Towards Designing Effective Security Messages: Persuasive Password Guidelines

Nur Haryani Zakaria
School of Computing Science
Universiti Utara Malaysia
Sintok, Kedah, MALAYSIA
haryani@uum.edu.my

Norliza Katuk
School of Computing Science
Universiti Utara Malaysia
Sintok, Kedah, MALAYSIA
k.norliza@uum.edu.my

Abstract— **The current state of information security compliance in workplaces is deteriorating. In many cases human factors were attributed as the cause of the problem. Humans are well known as the *weakest link* in the security chain. Commonly, end-users will depend on security messages when confronted with security-related decision making. Most of the time, end-users will try their best to make sense of unclear instructions in order to cope with situations. This indicates the way security messages are presented is of utmost importance. However, research focusing on designing effective security messages is quite limited. This paper presents research in progress, towards designing effective security messages focusing on passwords guidelines. Our initial review indicated the lack of persuasive elements in the current password guidelines may lead to unmotivated behaviour of producing good (strong) passwords. This paper also includes initial results obtained from pilot study which reveal promising results supporting the usage of persuasion strategies to improve the current state information security compliance.**

Keywords-Information security compliance,security messages, password guidelines, persuasion.

I. INTRODUCTION

Organisations have implemented variety of technical measures such as firewall and intrusion detection systems to strengthen their defences. However, deploying sophisticated security techniques is not sufficient in preventing security incidents [1]. Many people in the security business regard the human factor as the weakest link in security solutions [2]. User behaviour (e.g.: using weak passwords or sharing password) has played a part in many security failures. In accordance, information security compliance has become one of the most pressing issues facing organisation these days. The failure of obtaining compliance in the organisation poses a major threat and is currently desirable for effective solutions [3]. Although, training and educating people through awareness campaigns are certainly necessary countermeasures, unfortunately in many cases, human are still been attributed to the security failures [4].

In relation to this, users in the organisation rely heavily on security messages in making critical decisions related to information security [5]. Security messages include all types of information security communications conveyed to users; such as policies, guidelines, instructions, warnings, advices, reminders, notification, alerts and other relevant items. Failure in making sure that these security messages are conveyed in an understandable format will result in unclear, misconception and worst case confusing end users [6]. Besides that, the way of how security messages are conveyed played significant role in determining the users' compliance behaviour [5]. Hence, the way in which these security messages are framed is of particular importance. Unfortunately, there are limited numbers of research looking into how to design these security messages to maximise their effectiveness.

With the vast amount of possible information security application that involved security messages, perhaps the most common focus have been centred into password policies and guidelines [7,8]. This is due to passwords remain as the dominant means of authentication in-spite of growing number of alternatives such as graphical and biometrics authentication [9]. Many current studies for example studies in [8,9], emphasised their focus on users reluctance in adopting particular security messages (i.e.: policies and guidelines); however limited amount of studies have actually focus on designing and producing effective security messages that will be able to improve compliance behaviour.

Therefore, this study is undertaken to fill in this gap by choosing the popular path of password policies and guidelines domain of interest. The study aims to investigate how to design password security guidelines that will be able to convey the messages in the most effective way (i.e.: people will comply to the suggestion given in the security messages). In addition, we posit that messages contained in the password security guidelines can be framed more persuasively to invoke self-security-awareness.

Throughout this paper, related work will be discussed followed by an initial review of existing password related guidelines and policies. Then our research approach will be elaborated. Next is the research methodology which include an experimental study which will be carried out to test several interesting hypothesises. Since, this is a research in progress, the paper will be revealing initial results obtained from pilot study conducted to test the first two (out of four) hypotheses, followed by limitations of the study before concluding with some immediate future work to be undertaken.

II. RELATED WORK

Research that specifically looking into how to design an effective security messages is surprisingly quite sparse. One that is particularly relevant is a study in [5] which applied

Elaboration Likelihood Model (ELM) looking into how people process security messages. The researchers manipulated two message properties; quantity (i.e.: repeated messages) and comprehensibility (i.e.: messages that can be easily understood) and observed the effect on users thinking process. Their outcome found that message repetition is positively related to ELM while message comprehensibility is the opposite. The way we interpret this finding is that although users may have some basic awareness on information security, they need to be constantly reminded from time to time (i.e.: repetitively).

