?

Name: ...ads\AdobePhotoshop2014-32bit-mul\Set-up.exe
Publisher: Adobe Systems Incorporated
Type: Application
From: C:\Users\Nana\Downloads\AdobePhotoshop20...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Low battery
You should change your battery or switch to outlet power immediately to keep from losing your work.

•••••••••

Caps Lock is on
Having Caps Lock on may cause you to enter your password incorrectly

Press Caps Lock to turn it off before entering your password.

Fig. 2 Examples of security warnings

Although there is a standard that has been used, end-users are still baffled by security warnings that they encounter on a daily basis. For instance, a user study with 30 participants conducted to prevent phishing attacks the results show that participants ignore the warning especially when the web content looked legitimate [8].

On the other hand, a web based survey involving 114 users was conducted to evaluate the effectiveness of security warnings in a web browser setting [9]. The results revealed that users still ignore the warning as it did not convince them to make a better action. In addition, respondents claimed the warning displayed did not provide with sufficient information.

An empirical study on the effectiveness of phishing warnings revealed that 43% of participant (i.e. out of 47 respondents) did not comprehend the meaning of the warning that had been presented [10].

30 respondents were interviewed in relation to computer security warnings and it showed that the novice users often did not understand the technical terminology. These users always struggle to understand the meaning of the terminology because of the technicality and the difficulty of such terms [11]. In addition, the majority of respondents indicated that the novice users were unable to make informed decision about firewall warnings [12].

A big scale survey with 340 end-users on the usability of security software was conducted and it revealed that end-users find it difficult to understand the technical terminology. About 35% of the respondents were not able to understand the ActiveX jargon in Internet Explorer [13]. The summary of the security warning problems (i.e. in relation to usability context) can be illustrated in Table II.

Based on the evidences gathered, it can be noted that end users are still facing different types of problem in relation to security warnings. It can be noted that the warnings issued are not fixed to one scenario but it covers different types of circumstances. Thus, the next section will explore the method or techniques that have been put in place to counter the problems.

Table II. USABILITY ISSUES IN SECURITY WARNINGS [22]

Usability issues	**Description and findings from past studies**
i. Attention towards security warnings	▪ Users did not pay attention to web security cues warning, and easily misidentify small icon warnings (Whalen et al. 2005). ▪ Users ignored the phishing warnings especially when the web content looked legitimate (Wu et al. 2006). ▪ Users ignore web browser warnings in the study done by Seifert et al. (2006). They argued that it was influenced by the amount of information displayed by the warnings
ii. Understanding of security warnings	▪ Users were lacking of knowledge to differentiate fake and real warnings (Sharek et al. 2008). ▪ Users failed to understand the SSL warnings in the browsers (Sunshine et al. 2009). ▪ Users did not understand the meaning of the phishing

	warnings and the indicators needed to be more distinct (Egelman et al. 2008).
iii. Usage of technical terminologies	▪ Novice users did not understand technical wordings although they were heard about it (Bravo-Lillo et al. 2011b). ▪ Most of the users do not understand technical terminologies such as the meaning of ActiveX control in Internet Explorer (Furnell et al. 2006b). ▪ User still experienced significant problems on technical jargons used in security warnings (Zaaba et al. 2011)
iv. Users' motivation	▪ Users ignore security warnings because security warnings are seen as burdens, and offer poor cost-benefit trade off (Herley, 2009).

B. Methods to Improve Security Warnings

While the usability and security seem to compromise each another, the concept of Human-Computer Interaction and Security (HCISec) had been introduced in early 2003 which recognize the importance of usability in improving security [23]

The International Standard Organization (ISO) defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (T.I.S. Organization, 1998). The usability components such as learnability, efficiency, memorability, errors and satisfaction are essential part to be included in the design as they help the users to achieve their intended goals.

HCISec is a discipline that integrating the HCI and security. User interface alone is not sufficient enough to make the system usable hence the security should be presented in a meaningful way [35]. The focal point of HCISec is given to three main aspects namely the underlying system design, user expectations and education and economics and user incentives. Thus, the designer should adapt these aspects accordingly where later it would encourage the end-users to act in secure manner.

