Improving passwords: influence of emotions on security behaviour

Iwan Gulenko

Department of Information Systems, University of Technology Munich, Munich, Germany

Received 16 September 2013
Revised 20 January 2014
Accepted 23 January 2014

Abstract

Purpose – This paper aims to study the influence of emotions on security behaviour by reviewing Information Systems Security (ISS) topics in Information Systems (IS) literature. Researchers in ISS study how to motivate people to adhere to security policies; they mainly focus on cognitive models such as the technology acceptance model (Davis, 1985), innovation diffusion theory (Brancheau and Wetherbe, 1990), theory of planned behaviour (Mathieson, 1991) and social cognitive theory (Compeau and Higgins, 1995). Applying positive emotions such as joy and interest is feasible by adding emoticons and positive messages; we use this approach to improve password choosing.

Design/methodology/approach – We apply differential emotional theory (Izard 2002) from psychology to the context of ISS. Twenty-two participants took part in an experiment with the task of choosing strong but memorable passphrases. The dependent variable is the strength of the chosen passphrase. The task for the user is to come up with a passphrase that is both strong and memorable. We choose a between-subject design. The independent variable is the emotional interface that the user is confronted with.

Findings – We found that 5.35 words was the mean when participants were shown positive smiley faces and messages. When exposed to negative emoticons, the mean was only 4.35 words. Through ANOVA, we find the differences to be statistically significant ($F1; 20 = 3.16; p < 0.1$). We derive from the experiment that positive emotions should be used in ISS when making users start a habit (e.g. developing a new, individual password strategy), and we conclude from our literature review that negative emotions should be used when reinforcing a habit (e.g. taking care of shoulder surfing).

Originality/value – We contribute to practice by developing a user script that can be installed in all established Internet browsers. The script supports the user to choose a good passphrase strategy when registering for a new service. We find that trainings should not rely on facts only but must make use of emotions, which are crucial for human motivation.

Keywords Education, Information security, Security, Psychology, Training, Emotions theory, Passwords

Paper type Research paper

1. Introduction

This paper reviews Information Systems Security (ISS) topics in Information Systems (IS) literature. The lack of theory and theory testing in the literature about IS security training is still prevailing (Puhakainen and Siponen, 2010, pp. 759-761). The problems of inappropriate research designs and diversity of experimental tasks are methodological and thus easier to fix. Both can be mitigated by standardization. In medicinal psychology, it is widely accepted to develop an "exciting", new theory or treatment, etc., but it is tested with a "boring", standardized methodology, so others can verify the

Information Management & Computer Security
Vol. 22 No. 2, 2014
pp. 167-178

0968-5227
DOI 10.1108/IMCS-09-2013-0068

findings (Anonymous, 2010, pp. 29-32). The Publication Manual of the American Psychological Society (Anonymous, 2010)[1] teaches about the methodology for experiments with human participants. Such standards have already been transferred to information technology (IT)-related fields, such as human – computer interaction (MacKenzie, 2013) but have yet to be transferred to IS.

We want to find how much literature in IS covers ISS, how rigorous it is and how much it deals with security behaviour. Investigation the human component of ISS can be important than investigating the technology because it is changing a lot faster than human behaviour. However, security behaviour studies are limited to cognitive models such as the technology acceptance model (Davis, 1985), innovation diffusion theory (Brancheau and Wetherbe, 1990), theory of planned behaviour (Mathieson, 1991), (Gulenko, 2013) and social cognitive theory (Compeau and Higgins, 1995). The impact of emotion on motivation is known since centuries (Hume, 1741) but has rarely been applied to ISS, e.g. security training.

2. Literature review

We develop a search query in the EBSCO academic search engine[2] to find out about security topics in Information Systems literature. From the search string, the names of the queried journal can be seen: SU "security" AND (JN "MIS Quarterly" OR JN "Information Systems Research" OR JN "*Journal of the Association for Information Systems*" OR JN "*Journal of Management Information Systems*" OR JN "*Journal of Strategic Information Systems*" OR JN "*European Journal of Information Systems*" OR JN "Information Systems Journal" OR JN "Journal of Information Technology"). Security as a subject term results into 115 papers among 4,851 papers published in the Senior's Scholar basket[3] since 1977. Sixty-one papers deal with security as their main topic and only 17 deal with security behaviour as their main topic.

We find that top journal papers that contribute to ISS apply theory from other disciplines (e.g. Siponen and Vance (2010) apply "Neutralization theory" from criminology and Dinev and Hu (2007) apply "Theory of Planned Behaviour" from psychology). The Webster online dictionary defines prevention as "precaution, forethought"[4]. Science about preventive intervention includes research about prevention of HIV/AIDS, accidents, teenage pregnancy, delinquency, sexually transmitted disorders (STD's) or obesity, etc.[5]. Prevention of harmful behaviour towards corporative information systems, e.g. prevention of non-compliance of security policies, is central in ISS and much literature exists on this topic (Puhakainen and Siponen, 2010; Siponen and Vance, 2010; Siponen *et al.*, 2010; Beautement *et al.*, 2006; Bulgurcu *et al.*, 2010; Gulenko, 2013). Beaudry and Pinsonneault (2010) call for more research on emotions in IS. As a reply, we searched the literature of other disciplines for an application of emotions to preventive interventions. We find Izard (2002), who formulates seven principles for preventive intervention for misbehaving children (Table I).

2.1 Utilization of positive emotions

Using positive emotions enhances sociability, well-being and constructive behaviour. Positive emotions activate thought – action repertoires, mitigate or undo the emotional effects of negative events and increase mental flexibility. Through induction of positive emotions, it is possible to utilize them for preventive interventions. Izard (2002 p. 799)

introduces the interest – joy pattern that can be used for preventive intervention because there is a positive effect on exploration, learning and productivity.

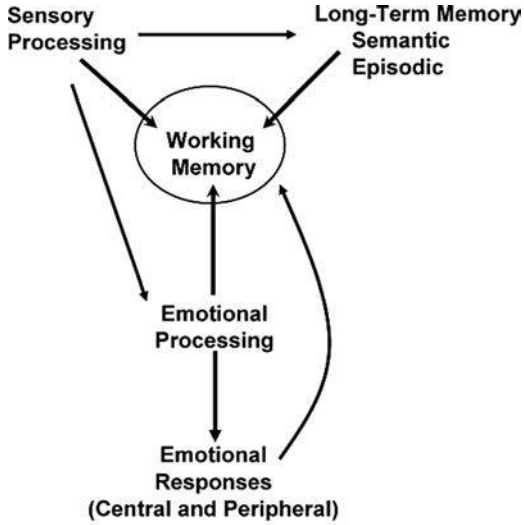
2.2 Utilization of negative emotions

Izard (2002) states that negative emotions influence learning and memory, also other authors, e.g. Lewis *et al.* (2008, p. 170) state: "The amygdala's influence on memory ensures that emotional events are also more likely to be remembered over time". The amygdala is a part of the brain responsible for handling emotions such as fear, anxiety and depression. It is also very important for memorizing. Lewis *et al.* (2008, pp. 171-172) state that there is a connection between emotions and consciousness. A strong emotion activates consciousness, consciousness activates the working memory and the working memory actives long-term memory, which is needed to remember passwords (Figure 1.

No	Summary	Useable
1	Using positive emotions such as joy and interest	X
2	Using negative emotions such as empathy to enhance memorability and learning	X
3	Overall theory on how to deal with anger	
4	High and low road to emotion	X
5	Processes, causes and effects and patterns of emotions	
6	Emotional deprivation in early life	
7	Modular and single, independent emotions	

Note: The useable principles for our scenario are checked

Table I.
Summary: seven principles of Izard (2002)



Source: Lewis et al. (2008), p. 172

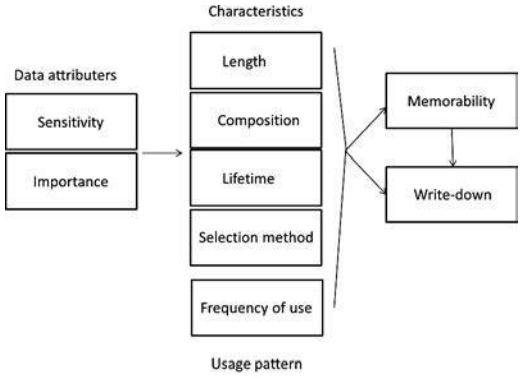
Figure 1.
How memory is connected to emotions

2.3 Emotion patterns in states and traits

This principle the difference between high and "low road to emotion", a term coined by LeDoux (1996). The latter is a way to process information rapidly, automatically and non-consciously. Feelings such as anger or fear can be processed this way. On the contrary, the high road is used for emotions that are caused more by thoughts of pride, jealousy or envy. Learning via the low road causes long-lasting memories that resist deletion (LeDoux *et al.*, 1989). Enforcing non-deletion of the chosen password from the users' brain would be useful, especially if we consider the costs that come from users forgetting their passwords and the efforts for resetting them. The usual password resetting mechanisms that ask for the mother's maiden name or the favourite movie are even higher security risks today because this information can often be easily acquired via social networks. If an emotion is activated via the low road, it crosses only a few synapses and, therefore, the use of the three-step technique is useless. Emotions activated by high-or low-road processes require different regulations in preventive interventions. The application and testing of the low road is yet to be done by psychologists, but researchers and practitioners have to keep in mind that those two principles, high and low road, exist (Izard, 2002, p. 806). We chose the feelings interest, joy, guilt and sadness because these emotions intersect Ekman and Friesen' s study (1971) that asserts that emotions are universal in humans and Izard's study (2002) that they can be used for preventive intervention.

3. Conceptual background

Recent breaches of databases show the low quality of passwords still chosen by users. Passwords are too short and too simple. An analysis of one million passwords in the breach of the Sony password database showed that 50 per cent of the passwords were less than eight characters long and only 1 per cent contained non-alphanumeric characters (Hunt, 2011). Although new authentication mechanisms like combining passwords and possession of tokens increases security, passwords are almost always required for access and often solely required to authenticate oneself (Whitman, 2003). Therefore, attempts to discover methods to improve password quality without loosing memorability are still valuable. If one enforces random, system-generated passwords, users find those passwords difficult to remember (Yan *et al.*, 2004) and as a result may start to write them down. Users do not believe that the chances of being attacked outweigh the extra work to choose a strong password (Adams and Sasse, 1999, 44). A large-scale study of password use and re-use habits came to the conclusion that providing instructions on how to create secure passwords, password managers or providing tools such as strength-meters to enforce the strength of a password had only limited success (Florencio and Herley, 2007). Many investigations tried to mitigate this. Forget *et al.* (2008) built an application that increases the security of a chosen password by inserting random characters. Ross *et al.* (2005) developed a browser extension that mingles the website to the password of the user, enabling him to reuse the same password for different sites. One of the most cited papers on passwords is Zviran and Haga (1999). He defined key issues regarding password security (Figure 2): length, composition, lifetime and selection method. One finds that increasing the length enhances the strength of a password exponentially, whereas increasing composition enhances it only linearly: c^l where c denotes complexity, meaning possibility for each position, and l denotes the length of the password.



Source: Adapted from Zviran and Haga (1999)

Figure 2.
Key issues in password security

Proactive password checking is considered effective to enforce password policies and prevent users from choosing weak passwords (Bishop and Klein, 1995, p. 6). When a user types his password, a proactive checker determines whether the choice is acceptable. Current design of password checkers among the big platforms such as Facebook, Twitter, Google Mail, Yahoo Mail or Hotmail are summed up in Table II. Facebook and Twitter enforce passwords that are at least six characters long. Hotmail enforces to use at least two different character types, offering four character types such as small letters, capital letters, numbers and symbols, and the password must be at least eight characters long. Yahoo enforces eight characters, but is the only platform that allows simple passwords such as 12345678. Google Mail enforces at least eight characters and gives advices not to choose personal information such as pet names as passwords or reuse passwords one already has chosen for other platforms. Twitter, Yahoo and Google Mail use a horizontal bar that gives instant feedback about the quality of the typed password. They also make use of words like "weak", "strong" or "very strong". We do not find those password checkers are built on publicly available, scientific work.

To solve the conflicting goals of security and memorability, Keith *et al.* (2007) researched on passphrases as an authentication mechanism. They can be used whenever the system allows a long string for example "to be or not to be" (Zviran and Haga, 1993). The idea is not new (Porter, 1982), but legacy systems (e.g. UNIX) limited the length of the password. Nowadays, online systems or modern operating systems accept very long strings as passwords. Increasing length is more influential than

Platform	Enforced policy	Visual validation	Advices
Facebook.com	Six characters		
Twitter.com	Six characters	X	
Hotmail.com	Eight characters, at least two different characters types		X
Yahoo.com	Eight characters	X	X
Mail.google.com	Eight characters	X	X

Table II.
State of the art of password checkers of major platforms

increasing the character set. However, with length security is gained but usability lost. Bad usability means that the user fails to log in. This can have two reasons. The users forgot the password or they mistype it. In a 12-week experiment, Keith *et al.* (2007) showed that users' experience and satisfaction with passphrases are no different from passwords, and the loss of usability almost solely comes from mistyping. Keith (2009) addressed this issue by choosing well-designed passphrases consisting of ordinary words, omitting numbers and special characters to maintain the normal "word processing mode" (Keith, 2009, p. 69). The problem of login failures because of typos disappeared.

Existing literature mainly focuses on what information to give users. Research has been based on cognition and less attention has been given to emotions (Beaudry and Pinsonneault, 2010). However, the impact and importance of emotion is known since centuries (Hume, 1741), and it is surprising that is has rarely been addressed in IS. We focus on ISS, a domain in IS, and derive two hypotheses from our literature review.

H1. Negative emotions should be used when reinforcing a habit (e.g. taking care of shoulder surfing when one logs in).

H2. Positive emotions should be used when starting a habit (e.g. when deciding over a new password strategy).

Since emoticons induce emotions in people (Yuasa *et al.*, 2006), even simply adding an emoticon to a existing proactive password checker seems promising for practice (Forget *et al.*, 2007). However, just adding a laughing smiley as a reward may not be enough because rewards seem not to have significant effect on compliance, and punishments seem to work in a statistically significant way (Siponen *et al.*, 2010, p. 69). We see that in existing literature punishments, and negative emotions are often used to reinforce a habit. Thus, we can derive that *H1* is supported just by the literature. It is not yet known when to use positive emotions and whether it has an effect on, e.g. security training. We derive proof for *H2* in the next chapter.

4. Training: choose strong but memorable passphrases

Ninety-three per cent of passwords have ten characters or less (Hunt, 2011). Therefore, we assume that passphrases are seldom used by the general public. We assume that most users are not familiar with it. Therefore, they can come up with a new, individual, not yet used passphrase. We replicate the methodology of Johnston and Warkentin (2010, p. 556) to test *H2* from the last chapter; drawing upon research in marketing, psychology and economics, we apply concepts of goal framing and self-view to investigate how attitudes and norms can be manipulated. The overarching theories are positive and negative emotions (Izard, 2002). In the context of this study, framing of a message serves to focus the individual either on preventing the threat and associated negative outcomes of a security violation (negative) or on the utilization of effective coping responses to create a safe, reliable internet environment (positive). The training can be accessed online[6]. It was pre-tested with five relatives of the author. Subjects were asked to participate via email, social media, etc. Self selection bias occurs but is constant among the groups. In Figure 3, one can see the training that allows to learn about passphrases in a few sentences that are built on insights about passphrases taken from Keith's (2009) study and other Internet sources[7]. A pre-and post-test survey is used to evaluate the knowledge of the user, both before and after the training.

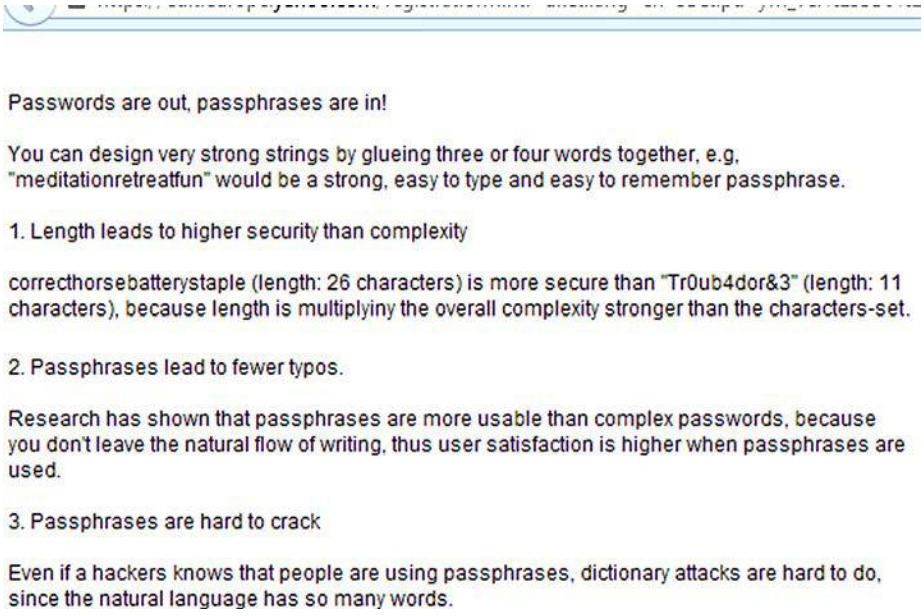


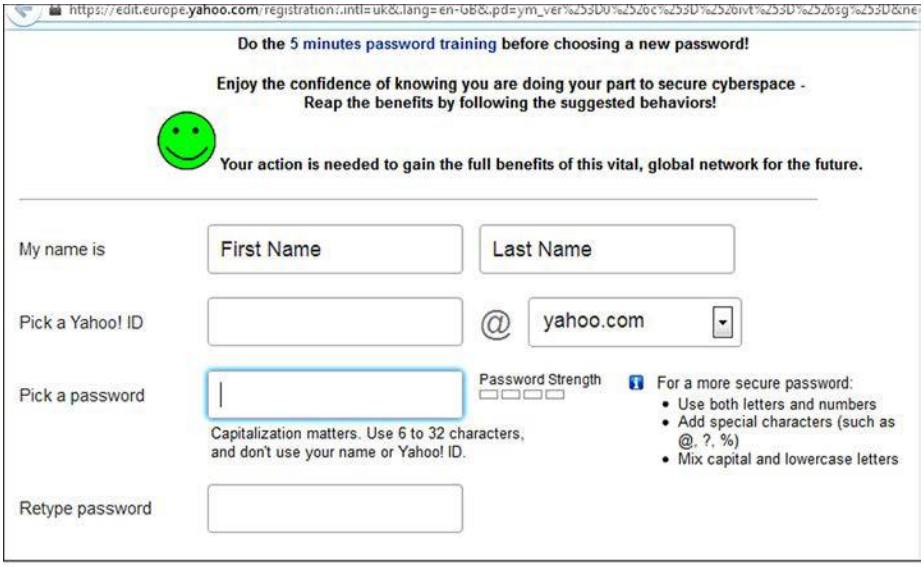
Figure 3.
Training to use passphrases instead of passwords

4.1 Data analysis

Twenty-two subjects took part in the training and were capable of coming up with new passphrases. Because our sample set is diverse (1 South Korean, 17 German, 2 Russian, 1, Finnish and 1 Czech), we take the US Internet population as reference. Table III is based on statistics of the Internet population of the USA[8]. All subjects showed a better understanding of the importance of length on the security of passwords after the training, but the crucial task was to come up with a strong but memorable new passphrase at the end of the training. Positive (see top of Figure 4) or negative (see top of Figure 5) emotions were triggered. We found that 5.35 words was the mean when participants were treated with positive smilies and messages. When treated with negative emotions the mean was only 4.35 words (Table IV). We use the methodology from the Publication Manual of the American Psychological Society (Anonymous, 2010) to analyze the data and present our results: Through an one-way between subjects ANOVA, we find the differences to be statistically significant ($F_{1,20} = 3.16, p < 0.1$). The number of words in a passphrase is, thus, higher when the participants are treated with positive emotions compared to being treated with negative emotions. Thus, *H2* from last chapter is supported. We derive that positive emotions should be used in ISS.