Another recent study in [6] investigated password generation behaviour. They found out that participants tried to match their perceived security level of the service to the estimated security level of the password. However surprisingly, all the passwords estimated as highly secure (uncrackable) and most of passwords regarded as secure (hard to crack) are passwords that contain a single word. Additionally, most of the passwords estimated as fairly secure are passwords that include a common word or name. These findings drew the authors to suggest that password guidelines contained in the security policies should be devised in order to avoid misconception among users. On the other hand, Gaw & Felton [10] reported on *"simplistic minded"* among users regarding password attacks. Majority of the participants rarely thought of the exact concept of dictionary attack but instead commonly associated it as an act done by someone (i.e.: human) and hence leads to the assumption that password guessing attacks would only occur if someone actually knows the person. Findings in [6 & 10] are pointing towards the idea that end-users' interpretation and perception out of the security messages they refer to are very important to ensure the desired behaviour (i.e.: compliance) can be obtained.

Researcher in [8] investigated the reason behind the rejection of security advices by users. By making comparisons between potential and actual benefits of security messages, he concluded that most security advices are rejected by users due to they offer a poor-cost benefit trade-off. He elaborated that user perceived security advice as a burden while the benefits of compliance towards the advices are not necessarily evident (i.e.: users would not appreciate their act of compliance when they do not eventually become the victim themselves). Also on the same vein, Inglesant & Sasse [9] suggested for a more flexible password policies tailored to mitigate the risks users actually face, in order to allow for the differing security needs of different work groups.

From theoretical perspective, Protection Motivation Theory (PMT) has been predominantly applied to motivate secure compliance behaviour as reported in [11,12]. Among the five elements in the PMT constructs, fear element has been studied quite frequently in several researches. For example, Weirich & Sasse [13] proposed the usage of fear appeal in order to motivate password behaviour compliance. They highlighted that in order for fear appeal to work, changes to existing policies is necessary to include the idea that punishment is being enforced by organisations and no misbehaviour will go unnoticed. Slightly on a different angle of fear appeal, Xu et al. [14] proposed threats (e.g.: spyware attacks) as the fear element to arouse users attention to motivate compliance behaviour. Although fear elements may result in changes towards attitudes or behaviour, the effectiveness is still questionable in longer term period of time, especially when punishment is associated. Punishment regime is seen as coercion mechanism which may result in rebellious situation once the end-users (humans) realised that surveillance is no longer being enforced.

Previous studies presented in this section had indicated that the way users perceived the messages are indeed important in supporting their actual understanding of a particular security message. Hence, designing effective security messages that can provide a clear understandable instruction is important to support users' decision especially with regards to behaving securely. The next section will entail an initial review conducted on the several selected existing security messages contained in the password related guidelines and policies.

III. REVIEW OF EXISTING PASSWORD RELATED GUIDELINES AND POLICIES

In order to have an insight into the current contents of password related guidelines and policies available on the Internet; we visited some of the websites lists obtained from study [7]. The focus of their study was to find correlation between characteristics of a particular websites compared to the strength of policies it offers. Their findings suggest that much extra strength demanded by the more restrictive policies is unnecessary that it caused more inconvenience instead of offering better usability. However, the study did not cover the content structure of the password guidelines in terms of what informational advices are given to users and how it is being displayed in order to guide the users in password creation. We chose five of the top traffic sites and five universities with top Computer Science Department from the list and conducted a review of the content structures of the password guidelines for each sites. The reason for choosing those sites is because we would like to find out any common patterns derived by comparing those two categories of sites. Among the elements that we are looking into are; 1) The instructions given for construction of a good password[1], 2) Reasoning/justification – provide explanation why such requirement/suggestion is given, 3) Supported examples – clear, understandable and relevant examples, 4) Approach – how the guidelines are presented, 5) Arrangement – layout: paragraphed, bullet points.

Table 1 below displayed an overview of the 3 elements identified above (1-3) for all the ten different websites surveyed. Based from the content elements that we surveyed, we conclude that inconsistencies exists in various parts of the of password guidelines. This has been the case

[1]The term good password and strong password are used interchangeably throughout this paper.

when different sites are using different approaches to convey the guidelines. Some of the sites failed to provide supported examples following the requirements stated to construct a good password.