Based on the current investigation and assessment, there is no one specific method to solve problems on security warnings. Researchers carried out various experimental studies on security warnings to explore the problems and possible solution. Table III presents a summary of studies on how to improve security warnings based on the early investigations that had been made [14].

TABLE III. SUMMARY OF STUDIES ON HOW TO IMPROVE SECURITY WARNINGS [14]

Authors	Methods/Techniques
Nodder (2005)	Proposed a new design of warning based on users' behaviour
Raja et al. (2009)	Proposed a new firewall interface design that helped users to develop a correct mental model and increased users' understanding on firewall configuration.
Bravo-Lillo et al. (2011b)	Introduced the concept of mental model on how novice and advanced users assessed security warnings.
Keukelaere et al. (2009)	Introduced Adaptive security dialogues (ASD) by matching the complexity of warning dialogues and the risk associated
Edwards et al. (2007)	Introduced security automation concept where decision is made by the system
Bravo-Lillo et al. (2011)	Proposed design changes that are able to help end-users to make better decision in relation to warning interaction.
Kauer et al. (2012)	Proposed that the risk should be communicated clearly in order to deliver the message in secure manner,
Raja et al. (2011)	Proposed a design solution based on the physical security metaphor and Human In the Loop (HITL),
Brustoloni & Villamarín-Salomón (2007)	Introduced Polymorphic and audited dialogue to improve security warning decisions.
Villamarín-Salomón & Brustoloni (2010)	Introduced security reinforcing applications (SRAs) which rewarded end-user based on their behaviours.
Maurer et al. (2011)	Proposed new concept of warning design where it appeared together when user wanted to key in the data online.

Authors	Methods/Techniques
Hardee et al. (2006)	Suggested that attributes or features should be utilised in security warnings
Stoll et al. (2008)	Introduced Sesame – visualisation system which showed to end-users the background process which were always hidden from them.

From this table summary, it can be noted that most of the methods improved security warnings by utilizing the features or attributes on warnings and by creating or designing new form of warnings. However, there is not much emphasis on new framework or architecture on security warning.

On the other hand, Table IV provides information on problems that had been highlighted with the proposed solutions by various researchers [14]. There are six common problems related to security warnings (i.e. attention towards warnings, understanding of warnings, use of technical wordings, evaluation of risk from warnings, user's motivation towards heeding warnings and user's assessment of the implication of warnings).

Table IV. COMMON PROBLEMS RELATED TO SECURITY WARNINGS AND TEHIR SOLUTIONS [14]

Common problems with security warnings	Proposed solutions
Attention towards warnings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Raja et al. (2011), Maurer et al. (2011) and Hardee et al. (2006).
Understanding of warnings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Kauer et al. (2012), Edwards et al. (2007), Bravo Lillo et al. (2011), Raja et al. (2011), Brustoloni & Villamarín-Salomón (2007), Hardee et al. (2006) and stoll et al. (2008).
Use of technical wordings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Raja et al (2011) and Hardee et al (2006).
Evaluation of risks from warnings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Kauer et al. (2012), Maurer et al. (2011), Raja et al. (2011) and Stoll et al. (2008).
User's motivation towards heeding warnings	Bravo Lillo et al. (2011b), Bravo Lillo et al. (2011), Raja et al. (2011) and Stoll et al. (2008).
User's assessment of the implication of warnings	Bravo Lillo et al. (2011b), Raja et al. (2011), Brustoloni & Villamarín-Salomón (2007), Villamarín-Salomón & Brustoloni (2010) and Stoll et al. 2008).

This classification is useful for the others to understand the initial problem and possible solution in relation to security warnings. It highlights useful literature review that had been gathered from the observation and initial studies.

C. Approaches Related to Security Warnings

There are many different conceptualizations of warning process. Overviews of warning process can be discussed from the warning science literature angle to the specific method in relation to security warning studies. This section will explore computer related frameworks that suit the security warnings domain.

One of the most cited papers in relation to warning domain is Communication-Human Information Processing (CHIP) as in Fig. 3 [15]. The framework highlights the steps in warning processes to identify the reasons for failures of one particular warning. By utilizing this framework, problems with the warnings process can be identified and later can be solved accordingly.