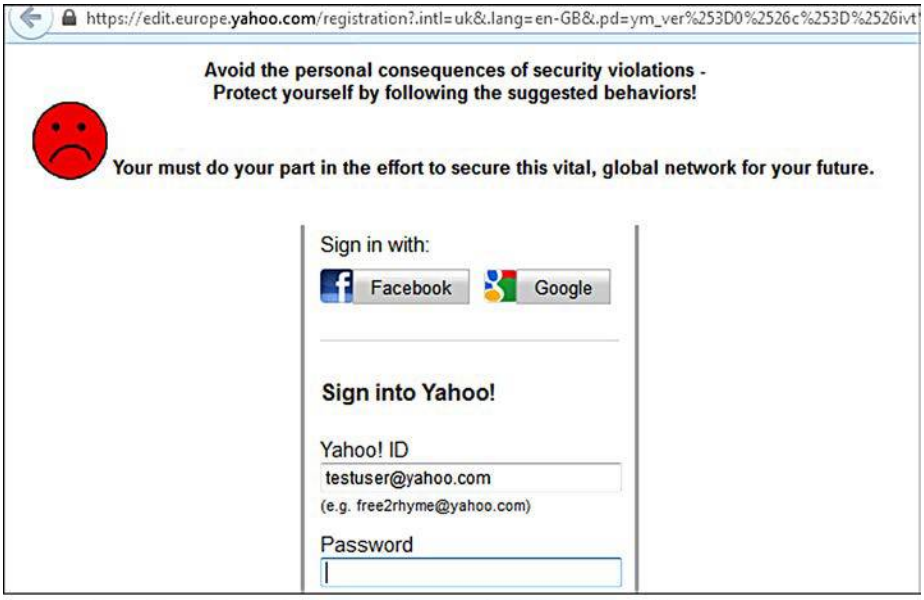
Demographic characteristics (Age: years)	Sample (per cent)	US internet population (per cent)
15-24	23	21
25-34	27	19
35-44	23	18
45-64	27	33
≥65	0	8

Table III.
Population using the internet and our sample ($N = 22$)



Source: Text adapted from Anderson and Agarwal (2010, pp. A9-A10)

Figure 4.
Positive emotions when registering



Source: Text adapted from Anderson and Agarwal (2010, pp. A9-A10)

Figure 5.
Negative emotions when logging in

4.2 Browser extension

The browser script implements the findings from the preceding chapters. It is written in JavaScript and can be installed using Greasemonkey[9] on Firefox or Tampermonkey[10] on Google Chrome. The user is faced with positive emotions, interest and joy during the registration phase (Figure 4). Thus, the user is encouraged to do the 5-minute password training. When the user wants to login, he is phased with negative emotions such that he watches out not to fall victim for shoulder surfing, etc. (Figure 5).

5. Discussion and conclusion

As stated by Dennis and Valacich (2001, p. 17), the best research designs tend to accept flaws and highlight their strengths. Our study suffers from several limitations. The sample is only 22 participants and although we had a slightly significant result ($p < 0.1$), a smaller value for p would be more reliable to prove the relationship between emotions of the users and passphrase strength. It is not clear how long the participants looked at the smiley, how carefully they read the message and, thus, how bad or good they felt. Moreover, it was assumed that more words lead to stronger strings, without distinguishing between short, long, rare or frequent words. Thus, negatively triggered participants may use fewer but more complicated words. Finally, our findings can only be applied to password-choosing behaviour and more studies are needed to confirm the findings or to extend them to security behaviour in general.

Following the call to research on emotions of Beaudry and Pinsonneault (2010), we applied differential emotional theory (Izard, 2002) from psychology to the context of ISS. We derive that the use of cognitive models such as the theory of planned behaviour (Gulenko, 2013) is not enough and positive emotions should be used in ISS when making users start a habit (developing a new, individual password strategy). We conclude from our literature review that negative emotions should be used when reinforcing a habit (e.g. taking care of shoulder surfing). We contribute to practice by developing a user script that can be installed in all established Internet browsers. The script supports the user to choose a good passphrase strategy when registering for a new service. We find that trainings should not rely on facts only but must make use of emotions, which are crucial for human motivation.

The goal of our study was to explain how emotions influence password choosing. The results imply that there is a significant effect of positive emotions on security behaviour – approaches that use positive emotions improve security behaviour more than means that use deterrence. Therefore, future research should focus on theories and methodologies that support this view. An example is motivational interviewing (Miller and Rollnick, 2002). It is an evidence-based treatment methodology that enables to train people to change their habits. It assumes that humans are not changing their bad habits because they have conflicting thoughts about the change; they are ambivalent and have a good motivation. They are rarely resistant with a bad motivation. People want to change, but they have to come up with a way and goal on their own – having the benefits

Group	Mean	SD
Positive emotion	5.35	1.68
Negative emotion	4.35	0.85

Table IV.
Mean and SD ($N = 20$)

of the change in mind. To extend the work described in this paper, future research should build on positive views, as used in techniques like motivation interviewing.

Notes

1. www.apa.org/ (accessed on 11.12.12).
2. http://search.ebscohost.com (accessed 12 December 2012).
3. http://home.aisnet.org/displaycommon.cfm?an=1&subarticlenbr=346 (accessed 4 March 2012).
4. www.webster-dictionary.net/definition/Prevention (accessed 6 November 2012).
5. www.preventionresearch.org/prevscience.php (accessed 6 November 2012).
6. http://password-training.site50.net (accessed 4 March 2012).
7. http://xkcd.com/936/ (accessed 4 March 2012).
8. www.census.gov/hhes/computer/ (accessed 19 February 2012).
9. https://addons.mozilla.org/en-US/firefox/addon/greasemonkey/ (accessed 4 March 2012).
10. https://chrome.google.com/webstore/detail/tampermonkey/dhdgffkkebhmkfjojejmpbldmpobfkfo (accessed 4 March 2012).

References

Adams, A. and Sasse, M.A. (1999), "Users are not the enemy", *Communication of ACM*, Vol. 42 No. 12, pp. 41-46.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34 No. 3, pp. 613-643.

Anonymous, A.P. (2010), *Publication Manual of the American Psychological Association*, American Psychological Association, Washington, DC.

Beaudry, A. and Pinsonneault, A. (2010), "The other side of acceptance: studying the direct and indirect effects of emotions on information technology use", *MIS Quarterly*, Vol. 34 No. 4, pp. 689-710.

Beautement, A., Sasse, M.A. and Wonham, M. (2006), "The compliance budget: managing security behaviour in organisations", *NSPW*, New York, NY.

Bishop, M. and Klein, D.V. (1995), "Improving system security via proactive password checking", *Computers and Security*, Vol. 14, 233-249.

Brancheau, J.C. and Wetherbe, J.C. (1990), "The adoption of spreadsheet software: testing innovation diffusion theory in the context of end-user computing", *Information Systems Research*, Vol. 1 No. 2, pp. 115-143.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Compeau, D.R. and Higgins, C.A. (1995), "Application of social cognitive theory to training for computer skills", *Information Systems Research*, Vol. 6 No. 2, pp. 118-143.

Davis, F.D. (1985), "A technology acceptance model for empirically testing new enduser information systems: theory and results", *Ph.D. thesis*, Institute of Technology, MA.

Dennis, A. and Valacich, J. (2001), "Conducting research in information systems", *Communications of the AIS*, Vol. 7 No. 5, pp. 1-41.

Dinev, T. and Hu, Q. (2007), "The centrality of awareness in the formation of user behavioral intention toward protective information technologies", *Journal of AIS*, Vol. 8 No. 7.

Ekman, P. and Friesen, W.V. (1971), "Constants across cultures in the face and emotion", *Journal of Personality and Social Psychology*, Vol. 17 No. 2, 124-129.

Florencio, D. and Herley, C. (2007), "A large-scale study of web password habits", *Proceedings of the 16th international conference on World Wide Web*, *ACM, New York, NY*.

Forget, A., Chiasson, S. and Biddle, R. (2007), "Persuasion as education for computer security", in Bastiaens, T. and Carliner, S. (Eds), *Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2007*, *AACE, Quebec City, Canada*.

