Persuasive Information Security

A Behavior Change Support System to Help Employees Protect Organizational Information Security

[1]Marc Busch, [2]Sameer Patil, [1]Georg Regal, [1]Christina Hochleitner, [1]Peter Fröhlich and [1]Manfred Tscheligi

[1]AIT – Austrian Institute of Technology GmbH
{FirstName.LastName}@ait.ac.at
[2]Department of Computer Science and Engineering
Polytechnic School of Engineering, New York University
sameer.patil@nyu.edu

Abstract. Digital information is an important asset in the corporate world. Organizations typically devise policies and guidelines to help employees protect the security of such information. Complying with these policies can often be confusing and difficult and may obstruct the task at hand, thus potentially leading employees to circumvent or ignore these policies. Commercial technology and training programs to mitigate this issue suffer from various shortcomings. To overcome these limitations, we present a Behavior Change Support prototype that implements six persuasive features: Security Points, Security Quiz, Challenges, Statistics, Personalization, and Risk Communication. Evaluation of the prototype established persuasive security as a promising approach for influencing user attitudes and behaviors regarding secure work practices. We apply the findings to offer suggestions for how the six persuasive features could be further enhanced.

1 Introduction

Breaches in organizational information security can have severe consequences. Loss or theft of sensitive digital information can cost millions and damage the organization's reputation. Organizations therefore have a strong incentive to protect their digital information. Sources of threats to information security are not limited to external entities. Studies show that a sizable proportion of information security breaches are caused inadvertently in the course of routine work of employees, despite absence of malicious intent.

One of the mechanisms used by organizations to deal with the protection of information is an information security policy, i.e., the rules and guidelines defining permitted and forbidden actions related to information assets. Naturally, organizations want and expect employees to adhere to the prescribed policy. However, employees may find it challenging to comply with their employer's information security policy. Factors that underlie these difficulties include perceived self-efficacy and subjective norms toward information security in the organization [1,15].

Enforcement of security policies via purely technical means (e.g., cutting access off when the network connection is insecure) takes away perceived behavioral control from employees, thus creating frustration and annoyance. We present a Behavior Change Support System that uses persuasive features aimed at promoting compliance with organizational information security policies without compromising perceived behavioral control.

We believe that the key to the effectiveness of such a system is educating employees regarding the risks and rationale that underlie the policy at hand [14]. Toward this end, we designed six features aimed at increasing employee awareness and knowledge of organizational information security policies and changing attitudes and behavior toward greater compliance with the policy while supporting engagement with the issue of organizational information security.

Specifically, we formulated the following research question: which persuasive system features are most likely to affect attitudinal and behavioral change regarding organizational information security?

To tackle the above question, we conducted a user study of a prototype implementation of our designs. We found that persuasive strategies could be beneficial for promoting secure user practices, albeit to varying extents. At a high level, our contribution consists of demonstrating the value of persuasive strategies as a means for promoting secure user practices.

We first describe the theoretical background of our work. Next, we describe the prototype design of the persuasive features followed by the details of the user study conducted to evaluate the features. We report the findings regarding the persuasiveness of the prototype Behavior Change Support System and conclude by reflecting on the findings.

2 Related Work

Technological approaches for increasing compliance with security policies include commercial applications that manage endpoint security (e.g., IBM Unified Endpoint Management). These applications often enforce information security policies without helping end users understand the importance of the policy and the consequences of violations. While training and awareness programs [10] empower employees regarding secure work practices, such programs are expensive and time-consuming and need periodic repetition.

A Behavior Change Support System [13] is an effective and popular approach for changing human attitudes and behavior. Based on principles of persuasion, we designed such a system in order to foster positive employee attitudes toward organizational information security, empower employees to make informed security decisions, and promote secure work practices as the subjective norm in the organization.

Technology that utilizes persuasive strategies has been applied to promote a variety of target behaviors in diverse domains, such as education, health, sustainability, etc. For example, Gamberini et al. [7] noted the effectiveness of personal statistics and tailored suggestions and advice for affecting power consumption, and Munson and

Consolvo [11] found that setting personal weekly goals and monitoring progress were useful in promoting greater physical activity. Research further shows that the effectiveness of persuasive technologies could be improved by taking into account individual differences in receptiveness to the underlying persuasive strategy [8]. For instance, Zuckerman and Gal-Oz [18] propose personalizing persuasive technologies based on an individual's receptiveness for self-quantification, virtual rewards, and social comparison.