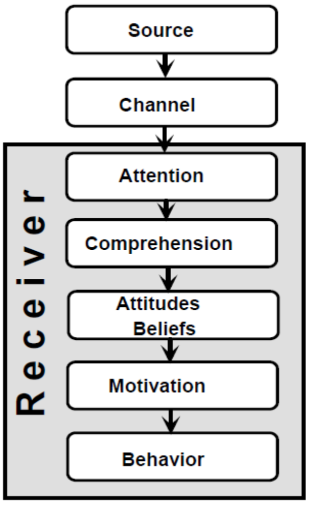


Fig. 3 Communication-Human Information Processing Framework (C-HIP) [15]

Cranor was among the first researchers to use C-HIP model to develop the Human in the Loop (HITL) (Fig. 4) security framework [16]. She used the CHIP as the basis to further enhance her own framework. HITL worked to identify security problems and helped to understand the end users' behaviors after performing security related functions.

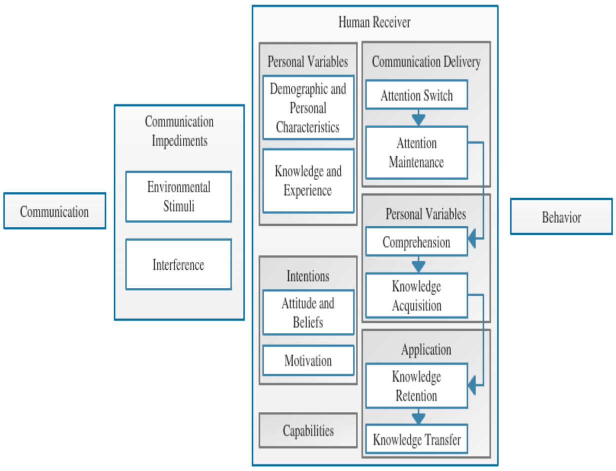


Fig. 4 Human in the Loop Security Framework (HITL) [16]

Security related functions normally actuate through security-related communication (i.e. the first element in HITL) which can be derived from warning, notices, status indicator, training or policy.

Four main features are involved in HITL such as communication, communication impediments, human receiver and behavior. She grouped the communication impediments with environmental stimuli and interference and she classified human receiver with personal variables, intentions, capabilities, communication delivery, communication processing and application. Finally, the framework showed that the aim of security communication is to promote and to ensure safe behavior.

She also introduced a four step iterative process also known as Human Threat Identification and Mitigation Process as shown in Fig. 5 [16]. It can be noted that HITL is part of the iterative process.

The task identification step involves system designer to identify whether the systems rely on human in order to perform security functions. Task automation step indicates whether security functions would be able to partially or fully automate. The failure identification step focuses on identifying the failure of security functions by utilizing the HITL framework and user studies. Finally, failure mitigation step prevents failures by identifying how users can be supported.

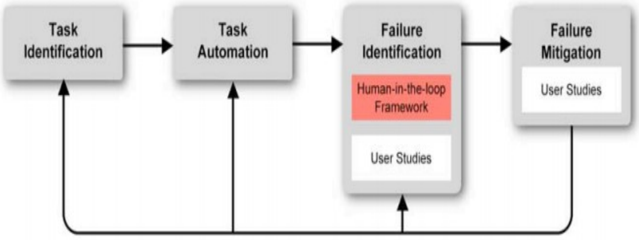


Fig. 5 Human Threat Identification and Mitigation Process [16]

She applied her research study to this framework by using anti phishing tools (i.e. passive warning indicators in web browsers were not effective to prevent users from phishing sites). She revealed from her findings that there is a need to find ways to correct users' mental model about phishing and proposed to focus on links to educational materials to improve anti-phishing warnings. She also recommended three high-level strategies to build a secure system for human beings to use as mentioned accordingly:

- To find ways to ensure human are out of the loop and build systems without involving human in security critical functions;
- To build systems that are intuitive and find method to make it easy to use;

- To teach human on how to perform the security critical task.

One notable advice that she mentioned was that individual or researchers cannot rely on one strategy to be successful. A combined approach is the best practice. One approach might not suit another situation. Therefore a combination will work better as it will support one another.

The Spectrum of automation approaches was introduced in 2007 [17]. It explained the strategies on how security automation for end-users can be implemented as shown in Fig. 6. The fixed policy indicates that the security decision policies are in tool and application (e.g. Karberos server – security kernel implementation). The customised policy allows the policy to be added or customised (e.g. managed by the system administrator) and finally the dynamic policy works in a flexible manner with dynamic policy adaptation (e.g. Bayesian spam filters).

In relation to security warnings, it can be suited to the spectrum the security warnings identified. With this approach, the decision making process will be much simpler as the decision is made automatically by the system. However, full consideration must be put in place as there are many challenges that limit the automation. For example, the social and environmental contexts of security must be considered. In addition, the consequences of security automation on end users would be a critical agenda to be highlighted.

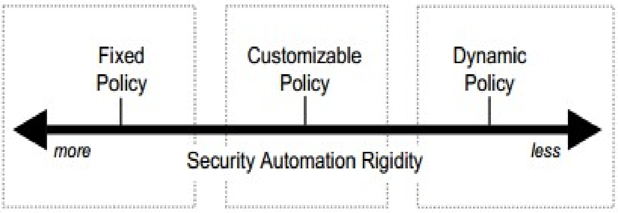


Fig. 6 The Spectrum of Automation Approaches [17]

Another approach is system visualization. It is used as a tool to provide more information to end users by highlighting how each process works in the computer system. However, not very much focus has been given on this area. Sesame was introduced as an interactive visualisation concept in order to help non-expert users make informed security decisions [18].

Sesame works by utilizing the desktop metaphor in order to show the background process when users wants to make security decision. Every steps involved will be shown to the users so that they will be able to comprehend ‘behind the scene’ scenarios (i.e. the technical process involves). The result of system visualisation is convincing as system activity, configuration and action can be viewed easily and better apprehended [19].

On the other hand, Iterative design is a design method that is based on cyclic process of prototyping, analysing, and refining the products or process (Instructional Design 2013). [24] defined that iterative development involves steady design refinement based on testing by user and other evaluation methods. Iterative design processes are widely used in many fields because of its effectiveness. Iterative design not only implemented in software application but also in engineering field, education field and research and development field [25,26,27,28].

One of the studies in improving security warning that used the iterative design process is done by [12]. They have conducted an iterative process of designing the warnings using common metaphors for each physical security such as locks, keys and walls. They have made comparisons between Comodo warnings (C-warnings) and their improved version of warnings (P-warnings). They have conducted two formative studies where the design of security warnings are utilising the iterative process. In the first formative study, the design of paper prototype of security warning was evaluated by 10 participants. Based on the feedback from first formative study, they redesigned the warnings by selecting the most appropriate design. Another formative study with 15 participants was conducted. The results from the second formatives study are analysed and the design of warnings are finalised. The results indicated that the majority of the participants favour their improved version of warning since it was easier to comprehend and encourage users to make a better decision.

Another study that implemented the iterative design process is conducted by Wash [27]. He used the iterative methodology to explore further on folk models of security. He conducted multiple rounds of interviews where the first round involves 23 semi-structured interviews. The second round of interview involves 10 interviews that are more focused and specific to investigate negative cases from the earlier results.

The similarities of both studies are that the models take the form of analogies or metaphors. In studies by [12], the designs of warnings are determined by the common metaphors of physical security. The common metaphors used in the initial design are locks, keys, doors, wall, policemen and stop sign. In their final design, they included a brick wall and a metal door to represent a physical firewall. In addition, they added a lock where it indicated the controlling access based on the formative studies done in their research earlier. Other than that, to represent application, they use a figure of a person who wants to go through the door.

While studies by [12] focusing on the metaphors, the studies by [27] used analogies instead. In the second round of the interview, he used additional technique which is known as hypothetical scenarios. The participants are presented with three themes which are:

- Finding out you have virus
- Finding out a hacker has compromised your computer
- Being informed that you are a victim of identity theft

The results suggested eight folks model of security threats that are commonly used by the home users (i.e. user decision on the usage of security software and security expert for them to follow). One observation can be made where the related research in utilising iterative design to improve security warnings are still in early stage (i.e. not widely practice yet). However, given the existing successful findings, it indicates that this approach is convincing. It would offer more new dimension on how security warnings can be further improved in various scenario (i.e. based on classification of security warnings).

The term mental model can be expressed as “small-scale models” of reality constructed by our mind to anticipate for events [29]. A mental model can be summarised as an explanation of a person’s thought about how a process works. It can be noted that the mental model is based on the perception, imagination, knowledge and comprehension of some aspect. Hence, a mental model can be addressed as a representation of a possibility that is common based on certain aspect [30].

In a recent study by [31], a mental model is designed based on the results of the surveys conducted. He had chosen four Microsoft warning messages scenarios mainly access denied warning, risky action confirmation, update notification and open attachment warning. The mental model results can be viewed as an illustrative of the behaviour for the technical and non-technical users when confronted with the security warnings. Based on the mental model results, the new security warnings were designed (i.e. known as enhanced warnings) and had been evaluated by the 32 participants from the Universiti Sains Malaysia. The results suggested that the enhanced warnings had improved the user understanding, motivation and action.

[32] on the other hand, proposes that mental model of risk communication could be utilise to improve the communication to end users about security risk in computer. She presented five mental models that are related to computer security namely physical security model, medical model, criminal model, warfare model and market model.

After a year, [33] had conducted an experiment based on card sort technique. Their studies recruited 22 experts and 49 non-experts in the first experiment. In the second experiment, 11 experts and 27 non-experts were included. All participants had prior knowledge or experience in computer related field. The experiments proved that experts and non-experts had different mental models. They proposed that the design of risk communication should also consider the non-expert mental models.

Then again, interviews with 10 advanced users and 10 novice users have been conducted by [34] to gain insights on their understanding of security warnings. A mental model was derived from the interviews and it shows significant differences in behaviour between the advanced users and novice users. Thus, the results suggested that mental model

D. Classifications of Security Warnings Approaches

After understanding the problems and the proposed solution of security warnings, this section highlights how each approach can be grouped or classified based on the techniques used. After gathering all information and evidences, four classifications are introduced (Fig. 6) [14]:

- Redesign the warnings by utilising the features and available information in the warnings
- Redesign the warnings by behaviour modification.
- Redesign the warnings by changing the presentation or layout

- Redesign the warnings by the adaptation of warnings

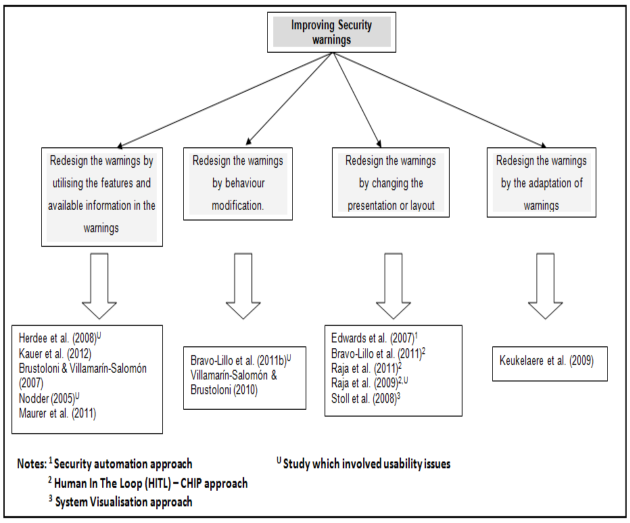

Improving Security warnings
Redesign the warnings by utilising the features and available information in the warnings
Redesign the warnings by behaviour modification.
Redesign the warnings by changing the presentation or layout
Redesign the warnings by the adaptation of warnings
Herdee et al. (2008)^{U}
Kauer et al. (2012)
Brustoloni & Villamarín-Salomón (2007)
Nodder (2005)^{U}
Maurer et al. (2011)
Bravo-Lillo et al. (2011b)^{U}
Villamarín-Salomón & Brustoloni (2010)
Edwards et al. (2007)^{1}
Bravo-Lillo et al. (2011)^{2}
Raja et al. (2011)^{2}
Raja et al. (2009)^{2,U}
Stoll et al. (2008)^{3}
Keukelaere et al. (2009)
Notes: ^{1} Security automation approach
^{2} Human In The Loop (HITL) – CHIP approach
^{3} System Visualisation approach
^{U} Study which involved usability issues

Fig. 6 Classification Approaches to Improve Security Warnings [14]

It can be noted that most of these findings were focusing on the redesign warnings. Warnings should be designed in a way that it will promote secure manner actions. In addition, users encounter the security warnings on daily basis which indicates the importance of delivering correct information and advise so that they are aware of possible menaces and possible action to take.

Based on Fig. 6, most researchers had focused on the first three classifications. However, “Redesign warnings by the adaptation of warnings” seem to be an unpopular one. Adaptive Security Dialog (ASD) fulfils the last classification to improve security warnings dialogs by producing a new architecture in order to promote a new type of interaction [20]. As the underlying cause of the security warnings problem had been addressed, it indicates there is a necessity to design security warnings in a way that can suit researchers’ Goal and objectives.

IV. DISCUSSIONS

Earlier, problems in relation to security warnings had been highlighted. Even though the problems were not thoroughly discussed but it provides some overview of problems faced by the end users. Table II highlights the classification of security warnings problems in regards to usability. On the other hand, Table III shows the works that had been done to improve security warnings.

Issues of usability continue become the focal point in security warning domain because it involve human where they are prone to make errors. In order to understand the fundamental or basis of the problem in regards to usable security, [40] mentioned the following:

“Encryption is one specific instance that deserves special mention. Well-encrypted messages can move safely through dreadfully weak systems. Encryption is well understood, but not widely employed. There is a ‘usability gap’ that translates directly into a ‘usage gap” [40].

Therefore, it is essential to bridge the gap which existed from the beginning by referring to the existing and the new challenges of security warnings. Many known approaches had been presented to improve security warnings as mentioned in aforementioned section C. However, there is no one standard way or rule of thumb has been used by the developers in the context of security warnings. There is a corresponding need to prepare a guide which can be the reference point for the developers before the creation of security warnings. In addition, security should be implemented as part of the product cycle instead of implementing it subsequently [46].

To our knowledge, there has been no similar compilation of literature in relation to security warning studies. Therefore, we took the initiative to provide this platform so that we can share this useful information. The classifications of all approaches are important to gather as much as possible works underlying security warnings studies. Apparently, there are four identified classifications as depicted in Fig. 6. There are room of improvement to combine those classifications (i.e. hybrid approach) to improve security warnings. The results can be evaluated to assess the fundamental of usable security aspect such as effectiveness, efficiency and satisfaction.

All of this information is useful for individual or researchers in security warnings domain. They can use this as a guide and as part of their literature review process. It is a challenging process to gather all these evidence and we hope that it will give positive benefits to others undertaking research in this area of study and to the general public.

Although the available gathered evidences has been presented accordingly, it can be suggested to be updated on regular basis (i.e. the gathered evidences are not conclusive). The pitfall of this work is in regards to the gathering of all available research papers within the domain of security warnings. There is a possibility that some outcomes have not been discussed or discovered yet.

Therefore, the problems of security warnings and the classification approaches can be improved or enhanced to suit the current context of security warnings implementation in various applications and platforms.

V. Future Work

There is a need to focus on a new framework or architecture to provide an effective security warnings design to suit end-users need. Only one study had satisfied this "redesign warning by the adaptation of warnings". We have similar intention to improve security warnings in the security dialogs context, thus, we will focus on this approach as the next focal of study.

VI. Conclusion

In conclusion, problems in relation to security warnings studies had been highlighted. In addition, the possible solutions are presented based on the classification of the mentioned problems. Suitable approaches had been described accordingly based on suitability of the problems. From one perspective, security warnings are supposed able to warn end-users from becoming the victims of malicious intention. However, it will not work solely by depending on the security warnings without prior commitment from the users. They need to equip themselves with knowledge and awareness so that they will be able to comprehend the warnings on the first place. Thus, it will not jeopardize them to become the victims of possible menaces attacks.

It can be highlighted that there are many ways to improve security warnings. The classification of approaches as presented (Fig. 6) can be considered as a new contribution in security warning studies which provides the benefits to the research community and to the general public. For the developers, it might be useful to consider these evidences in order to develop a better risk communication in regards to the application and security technologies products.

Acknowledgment

The research has been conducted with the collaboration between the Universiti Sains Malaysia and the Centre for Security, Communication and Network Research, University of Plymouth, United Kingdom.

References

[1] Wogalter, M.S. "Purposes and Scope of Warnings, In Handbook of Warnings. (Human Factors /Ergonomics)" (Assoc LE, Ed), 2006, pp. 3-9, ISBN 0805847243.

[2] Tuchscheerer, S., Dittmann, J., Hoppe, T. and Krems, J. F. "Theoretical analysis of security warnings in vehicles and design challenges for the evaluation of security warnings in virtual environments', Proceedings of the First International Workshop on Digital Engineering", Magdeburg, Germany. ACM, pp. 33-37.2010.

[3] Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N. & Cranor, L. F. "Crying wolf: an empirical study of SSL warning effectiveness", Proceedings of the 18th conference on USENIX security symposium. Montreal, Canada USENIX Association, pp. 399-416. 2010.

[4] Weir, C. S., Douglas, G., Carruthers, M. and Jack, M. "User perceptions of security, convenience and usability for ebanking authentication tokens", *Computers & Security*, vol.28, 1-2, pp. 47-62.2009.

[5] Lampson, B. "Privacy and security: Usable security: how to get it", Communication of ACM, vol.52, 11, pp. 25-27.2009.

[6] Nodder, C. "Users and Trust: A Microsoft Case Study". In Cranor, L.F. and Gar-finkel, S. (eds) Security and usability. Designing Secure Systems That People Can Use. O'Reilly, 2005, pp. 589-605, ISBN 0596008279.

[7] Microsoft. "Windows User Experience Interaction Guidelines"[Online]. 2010. Available at: http://msdn.microsoft.com/en-us/windows/aa511258.aspx

[8] Wu, M., Miller, R. C. & Garfinkel, S. L. "Do security toolbars actually prevent phishing attacks?" Proceedings of the SIGCHI conference on Human Factors in computing systems, Montreal, Quebec, Canada ACM, pp. 601-610.2006.

[9] Seifert, C., Welch, I. & Komisarczuk, P. "Effectiveness of security by admonition: a case study security warnings in a web browser setting", *Secure Magazine*, pp. 1-9.2006.

[10] Egelman, S., Cranor, L. F. & Hong, J. "You've been warned: an empirical study of the effectiveness of web browser phishing warnings", Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, Florence, Italy ACM, pp. 1065-1074.2008.

[11] Bravo-Lillo, C., Cranor, L. F., Downs, J. S. & Komanduri, S. "Bridging the Gap in Computer Security Warnings: A Mental Model Approach", *Security & Privacy*, IEEE, vol.9, 2, pp. 18-26.2011.

[12] Raja, F., Hawkey, K., Hsu, S., Wang, K. L. C. & Beznosov, K. "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, ACM, pp. 1-20.2011.

[13] Furnell, S. M., Jusoh, A., Katsabas, D. & Dowland, P. S. "Considering the Usability of End-User Security Software", Proceedings of 21st IFIP International Information Security Conference (IFIP SEC 2006), Karlstad, Sweden. Springer Boston, pp. 307-316.2006.

[14] Zaaba, Z. F., Furnell, S. M., Dowland, P. S .'A Study on Improving Security Warnings', Proceedings of the 5th International Conference on Information & Communication Technology for The Muslim World (ICT4M). Kuching, Sarawak, Malaysia. 2014.

[15] Wogalter, M. S., Dejoy, D. M. & Laughrey, K. R. "Organizing Theoretical Framework: A Consolidated Communication-Human Information Processing (C-HIP) Model". In Wogalter, M.S., Dejoy, D.M. and Laughrey, K.R. (eds.) Warning and Risk Communication. 1999 Taylor & Francis, pp. 13-21. ISBN 0748402667.

[16] Cranor, L. F. "A framework for Reasoning About the Human in the Loop", USENIX : Usability, Psychology and Security (UPSEC), San Francisco, USA, pp. 1-15.2008.

[17] Edwards, W. K., Poole, E. S. & Stoll, J. "Security Automation Considered Harmful", Proceedings of the 2007 Workshop on New Security Paradigms, North Conway, USA, ACM, pp. 33-42.2007.

[18] Stoll, J., Tashman, C. S., Edwards, W. K. & Spafford, K. "Sesame: informing user security decisions with system visualization", Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, Florence, Italy, ACM, pp. 1045-1054.2008.