TABLE I. OVERVIEW OF SEVERAL IDENTIFIED ELEMENTS (ELEMENTS 1 TO 3) CONTAINED IN PASSWORD GUIDELINES OF THE TEN SELECTED WEBSITES

Websites/ Elements	Good Password Construction:			Reasoning	Supported Examples
	What?	*Why?*	*How?*		
5 Top traffic sites					
Google	×	×	✔	×	✔
Facebook	×	×	✔	×	×
Yahoo	✔	✔	✔	×	✔
AOL	×	×	✔	×	✔
E-bay	×	×	×	×	✔
5 Top CS Department (academic institutions in the US)					
MIT	✔	×	✔	×	✔
Stanford	✔	✔	✔	×	×
UC Berkeley	✔	✔	✔	×	✔
CMU	×	×	✔	×	✔
Princeton	×	×	✔	×	×

More importantly, a key element was found missing in all the sites surveyed; ***reasoning***. This refers to justification as to why such requirements are needed or such suggestions are proposed to the users. For example, many sites failed to highlight the reason as to why it is important for them to create a good password. Providing reason will increase the likelihood of compliance to a certain request [15]. However, this is found to be lacking in many guidelines available which possibly be the main factors leading to misconception. Although arrangement aspect may not be as important as other elements, it does contribute as a factor (i.e.: *complexity* versus *brevity*) in determining whether users are willing to spend their time and effort to read the guidelines. Moreover, none of the password guidelines surveyed seems to apply certain approach in displaying their guidelines – most guidelines appeared neither convincing nor persuasive in attempting to motivate the audience to follow their suggestions.

With the initial findings above, we realise that it is important to find ways to deliver security messages more persuasively; ultimately producing more effective security messages that will be able to improve compliance behaviour. The next section will be discussing on our chosen approach; persuasion.

IV. RESEARCH APPROACH: PERSUASION

The findings in section III have indicated the necessity to present security messages in more persuasive and convincing way so as to exert a pull on effect on users reading password security guidelines. Aligned with this intention, we have decided to use two different persuasion strategies. One of the strategies is adopted from the advertising domain that is using *rational* and *emotional appeal*. The reason for choosing an appeal strategy is because the advertising literature has shown that this strategy is well known for its success in promoting goods and services to consumers [16]. The *rational* appeal focuses on providing logical and reasoning approach in order to persuade while *emotional* appeal focuses on involving audiences into the real situation so as to trigger their feelings. Statistical evidence or published reports were usually used to support *rational* appeal presentations while true stories or real cases will normally be used to support *emotional* appeals [17].

The second persuasion strategy is adopted from Cialdini's [15] six weapons of influence namely; *reciprocation, authority, commitment & consistency, liking, scarcity* and *social proof*. Out of the six Cialdini's weapons of influence, only two will be used in this study that is *social proof* and *commitment & consistency*. The principle of *social proof* state that human determine what is correct by finding out what other people think is correct. Apparently this principle works best in two situation; uncertainty and similarity. If people are in an uncertain situation, they will find somebody to copy or having a high tendency to follow what others have decided [18]. The idea of being similar to others is also appealing since deviation might indicate weirdness and this is obviously not favourable to most people [15]. On the other hand, the principle of *commitment & consistency* stated that once people decide or take a stand, they encounter personal or interpersonal pressures to behave consistently with that commitment [18] and the best way to enforce this principle is by getting people to write down their commitment or make it known to public. The two persuasion strategies (as mentioned above) will be used to frame specific section in password security guidelines (i.e.: providing reasons as to why good strong password is important).

Besides that, the password security guidelines will be design in such a way that it is organised according to the stages in the Yale Approach. Yale approach was introduced by Hovland et al [19] with the main intention to increase the persuasive effect in delivering the security messages. The stages in the Yale approach includes *Exposure > Attention > Comprehension > Acceptance > Retention > Behaviour* [9]. Mainly, this research will concentrate on the first three stages in the Yale Approach while the later stages will be part of the on-going evaluation of the study. The next section describes our research methodology to be carried out to validate our research approach.

V. RESEARCH METHODOLOGY

In order to validate the suggested persuasion strategies, an experimental based setting will be carried out. The experiment will use the *"between subject"* design where each participant will be exposed to only one of the condition. The independent variable of this experiment will be the persuasive security messages while the dependent

variable will be the compliance information security behaviour. This study was done with the intention to test the following hypotheses:

H1 – Compliance behaviour will improve when users are exposed to security messages which are framed with persuasive contents, specifically when reasoning elements are included to justify the importance of the required behaviour.
H2 – The usage of the Yale Approach stages in designing password security guidelines managed to gain better compliance from subjects compared to those who only exposed to standard password security guidelines.
H3 – The appeal strategy (rational & emotional) will have significant effect on gender factor; male subject will be more likely to be drawn by the rational appeal while female on the other hand will likely to be drawn by emotional appeal.
H4 – The commitment & consistency group will have higher compliance rate compared to social proof group; as subjects in the earlier group have made their stand publicly by signing of and submitting the commitment form.

For the purpose of this experiment, creating good password has been chosen as the behaviour that will be observed. As previously mentioned, the password security guidelines will apply the persuasive stages as suggested by the Yale Approach. The study will manipulate the usage of persuasive password security guideline which was designed based on the first three stages of the Yale Approach as follows; 1) *Exposure stage*: To give overview or basic understanding of the targeted behaviour, 2) *Attention stage*: To grab the audience interest to engage in the target behaviour, 3) *Comprehension*: To provide support on how to engage in the target behaviour.

Figure 1, shows an example of explanation given in the *exposure* stage as to provide explanation of what a password is. The *attention* stage will display reasons as to why having good strong password is important. This is believed to be able to draw audience attention to engage in the desired behaviour. Finally the *comprehension* stage will provide clear examples of how to construct a good strong password which is intended to support the audience into engaging in the desired behaviour. There will be four experimental groups involved namely; *rational appeal group, emotional appeal group, social proof group* and *commitment & consistency group.* Each experimental group represent each persuasion strategy that will be induced upon the subjects in the experiment such as follows:

- *Rational appeal group*: Subjects in this group will be exposed to logical and reasonable arguments. Simple common sense statement will also be used to support the argument.
- *Emotional appeal group*: Subjects in this group will be exposed to idea of possibility of becoming a real victim. Real life examples can be included to support the argument.
- *Social proof group*: Subjects in this group will be exposed to the vulnerabilities of personal reputation being tarnished; hence implicating others in their circle of social relationship. Since the usage of social networking sites is popular these days, it is included to support the argument.
- *Commitment & consistency group*: Subjects in this group will be exposed to the idea of putting their commitment in the form of signed documents. Submitting the piece of signed documents will be used as a support mechanism.

On the other hand, subjects in the control group will be exposed to standard password guidelines – providing basic instructions on how to create passwords as shown in Figure 2 below.

What is a password...?

Imagine a password as the key to your treasure chest - that contains important information like account numbers, personal information, health records. It is like the key to your home's front door - obviously you don't want to leave it under the welcome mat. It is your first line of defence in protecting all that important information. You may think that with a password you may be safe. Well, that depends on the password you have chosen! While making a strong password will take a little extra work, this practice will go a long way to help you secure your valuable information and applications.

Figure 1. Example of Explanation Involved in the Exposure Stage

The way to set a password:

Think of a phrase of **eight** words (or more) which contains at least one **upper case** (capital) letter and at least one **number**, and then use the initial letters of the phrase. For example:

"My black cat Whiskers is 9 years old" = **MbcWi9yo**
"I was born in Buenos Aires in 1987" = **IwbiBAi87**
"Alan Shearer scored 2 penalties against Man U" = **ASs2paMU**
"That boy with glasses and ginger hair is the one for me" = **Tbwgaghi14me**

Windows now also allows whole sentences, so in fact you could use "**Whiskers is 9 years old**".

Figure 2. The Standard Password Security Guidelines (used in Control Group)

The following sub-section entails the procedures of the pilot study that has been carried out to test the hyphothesises of this study:

A. Procedures: Pilot Study

The pilot study has recurited 55 participants (25 male and 30 female) age ranging from 20-58 years old. Each participant was given a URL address that will direct them to specific website that contains a set of tasks they need to complete such as follows; 1) Fill in consent form, 2) Read security guidelines carefully and checked in the button at the bottom to indicate they have done so. Each security guideline contains different persuasive strategies depending on which group they were assigned, 3) Read a given scenario – was prompted to create good strong password based on the security guideline they have read earlier, 4) Finally, they filled in some demographic information and proceeded to create a set of username and password.

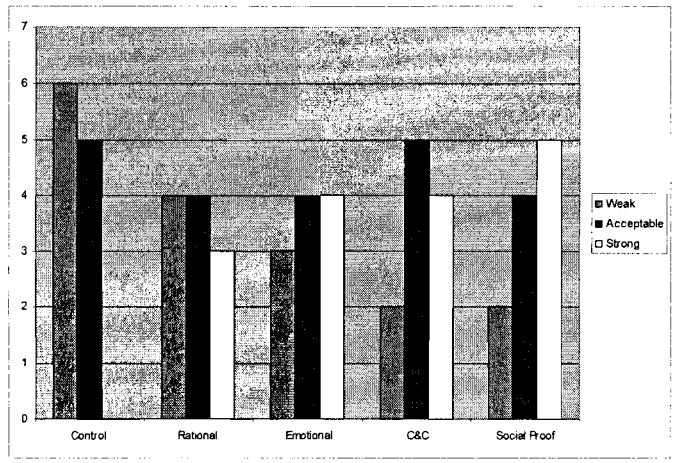
VI. DATA ANALYSIS

In our pilot study, we attempted to validate the first and second hypotheses; that is to see whether it is worth putting an effort on persuading end-users to create good strong passwords by framing the reasoning message persuasively. The compliance behavior in our study was measured through password length, password strength and password entropy. The definition of each measurement is stated as follows, followed by password categories in Table II below; 1) *Password length*: the number of characters that constitute a password, 2) *Password strength*: is a measurement of the effectiveness of a password in resisting guessing and brute-force attacks. Specifically, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to correctly guess it, 3) *Password entropy* (measured in bits): is the amount of variation of characters in the password.

TABLE II. PASSWORD CATEGORIES

Password categories	Weak	Acceptable	Strong
Password length (characters)	0 – 7	8 - 12	> 12
Password strength	0 - 19	20 - 30	> 30
Password entropy (bits)	≈ 25.1	≈ 39.1	≈ 53

Using the above measurements, we found that most of our participants (70%) have created higher numbers of acceptable and stronger passwords in the experimental groups which used the persuasive arguments compared to the standard password guidelines (control group).



Fugure 3. Number of passwords created for each experimental group according to password categories

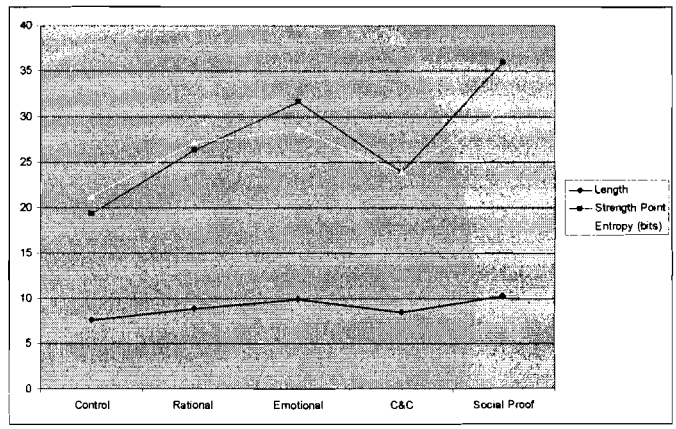


Figure 4. Number of passwords created for each experimental group according to password length, strength and entropy

In addition, Figure 4 above also strengthen the findings that participants in the experimental groups have created higher password length, strength and entropy which indicates that compliance behaviour with regards to creating good strong passwords is better in the experimental groups compared to the control group. Among the four experimental groups, participants in the *social proof* groups performed the best (highest password strength = ≈36, highest password entropy = ≈31bits) – indicates that using social proof techniques will provide better compliance behaviour among end-users. Hence, figure 3 & 4 have supported the first two of our hypotheses as follows:

H1 – Compliance behaviour will improve when users are exposed to security messages which are framed with persuasive contents, specifically when reasoning elements are included to justify the importance of the required behaviour – ***supported by the findings.***

H2 – The usage of the Yale Approach stages in designing password security guidelines managed to gain better

compliance from subjects compared to those who only exposed to standard password security guidelines – ***supported by the findings.***

Since this is a work in progress, we are still in the process of granulating the data to perform deeper analysis as to confirm the rest of the hypothesis for this study. However, this finding should be subject to higher statistical power to confirm.

Nevertheless, the initial findings have generally indicated that our proposed approach using persuasion is worth to be explored further to improve information security compliance which in our context referred to creating good passwords.

VII. LIMITATION OF THE STUDY

This study has several limitations that should be taken into consideration. First, it is important to note that the security behaviour that was being observed in the experiment was creating good (strong) password. Caution should be applied when generalising the results to other security behaviour. Secondly, we have no way to determine whether the users' behaviours are explicitly due to exposure from the security messages given to them and not due to other contributing factors. Other contributing factors such as present level of security awareness or individual perception are ignored in this study.

VIII. CONCLUSION & FUTURE WORK

This paper has presented an approach towards designing effective security messages focusing specifically on password security guidelines. Persuasion has been chosen as the approach to provide more convincing and appealing messages to the intended audiences. Alongside with the persuasion strategies, the Yale approach has also been considered in the process of designing the password guidelines. The initial findings obtained from a review work done have shown the importance of framing security messages that not only able to provide clear and understandable instructions but also manage to convince audience to follow the suggested guidelines.

We strongly believed that this study can contribute in several ways. First, the potential outcome of this study will be able to provide better insights into how to design an effective security messages. Secondly, the findings in this study will also enable us to confirm that it is significance to frame security messages with persuasive content and this is definitely relevant to preparing content for information security awareness programs as well as security policy implementers out there. In addition, the outcome is also relevant to HCI communities who involve in designing persuasive content for security applications.

In future, we would like to extend the study with other persuasion strategies. We also plan to invite subjects from various backgrounds for our experimental studies to produce a more generalizability findings. In addition, we intend to study personality factors in relation to persuade different people with different personalities. Finally, using this current work as a foundation, we plan to propose a persuasion framework which will provide better guidance to researchers and practitioners in designing persuasive messages for security applications in general.

REFERENCES

[1] B. Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World.* New York: Springer-Verlag, 2003.

[2] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming The 'Weakest Link' - A Human/Computer Interaction Approach to Usable Security and Effective Security," *BT Technology Journal,* vol. 19, pp. 122 - 131, 2001.

[3] M. T. Siponen, S. Pahnila, and M. M. Adam, "Compliance with Information Security Policies: An Empirical Investigation. ," *IEEE Computer,* vol. 43, pp. 64-71, 2010.

[4] K. Aytes and T. Conolly, "A Research Model for Investigating Human Behavior Related to Computer Security," in *Americas Conference on Information Systems*, 2003, pp. 2027 - 2031.

[5] T. Qing, Y. B. Ng, and A. Kankanhalli, "Individual's Response to Security Messages: A Decision-Making Perspectives," International Conference on Decision Support System, 2007.

[6] B. Grawmeyer and H. Johnson, "Using Multiple Password: A Week to a View," *Interacting With Computers,* vol. March, 2011.

[7] D. Florencio and C. Herley, "A Large-Scale Study of Web Password Habits," in *World Wide Web Conference* Alberta, Canada, 2007.

[8] C. Herley, "So Long And No Thanks for the Externalities: The Rational Rejection of Security Advices by Users," in *NSWP'09*, Oxford, UK, 2009.

[9] P. Inglesant and M. A. Sasse, "The True Cost of Unusable Password Policies: Password Use in the Wild," in *CHI 2010*, Atlanta, Georgia, 2010.

[10] S. Gaw and E. W. Felten, "Password Management Strategies for Online Accounts," in *Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, USA., 2006.

[11] L. Zhang and W. McDowell, C., "Am I Really At Risk? Determinants of Online Users' Intention to Use Strong Passwords," *Journal of Internet Commerce,* vol. 8, pp. 180-197, 2009.

[12] T. Herath and H. R. Rao, "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems,* vol. 18, pp. 106-125, 2009.

[13] D. Weirich and M. A. Sasse, "Pretty Good Persuasion: A First Step Towards Effective Password Security In The Real World," in *NSPW'01* New Mexico, USA: ACM, 2002.

[14] H. Xu, M. B. Rosson, and J. M. Carroll, "Increasing the Persuasiveness of IT Security Communication: Effects of Fear Appeals and Self-View," in *Symposium On Usable Privacy and Security*, Pittsburgh, PA, 2007.

[15] R. B. Cialdini, *Influence: Science and Practise* 4th ed. Boston: Pearson Education, 2001.

[16] N. D. A. Miller and M. R. Stafford, "An International Analysis of Emotional and Rational Appeals in Services vs Goods Advertising," *Consumer Marketing,* vol. 16, pp. 42-57, 1999.

[17] F. Rosselli, J. J. Skelly, and D. M. Mackie, "Processing Rational and Emotional Messages: The Cognitive and Affective Mediation of Persuasion," *Journal of Experimental Social Psychology,* vol. 31, pp. 163-190, 1995.

[18] R. B. Cialdini, "The Power of Persuasion," in Stanford Social Innovation Review, 2003.

[19] C. I. Hovland, I. L. Janis, and H. H. Kelley, *Communication and Persuasion: Psychological Studies of Opinion Change.* New Haven:: Yale University Press. , 1953.