However, some of the above studies report contradictory results. For instance, Zuckerman and Gal-Oz [18] found that virtual rewards led to increased physical activity, yet most of their study participants did not find the rewards meaningful. Similarly, Gabrielli et al. [6] received mixed reactions toward the strategies of challenges, statistics, rewards, social comparison, and suggestions (via text messages); some participants described them as motivating while others did not find them useful. These contradictions point to the need for further investigation that could help reconcile these discrepancies.

3 Prototype of Persuasive Features

Only a few studies [3,5,17] have so far applied persuasive technology for usable security. However, these studies utilized relatively small student samples, not our target population of knowledge workers. Moreover, these explorations were limited to specific practices, such as choosing passwords, rather than considering all work practices that impact the security of the organization's information resources. To address this gap, we built a prototype that utilized 8 of the 28 persuasive strategies from the comprehensive framework outlined by Oinas-Kukkonen and Harjumaa [12]. The prototype was an interactive front-end interface for an information security application. This application is intended to be installed on the work devices of employees. As an initial exploration of the front-end interface, our prototype was implemented to function within a Web browser. The prototype system covered the following eight persuasive strategies described by Oinas-Kukkonen and Harjumaa [12]:

Rewards: The system rewards the target behavior, in our case with Security Points and Security Badges.
Tailoring: The system is personalized to a user’s interests and personality, here through a questionnaire that determines features of potential interest to each user.
Competition: The system promotes competition with others, in our application through Challenges.
Simulation: The system provides a means for understanding the connection between behavior and its consequences, in our case by communicating potential risks.
Social comparison: The system allows comparing one’s performance with others, in our prototype via statistics of past security behavior.
Suggestions: The system recommends appropriate behavior at opportune moments, in our application by suggesting interesting features determined using questionnaire responses.

(Social) learning: The system facilitates learning about target behavior, in our prototype by a Security Quiz with questions about the information security policy.
Self monitoring: The system provides a means to track one's performance and status, in our implementation via Statistics of past security behavior.

We term an operational system *implementation* of one or more persuasive strategies as a persuasive *feature*. Our prototype incorporated the above eight persuasive strategies in the form of six persuasive features, viz., Security Points, Security Quiz, Challenges, Statistics, Personalization, and Risk Communication. We chose strategies and features based on the promising techniques identified in the literature, e.g. Gamberini et al. [7]. We limited the exploration to six persuasive features in order to maintain a number manageable within one study.

Table 1. Mapping between prototype features and persuasive strategies.

Prototype Feature	Primary Persuasive Strategy	Secondary Persuasive Strategy
Security Points	Rewards	-
Security Quiz	(Social) learning	Rewards
Challenges	Competition	Rewards
Statistics	Self monitoring	Social comparison
Personalization	Tailoring	Suggestion
Risk Communication	Simulation	Rewards

Table 1 shows the mapping between the persuasive strategies we employed and the corresponding persuasive features within our prototype. It can be noted that each feature operationalized a primary and a secondary strategy. The exception was Security Points, which did not incorporate a secondary strategy. We summarize each of these features below. Busch et al. [2] provide further details.

Security Points. Users could collect virtual rewards in the form of Security Points. As described below, Security Points could be earned by taking a Security Quiz, completing Challenges, or answering a Personalization questionnaire. Users were awarded Security Badges corresponding with the progressive accumulation of Security Points, viz., Beginner, Intermediate, Expert, Professional, and Master. Security Points could be used to "buy" perks, such as time to use social media and colors to change the look-and-feel of the prototype. Points were deducted if the user's actions were deemed insecure for organizational information security. As mentioned below, the Risk Communication feature of the prototype warned users about the loss of Security Points resulting from insecure behavior.

Security Quiz. In order to facilitate learning, users were presented with quizzes on practices and scenarios related to the information security policy. Each question offered multiple answer choices, only one of which could be chosen as the answer. Although one of the answer options was the best choice, the other options could also be appropriate choices. Users were rewarded with Security Points corresponding to the appropriateness ranking of the chosen answer.

Challenges. Motivation through competition among employees was promoted by this feature. Users could accept Challenges that were either competitive (e.g., "Behave more securely than your colleagues for one week.") or individual (e.g., "Comply with all security policies for one week."). Users were rewarded with Security Points upon successful completion of the assigned Challenges.

Statistics. The Statistics feature showed the number of information security policy violations per week committed by the user as well as the average number of violations for other employees across the organization. The user was presented with visualizations of various Statistics regarding security compliance, enabling comparison of his or her practices with those of co-workers and promoting the persuasive strategies of self-monitoring and social comparison.

Personalization. By answering a questionnaire that determined persuadability for each of the six persuasive features, a user had the possibility to choose features that could be especially fitting for him or her. The Personalization questionnaire consisted of statements related to the persuasive features (e.g., "I like to compete against others" related to the Challenges feature) rated on a Likert-type scale. For each persuasive feature, the individual obtained a persuadability score which determined his or her individual receptiveness to that feature. Based on questionnaire responses, the system made personalized suggestions for helping the user follow secure information practices. For example, if questionnaire responses indicated that the user is greatly influenced by social comparison, the prototype encouraged the user to consult the Statistics (see above) to compare his or her practices with those of co-workers. To incentivize personalization, users were awarded Security Points for completing the questionnaire.

Risk Communication. The prototype integrated with the underlying operating system to detect when a user might be engaging in risky information security practices. In such cases, the prototype warned the user of the risk for the organization as well as personal consequences for the user (simulation). For example, if the user attempted to transfer a sensitive document using an insecure connection, a popup window warned the user that the practice violated organizational security policy and he or she would lose Security Points. For documents with low sensitivity, the user could choose to heed or ignore the warning. For highly sensitive documents, access was blocked.

4 Method

We employed the prototype to conduct a user study evaluating the perceived persuasiveness of the implemented features. The user study was carried out online via the Web. Participants read the following scenario: *You are waiting at the airport to embark on a business trip. While waiting, you wish to prepare a business document. In order to work on the document, you need sensitive information from a file stored on the company's servers. The security policy of your employer states that you should access sensitive company information only from encrypted (secure) network connections. The wireless Internet connection at the airport is unencrypted.*

The scenario served as the background for framing the study. However, our questions to the participants about the persuasive features were independent of the scenario. Participants were asked to imagine themselves in the scenario and open our Web based prototype and explore and interact with each feature one at a time by clicking the corresponding prototype tab. The Security Points tab described how the user's behavior could lead to earning or losing points and badges. Participants were also shown the current point balance along with an explanation of how it could be redeemed for rewards. The Security Quiz tab included one example question: "How can I best protect the information in my office?" Participants were awarded 1 Security Point for answering correctly or provided feedback if their answer was incorrect. The Challenges tab provided the opportunity to earn Security Points by committing to two example challenges, one competitive ("Behave more securely than your colleagues for one week." – 10 Security Points) and one individual ("Comply with all security policies for one week." – 20 Security Points). The Statistics tab showed a temporal graph of security policy violations committed by the user along with the average number of violations across all employees of the organization. The Personalization feature presented the participant with a questionnaire regarding his or her attitudes and behaviors. The prototype was not connected to a back-end system. Therefore, upon completing the questionnaire, participants received an explanation regarding how the responses would have been utilized for personalized suggestions when connected to the back-end security system. To evaluate the sixth feature, viz., Risk Communication, participants were asked to open another application called "File Explorer." Within this application, participants were instructed to (try to) open 'Low-Sensitive Document.pdf,' 'Medium-Sensitive Document.pdf,' and 'High-Sensitive Document.pdf.' Clicking on the 'Low-Sensitive Document.pdf' brought up a warning regarding a security policy violation. Given the low sensitivity of the file, the warning allowed the user to proceed if he or she desired. The warning popup for the other two files blocked opening the file with no user override.

With the exception of Risk Communication, all features were presented in random order by randomizing the tab sequence in the prototype. In the case of Risk Communication, we felt that the effort of starting a new application and then returning to the prototype might lead to attrition. We therefore excluded the Risk Communication feature from randomization; it was always the final task.

After encountering each persuasive feature, participants were asked to rate items regarding usefulness, enjoyment, increase in awareness, attitude and behavior change (adapted from Drozd et al. [4] and Venkatesh and Bala [16]) on a 7-point Likert-type scale from Strongly disagree (1) to Strongly agree (7). These items were inspired by a persuasiveness model [9] and the Technology Acceptance Model 3 [16].

The participants were recruited from a database of voluntary study participants from Austria. We screened potential participants such that only those who were employed full- or part-time were eligible. Participants worked at various organizations in and around Vienna, Austria.

5 Initial Findings

Of the 81 participants, we retained the 64 who indicated the presence of explicit information security policies at their organizations. Gender distribution was roughly equal (33 females and 31 males) with ages ranging from 21 to 60 (median = 32). As the five items for measuring the persuasiveness of the single features were adapted from several different scales [4,16], we checked the dimensionality of these items with an exploratory factor analysis. The corresponding scree plots for each feature pointed to a single underlying latent factor based on the eigenvalue criterion (eigenvalue > 1). We interpreted and labeled this factor as the *persuasiveness* of the feature, leading to a single overall persuasiveness score for each prototype feature.

Shapiro-Wilk normality tests revealed that some of the scores violated the assumption of normality. Therefore, we used non-parametric statistical tests in subsequent analyses. Consequently, we report the medians of these scores, instead of means.

Figure 1 shows notched box plots of the persuasiveness scores for each feature, with higher values indicating greater persuasiveness. The notches in the boxes indicate the 95 percent confidence interval of the median. The line at 4 on the y-axis marks the neutral mid-point of the 7-point Likert-type scale. Based on the medians, Risk Communication, Statistics, and Security Quiz were rated as more persuasive, while Security Points, Challenges, and Personalization were found less persuasive.

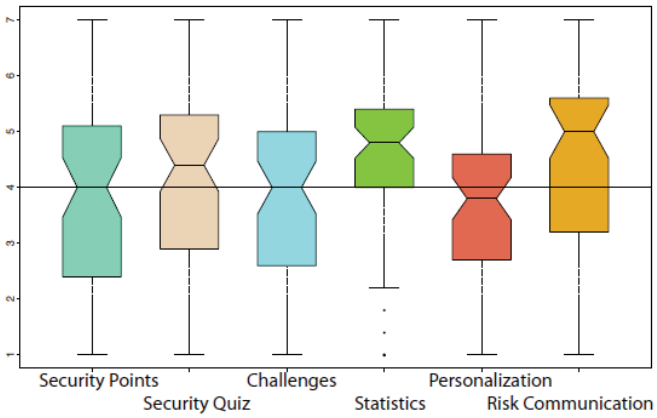

Figure 1. Persuasiveness scores for each prototype feature with 1= Strongly Disagree to 7= Strongly Agree.

We employed one-sample Wilcoxon tests to examine if each feature was rated significantly better or worse than the neutral mid-point (4) of the 7-point Likert-type scale. We found that Statistics ($V = 1380.5$, $p < 0.001$) and Risk Communication ($V = 1225$, $p < 0.05$) were rated significantly better than the mid-point. The ratings for Security Quiz ($V = 1062$, $p = 0.40$) were not significantly better than the mid-point, while those for Personalization ($V = 704.5$, p-value = 0.33) were not significantly worse. Finally, Security Points ($V = 658.5$, $p = 0.26$) and Challenges ($V = 729.5$, $p = 0.44$) were neither significantly better nor worse than the mid-point.

6 Discussion

By its nature, security is secondary to an ongoing task, often obstructing the task at hand. Therefore, even neutral ratings of security features can be seen as a success. Our results thus indicate the promise of persuasive security for helping employees understand and follow secure work practices compliant with the organizational security policy.

At the same time, the variance within each feature suggests that individuals could react to a particular feature in differing ways. Ensuring coverage across such diversity of views may require a combination of several features and strategies, instead of relying on a single aspect. Our preliminary findings (see Figure 1) indicate that Statistics, Risk Communication, and Security Quiz are especially promising persuasive strategies in the information security context.

Open-ended participant responses pointed to further improvement in each of the persuasive features in the prototype:

Security Points. Features such as Security Points and Badges introduced playful and game-like aspects to the interaction. Participant responses indicated that it is important to consider the presentation of such elements for an organizational context, where professionalism and seriousness are important and run counter to playfulness.

Security Quiz. Despite including only a single question, participant reactions to the Security Quiz feature provided useful design insight. In particular, we found that it is essential not only to reveal the correct answer but also to explain the rationale behind how the answer was derived.

Challenges. Our implementation of Challenges included a group task that asked users to compete with fellow employees. