Security Warning Life Cycle: Challenges and Panacea

Nur Farhana Samsudin and Zarul Fitri Zaaba
School of Computer Sciences, Universiti Sains Malaysia 11800 Penang, Malaysia.
nfarhana.ucom12@student.usm.my

***Abstract*—Security warning is a very important aspect in computer security. Security warning is a form of message conveyed to inform user on the risk of allowing an application to run on the computer system. Security warning plays an important role in notify, warn and advise user about the potential result of an action beforehand. However, security warnings are often being ignored due to various reasons such as poor design of security warnings and too many technical terms used in security warnings. This research highlights insights into the discovery of problems and difficulties encountered by the users, approaches in improving security warnings and future direction of the security warning improvement process. We proposed to utilise the hybrid approach of iterative design and mental model in the effort to enhance the current implementation of security warning. Iterative design is a cyclic design process where prototyping, testing and refining are done repeatedly. A mental model is a person's psychological representation of how they perceive and understand something. It is expected that this paper would benefit the researchers to comprehend approches and challenges to improve security warnings.**

***Index Terms*—Security; Security Dialogues; Security Warning; Usability; Usable Security.**

I. INTRODUCTION

Nowadays people are very dependent on computer systems to perform various of tasks ranging from business to education and health care. The diverse use of computer systems in life have made the users vulnerable to possible harm such as financial loss, identity theft and system integrity [1]. Security warnings are encountered almost every time we use the computer. It is a form of message to help the user in defending their systems from unwanted harm. Users with knowledge in computer might have the capabilities to handle the security warning for better protection whereas for laymen, they might have little knowledge on how to deal with the warning [2].

Even though its purpose is to defend the systems from harm, users still finds the security warning as an annoyance. It is important to understand the difficulties and perceptions from the end-users perspectives as they are the one who experienced the problems. Other than that, usability issues of the computer security warnings have been an interest to researchers for decades as it is one of the important aspects in computer security. Therefore, the study in the aspect of improving security warnings still have a lot to be figured out. Thus, it is important to understand end-users comprehension of warning because it will provide useful insights on how security warnings should be presented in technological tools.

The outline of this paper is shown accordingly: starting with Section 2 that discusses the problem of the current implementations of security warning, Section 3 explores on the approaches that have been carried out to improve security warnings, Section 4 highlights the promising direction of security warning improvements and lastly, Section 5 ending with conclusions.

II. RELATED WORKS

Warning is a form of risk communication that is used to alert, notify and advice people so that potential harm can be avoided [3]. In addition, warnings have been defined as anything that is capable of distracting an individual's attention towards possible danger [4]. Warning can be summarised as something that can makes users aware of possible harm or consequences. In a similar concept, warning is applied in computer context and it can be described as a representation that diverts user's attention to alert and notify the user on the possible consequences of an action in advance [5]. Computer security warnings are normally encounter whilst trying to open an attachment, running an application that is downloaded from the Internet or low battery level and these warnings usually pop up instantly and needs immediate action as shown in Figure 1. In computer context, security warning can be presented into five different types namely dialogue box, in-place, notification, balloons and banners context [1].

In order to enable the end-users to responds correctly to security warnings, the interface should follow the usability guidelines. The concept of usability is extracted from the term user-friendly. [6] define the term usability as one particular products able to be used by the intended users in order to meet the goals within the context of usage. [7] claimed that usability can be associated to five usability attributes. The system should be easy to learn, efficient to be used, easy to memorise, have low rate of errors and pleasant to use. Usability studies usually involve a number of participants who are tested to perform some task [7]. The common approaches in measuring usability are performance tests and attitude tests [8]. Performance tests focus on the users' effectiveness in performing task and usability is measured in regards to speed, accuracy and/or errors. On the other hand, attitude tests capture the satisfaction and the perception of end users. In order to execute these, questionnaire, survey and interviews are used.

HCI relates closely to the system usability of a computer. It is a study of how humans interact with computers with a focus on how to make computer usable [9]. In addition, [10] viewed HCI as a field which involves the design, validation, evaluation and execution of interactional computer to be used by human being. Thus, in every interface on the computer system, it must involve both elements. The appropriate design of interface will enhance the usability of the system.