[19] De Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., Rien, J., Rode, J. A. & Filbo, R. S. "In the eye of the beholder: A visualization-based approach to information system security", *International Journal of Human-Computer Studies*, vol.63, 1-2, pp. 5-24.2005.

[20] Keukelaere D. F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L. & Zurko, M. "Adaptive Security Dialogs for Improved Security Behavior of Users", Human-Computer Interaction – INTERACT 2009', Springer Berlin / Heidelberg, pp. 510-523.2009.

[21] Krol, K. Moroz, M. & Sasse, M. A. , Don't Work. Can't Work? Why It's Time to Rethink Security Warnings, Proceedings of the Seventh International Conference on Risks and Security of Internet and Systems (CRiSIS). IEEE, pp. 1-8.2012.

[22] Zaaba. Z. F. & Boon, T. K. (2015), "Examination On Usability Issues of Security Warning Dialogs (2015), Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol (2) No . 6. PP. 1337-1345. 2015.

[23] Cranor, L. F. & Garfinkel, S. (2005), Security and Usability: Designing Secure Systems that people can use, O'Reilley, ISBN: 100596008279.

[24] Nielsen, J (1993), Usability Engineering. Academic Press. ISBN 0-12-518405-0.

[25] Miller, F., Paradis, R. & Whalen, K., Iterative Development Life Cycle (IDLC): A Management Process for Large Scale Intelligent System Development, Proceedings of IEEE International Conference on Tools for AI, San Jose, California, Tools for Artificial Intelligence, pp.520-521.1991.

[26] Wong, A. & Park, C. B., A Case Study of a Systematic Iterative Design Methodology and its Application in Engineering Education, Proceedings of the Canadian Engineering Education Conference, Ontario, Canada.2010.

[27] Wash, R., Folk Models of Home Computer Security, Symposium on Usable Privacy and Security (SOUPS) , Redmond, ACM, 15.2010.

[28] Sullivan, G. F., The Iterative Design Process in Research and Development, National Aeronautics and Space Administration, Texas, US.2013.

[29] Craik, KJW 1967, The Nature of Explanation, Cambridge University Press. ISBN 0521094453.

[30] Johnson-Laird, P. N. Girotto, V. & Legrenzi, P., Mental Models: A Gentle Approach for Outsiders, System Intelligent, vol. 9, no. 68, pp. 1-13.1998.

[31] Ahmad, R., Improving Computer Security Warnings: A Mental Model Approach in Higher Education MSc Thesis, Universiti Sains Malaysia. 2015.

[32] Camp, L. J., Mental Models of Security, IEEE Technology & Society.2006.

[33] Camp, L. J., Asgharpour, F. & Liu, D., Mental Models of Computer Security Risks, Workshop on the Economics of Information Security, Pittsburgh, PA (USA).2007.

[34] Bravo-Lillo, C., Cranor, L. F., Downs, J. S., & Komanduri, S. , POSTER: What is still wrong with security warnings: A mental models approach, Proceedings of the Sixth Symposium on Usable Privacy and Security. Redmond, WA.2010.

[35] Kainda, R., Flechais, I., Roscoe, A. W., "Security and Usability: Analysis and Evaluation," Availability, Reliability and Security, ARES '10 International Conference, pp. 275-282.2010.

[36] Johnston, J, Eloff, JHP & Labuschagne, L. Security and human computer interfaces', Computers & Security, vol. 22, no. 8, pp. 675-684. 2003.

[37] Whitten, A. & Tygar, J. D. 'Safe Staging for Computer Security', Proceedings of the 2003 Workshop on Human-Computer Interaction and Security Systems. Fort Lauderdale, Florida. 2003.

[38] Proctor, R. W., Lien, M.-C., Salvendy, G. & Schultz, E. E. 'A Task Analysis of Usability in Third-Party Authentication', Information Security Bulletin, 5, (W3schools), 49-56. 2000.

[39] Wool, A.'The use and usability of direction-based filtering in firewalls', Computers & Security, vol.23, 6, pp. 459-468. 2004.

[40] Computing Research Association (2003) 'Grand Research Challenges in Information Systems'. [Online]. Available at: http://archive.cra.org/reports/gc.systems.pdf.

[41] Meier, J. D.'Web application security engineering', Security & Privacy, IEEE, vol.4, 4, pp. 16-24. 2006.