Forget, A., Chiasson, S., van Oorschot, P.C. and Bibble, R. (2008), "Improving text passwords through persuasion", *SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security*, ACM, New York, NY.

Gulenko, I. (2013), "Social against social engineering: concept and development of a facebook application to raise security and risk awareness", *Information Management and Computer Security*, Vol. 21 No. 2, pp. 91-101.

Hume, D. (1741), *A Treatise of Human Nature*, Reprint Oxford University Press, Oxford.

Hunt, T. (2011), "A brief Sony password analysis", available at: www.troyhunt.com/2011/06/brief-sony-password-analysis.html

Izard, C.E. (2002), "Translating emotion theory and research into preventive interventions", *Psychological Bulletin*, Vol. 128 No. 5.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549-566.

Keith, M. (2009), "A behavioral analysis of passphrase design and effectiveness", *Journal of the Association for Information Systems*, Vol. 10 No. 2.

Keith, M., Shao, B. and Steinbart, P.J. (2007), "The usability of passphrases for authentication: an empirical field study", *International Journal of Human-Computer Studies*, Vol. 65 No. 1, pp. 17-28.

LeDoux, J. (1996), *The emotional brain: the mysterious underpinnings of emotional life*, Touchstone book, Simon & Schuster.

LeDoux, J.E., Romanski, L. and Xagoraris, A. (1989), "Indelibility of subcortical emotional memories", *Journal of Cognitive Neuroscience*, Vol. 1 No. 3, pp. 238-243.

Lewis, M., Haviland-Jones, J. and Barrett, L. (2008), *Handbook of Emotions*, 3rd ed., Guilford Publications.

MacKenzie, I. (2013), *Human-Computer Interaction: An Empirical Research Perspective*, Elsevier Science.

Mathieson, K. (1991), "Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior", *Information Systems Research*, Vol. 2 No. 3, pp. 173-191.

Miller, W.R. and Rollnick, S. (2002), *Motivational Interviewing: Preparing People to Change*, Guilford Press.

Porter, S.N. (1982), "A password extension for improved human factors", *Computers and Security*, Vol. 1 No. 1, pp. 54-56.

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: an action research study", *MIS Quarterly*, Vol. 34 No. 4, pp. 757-778.

Ross, B., Jackson, C., Miyake, N., Boneh, D. and Mitchell, J.C. (2005), "Stronger password authentication using browser extensions", *Proceedings of the 14th conference on USENIX Security Symposium – Volume 14*, *USENIX Association, Berkeley, CA*.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-503.

Siponen, M., Pahnila, S. and Mahmood, M. (2010), "Compliance with information security policies: an empirical investigation", *Computer*, Vol. 43 No. 2, pp. 64-71.

Whitman, M.E. (2003), "Enemy at the gate: threats to information security", *Communication of ACM*, Vol. 46 No. 8, pp. 91-95.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2004), "Password memorability and security: empirical results", *Security Privacy, IEEE*, Vol. 2 No. 5, pp. 25-31.

Yuasa, M., Saito, K. and Mukawa, N. (2006), "Emoticons convey emotions without cognition of faces: an fmri study", *CHI '06 Extended Abstracts on Human Factors in Computing Systems*, ACM, New York, NY.

Zviran, M. and Haga, W.J. (1993), "A comparison of password techniques for multilevel authentication mechanisms", *The Computer Journal*, Vol. 36 No. 3, pp. 227-237.

Zviran, M. and Haga, W.J. (1999), "Password security: an empirical study", *Journal of Management Information System*, Vol. 15 No. 4, pp. 161-185.

About the author

Iwan Gulenko holds a BSc in Information Systems from Technische Universität München and is now studying an Msc in Computer Science with focus on IT Security. With his bachelor's thesis, he won the second prize in the "IT security conference for the next generation" from Kaspersky Labs; in the subsequent year, his master's thesis was ranked third among more than a hundred initial applications. Iwan Gulenko can be contacted at: gulenko@in.tum.de

This article has been cited by:

1. Sangseo Park, Jane MoonStrategic Approach towards Clinical Information Security 329-359. [CrossRef]