Therefore, the HCI can be used as a basis of designing computer system interface.

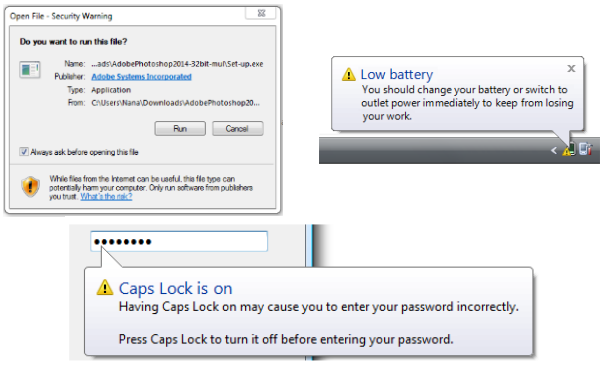

Figure 1: Examples of security warnings in computer [1].

From the context of security, usability and security can be linkage by HCI-S (Human Computer Interaction-Security). [11] define HCI-S as a field that link between human and computer with security. The goal of HCI-S is to enhance the interface hence improving the security. The criteria are based on the study of [12] in HCI (Human Computer Interaction) criteria. He analyses the interface of the existing Windows XP's Internet Connection Firewall (ICF) and proposed ICF based on the HCI-S criteria. The criteria suggest that security warning interface should convey features, visible in terms of system status, easy to learn, aesthetic and minimalist design, show errors or give guide to obtain help, satisfied the user and lead to trust. The detailed descriptions of the criteria are depicted in Table 1.

Table 1
HCI-S criteria [11]

No.	Criteria	Description
1	Convey features	The interface is conveyed with the available security features
2	Visibility of system status	Users able to observe the status of security system (i.e. internal system)
3	Learnability	The interface needs to as user friendly as possible.
4	Aesthetic and minimalist design	Only shown applicable security information.
5	Errors	The error message to be elaborated and recommendable with help function.
6	Satisfaction	Does the interface comprehend users using such system?

On the other hand, usable security concept relates closely with HCI, usability and HCI-S. In conceptual definition, usable security is defined as matching the security context with end user knowledge and motivation [13]. Their study suggests that the security software can be considered usable if the users have the details as discussed below such as:

1. End users know the context of security tasks
2. End users capable to execute the tasks without having problems.
3. End users do not make any risky decision or errors.
4. End users satisfy and happy with the interface.

To date, not much focus has been given in the area of usable security. As more application and security features have been developed, the interaction between users and computer systems must be simple and comprehensible. The technicalities such as the usage of jargons and terminologies can be reduced to the minimum level. As not much has been researched within this area, it opens more opportunities and dimension to be explored by scholars.

A. Issues and Challenges

Previous researchers have conducted studies on security warnings in the context of dialogue box [2,5,14]. Studies suggest that there are six common difficulties faced by the users when they received security warnings. The issues and challenges are presented in studies by [5].

In terms of attention towards warning, it can be revealed that users are not attentive towards warnings. The habituation effect also one of the cause of users' lack of attention in encountering security warnings. Habituation effects is the reduce of attention because of too much exposure to something [15]. [14] claimed that there has been a little research on habituation effect in the context of computer security. Since it is one of the major influences of why end users ignore the security warning, they discovered the studies on how the polymorphic warnings reduces the habituation in security warning.

With regards to use of technical wordings, studies by [2] revealed that beginners have a hard time in comprehend the technical terminologies presented in the security warnings. They have conducted interviews study with 30 participants and they reported that their participants have heard of the words however it is quite complicated for them to explain the meaning of jargons used.

From other perspective, it can be noted that the end users have inadequate mental models of the system security. With the evolving of computer security challenges and threats, the users still experience significant poor comprehension of the security system and lack of knowledge on how to react to the threat. A variety of mental model have been proposed by [16] that used as guidelines to perform security decisions. His study revealed that end users' security decision correlates to their conceptualisation of risks.

It can be noted that the end users are still facing problems with regards to security warnings. To summarise the issues and challenges that the users faced in the current context of computer security, a classification or taxonomy of issues and challenges of computer security are developed as depicted in Figure 2.

B. Approaches to Improve Security Warnings

There are many approaches that have been used to improve security warnings. The approaches that are discussed within this section is Communication-Human Information Processing (C-HIP), Human in the loop (HITL), in-context type of warning, iterative design and mental model approach.

[3,17] introduced a diagnostic tool that identify reasons for failure in warning known as C-HIP framework. By implementing the framework, specific area of warning implementation might be recognised and correction can be made. Figure 3 shows the C-HIP framework.

Besides C-HIP framework, a model called Human in the Loop (HITL) security framework have been developed by [18]. The framework is almost similar to C-HIP but her approach is more specific on the security tasks. In the framework, there are four main features mainly communication, communication impediments, human receiver and behaviour. The framework provides an organised method to rough out security issues and aid to understand user's behaviour as they carried out security-critical function.

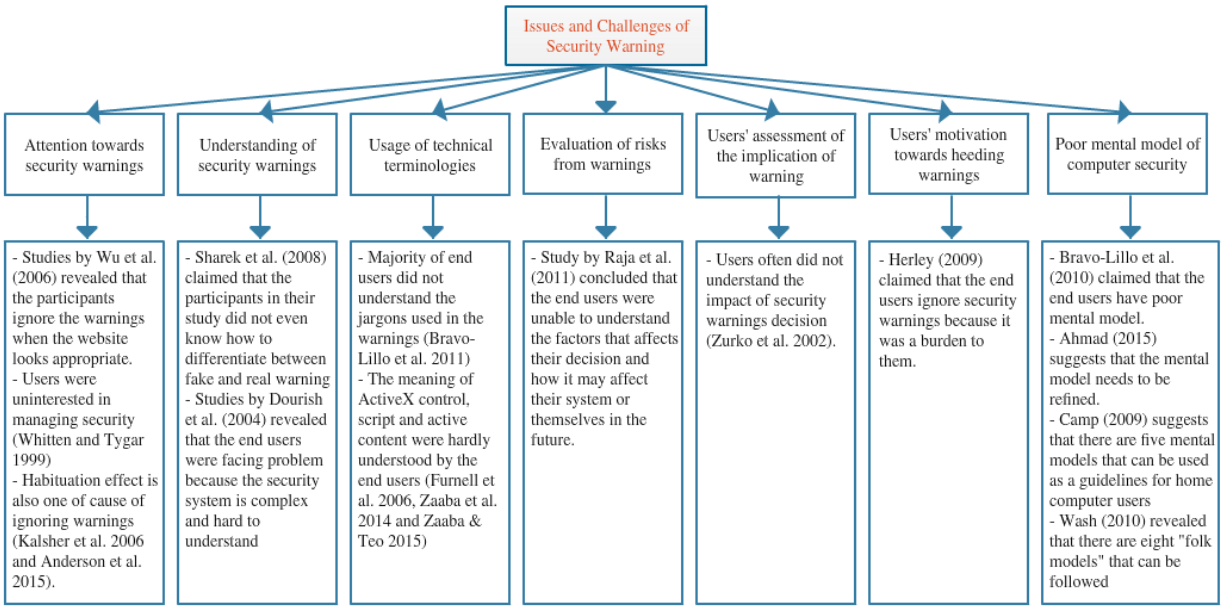

Figure 2: Issues and challenges in computer security warning

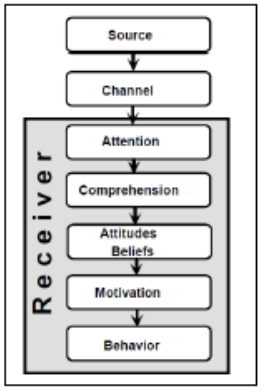

Figure 3: C-HIP framework [17].

Another approach that are used in improving security warning is by implementing in-context type of warnings where they appear right next to the critical data the user just entered [19]. The warning does not immediately disturb the user but appear while user are interacting (i.e. as the user types with keyboard) with the website. Users could instantly consider the website validity before submitting the critical data. In addition, this concept reduces the habituation effects in warnings since it shows a different type of warning rather than the usual dialogue box type.

Iterative design is also one of the approach that can be used to improve security warnings. It is a design method that are established on the cyclic process that utilising the prototyping, analysing, and refining the products or process [20]. Iterative design process is widely accepted in many domain areas because of its effectiveness. Iterative design not only implemented in software application but also in engineering, education, research and development field. Yet, iterative approach has not been fully utilised to improve security warnings.

On the other hand, the term mental model can be expressed as "small-scale models" of reality that has been developed in users' mind [21]. A mental model can be summarised as an explanation of a person's thought about how a process works. Hence, mental model can be understood as a possibility that is common based on certain aspect [22]. When people encounters a warning about hazard, they usually overcome the situation by depending on their previous experience, personal psychology and beliefs [23]. The utilisation of mental model have been used in other niche such as intelligent agents [24]. They introduced a new three layered architecture to share mental models in the aid multi-agent system that they designed. However, the discovery of mental model in computer security is still in early phase. In the computer security information field, it is essential to comprehend and to gather the information about a person's attitudes and perception before any redesign phase or attempts to improve the available security warning.

III. Categorisation of Security Warning Approaches

Clear understanding of how end-users perceive warnings is the core issue before developing security features or even application for end-users. According to [5], there are four classifications in order to improve security warnings as shown in Figure 4.

The first classification proposed that security warning are improved with appropriate used of icons, words, colours, technical terminologies and information to comprehend the meaning of warning. Many previous research realised that the features on security warnings should be used accordingly [25]. The second classification targets to have user makes appropriate secure decisions. The popular approaches used in this classification is mental model approach as proposed by [26]. The third approach proposed that the warnings are improved by changing the layout or presentation. However, the changing of layout or presentations of security warning can only work best if the attributes used in the enhanced warnings are understood by the end users. The fourth approach suggested that rather than change interface, warnings can be adapted based on the needs. Studies by [27] combined a new architectures and new method to communicate using security dialogues. The warning dialogues are presented differently based on users' preferences (i.e. whether more or less information should be

presented in the warnings). Since no one specific approach has been used, a hybrid approach may give a promosing results (i.e. combining more than one classifications).

Our works made a contribution by updating with more recent works to the original template [5]. Studies by [28,29,30] are added to the second classifications whilst study by [5] is added in the fourth classifications. These additions are made to equip the classifications with more recent works as more research within this domain are continually expanding. The improved version of the classification is represented in Figure 4.

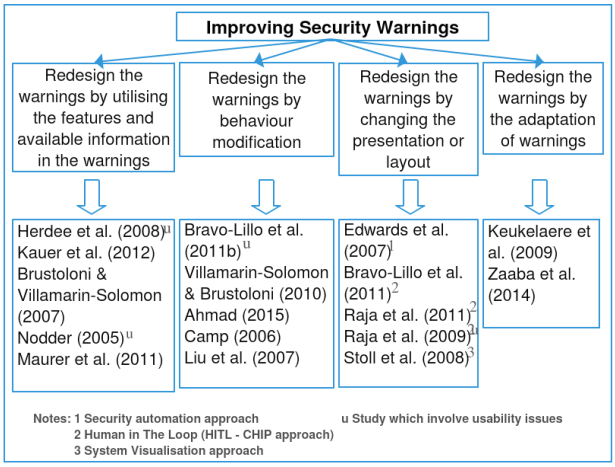

Figure 4: Improved classification of approaches in improving security warnings [5].

IV. Promising Direction of Security Warning Improvements

All mentioned approaches used in improving security warnings have their own benefits and impact to the development of security warnings. Based on our investigation, to date there is no research based on the hybrid approach of iterative design and mental model in improving security warning have been conducted before. We proposed to improve security warning based on combining both approaches. It can be revealed that from the mental model proposed by [2,28], people will consider the look and feel of the warning and the end users consider the warning text as an important aspect.

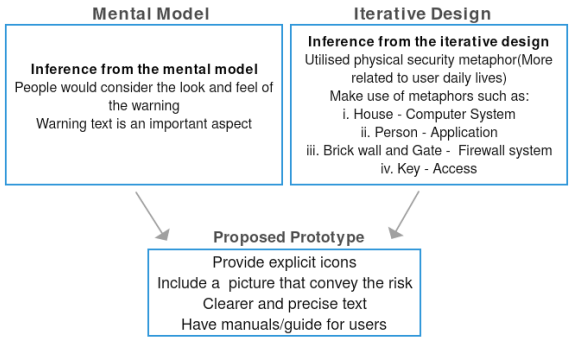

Figure 5: Mapping of iterative design and mental model approach.

With regards to iterative design, it can be noted that the physical security metaphors are the suitable approach since it is more relateable to users' daily lives activities. It can be found that using metaphors to enhance risk communication is one of the possible and effective ways. Previous studies by [31] show an implementation of comic approach in improving cyber security. Based on their studies, it can be noted that users were better informed of the risk and likelihood of hazard after experiencing and read the comic. The integration of mental model and utilisation of infographics can be considered as one of possible ways to improve the current implementation of security warnings. [32] have use the physical security metaphors as a guidance to design the personal firewall and the studies shows that the implementation of iterative design using metaphors is widely accepted.

With the hybrid approach of mental model and iterative design, the design of enhanced security warning is expected to have an explicit icon, have a clearer and precise texts, includes a risk level animation and have a manual or guide about the security warning as depicted in Figure 5.

V. Conclusions

In conclusion, this paper provides significant literatures that can be a guidance and reference point for other scholars in the security warning niche. Warnings plays an essential part in the computer systems. It becomes an essential aspect in defending the systems from possible harm. There are seven issues in usability which have been higlighted earlier. Even though the studies of improving security warning have been carried out for decades, there are still some gap exists based on the highlighted findings. There are numbers of approach mentioned in this study such as C-HIP, HITL, in-context type of warning, iterative design and mental model. Currently, we are in the process of designing the enhanced version of security warning by utilising the iterative design and mental model approach. It is expected that the proposed hybrid approach could improve the current implementation of security warnings so that the risk communication could better be conveyed to the end users. In addition, other possible combination can be conducted to give a wide spectrum of methods to improve security warnings.

Acknowledgments

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

References

[1] Microsoft "Warning Messages", [Online]. Available from: https://msdn.microsoft.com/en-us/library/dn742473.aspx (Accessed: 13 January 2016) (2015).

[2] Bravo-Lillo, C. Cranor, L. F., Downs, J. S. and Komanduri, S., "POSTER: What is still wrong with security warnings: A mental models approach", Proceedings of the Sixth Symposium on Usable Privacy and Security. New York, USA. (2010), 1-2.

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

[4] Rogers, W. A., Lamson, N., and Rousseau, G. K., "Warning Research: An Integrative Perspective", *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 42, no. 1, (2000), 102-139.

[5] Zaaba, Z. F., Furnell, S. M. and Dowland, P. S., "A Study on Improving Security Warnings", Proceedings of the Fifth International Conference on Information and Communication Technology for The Muslim World (ICT4M). Kuching, Malaysia, (2014), 1-5.

[6] ISO, "ISO 9241-11: Guidance on usability (1998)", International standards for HCI and Usability, Available from:

http://www.usabilitynet.org/tools/r_international.htm#9241x. (Accessed: 6 October 2015)(1998).

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

[8] Redmond-Pyle, D. and Moore, A., GUIDE – Graphical User Interface Design and Evaluation – A Practical Process, Prentice Hall Europe, (1995).

[9] Scheiderman, B. and Plaisant, C, *Designing the user interface: Strategies for effective Human-Computer Interaction*, 4th ed, Addison-Wesley, USA, (2005).

[10] Hewett, T. T., Baecker, R. M., Card, S., Carrey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G. and Verplank, W., "Curricula for Human-Computer Interaction", Available from: http://old.sigchi.org/cdg/cdg2.html. (Accessed 6 November 2015), (1996).

[11] Johnston, J., Eloff, J. H. P. and Labuschagne, L., "Security and human computer interfaces", *Computers & Security*, vol. 22, no. 8, (2003), 675-684.

[12] Nielsen, J., "10 Usability Heuristics for User Interface Design", Nielsen Norman Group, Available from: http://www.nngroup.com/articles/ten-usability-heuristics/. (Accessed 30 September 2015), (1995).

[13] Whitten, A. and Tygar, J. D., "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0". in USENIX Security Symposium, (1999).

[14] Anderson, B. B., Kirwan, C.B., Jenkins, J.L., Eargle, D., Howard, S. and Vance, A., "How polymorphic warnings reduce habituation in the brain: Insights from fMRI study", Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, (2015), 2883-2892.

[15] Kalsher, M. J. and Williams, K. J., "Behavioral Compliance: Theory, Methodology, and Result," In Handbook of Warnings, Mahwah, New Jersey, (2006), 313-329.

[16] Wash, R., "Folk Models of Home Computer Security", Symposium on Usable Privacy and Security (SOUPS) 2010, Redmond, WA, US, (2010).

[17] Wogalter, M. S., Dejoy, D. M. and Laughrey, K. R., "Organizing Theoretical Framework: A Consolidated Communication-Human Information Processing (C-HIP) Model", Warning and Risk Communication, Taylor & Francis, (1999), 13-21. ISBN 0-7484-0266-7.

[18] Cranor, L. F., "A framework for reasoning about the human in the loop", Proceedings of the 1st Conference on Usability, Psychology, and Security, Berkeley, CA, USA, (2008), 1–15.

[19] Maurer, M-E, Luca, A. D. and Kempe, Sylvia, "Using Data Type Based Security alert Dialogs to Raise Online Security Awareness", Proceedings of the 7th Symposium on Usable Privacy and Security, Washington, US, (2011), 1-13.

[20] Iterative Design, Available from: http://www.instructionaldesign.org/models/iterative_design.html. (Accessed: 15 October 2015), (2013).

[21] Craik, K. J. W., "The Nature of Explanation", Cambridge University Press, (1967), ISBN 0521094453.

[22] Johnson-Laird, P. N., Girotto, V. and Legrenzi, P., "Mental Models: A Gentle Approach for Outsiders", Sistemi Intelligenti, vol. 9, no. 68, (1998), 1-13.

[23] Fischhoff, B., Riley, D., Kovacs, D. C., and Small, M. "What information belongs in a warning? A mental models approach." Psychology & Marketing, vol. 15, (1998), 663-686.

[24] Salehi, S., Taghiyareh. F., Saffar. M. and Badie, K., "A context-aware architecture for mental model sharing through sematic movement in intelligent agents", International Jouenal of Engineering TRANSACTIONS B: Applications Vol. 25, No. 3, (2012), 233-248.

[25] Kauer, M., Pfeiffer, T., Volkamer, M., Theuerling, H. and Bruder, R., "It is not about the design - it is about the content! Making warnings more efficient by communicating risks appropriately", GI SICHERHEIT 2012 Sicherheit – Schutz und Zuverlassigkeit, (2012).

[26] Bravo-Lillo, C., Cranor, L. F., Downs, J. S. and Komanduri, S. "Bridging the Gap in computer Security Warnings: A Mental Model Approach". *Security & Privacy*, vol.9, no. 2, (2011), 18-26.

[27] Keukelaere D. F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L. and Zurko, M., "Adaptive Security Dialogs for Improved Security Behavior of Users Human-Computer Interaction – INTERACT 2009". Springer Berlin / Heidelberg, (2009), 510-523.

[28] Ahmad, R., "Improving Computer Security Warnings: A Mental Model Approach in Higher Education" MSc Thesis, Universiti Sains Malaysia, (2011).

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

[30] Liu, D., Asgharpour, F., and Camp, L., "Risk Communication in Security Using Mental Models". *Usable Security*, vol. 7, (2009).

[31] Zhang-Kennedy, L., Chiasson, S., and Biddle, R., "The Role of Instructional Design in Persuasion: A Comic Approach for Improving Cyber Security", International Journal of Human-Computer Interaction, (2016), 302-322.

[32] Raja, F., Hawkey, K., Hsu, S., Wang, K. L. C., and 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, (2011), 1-20.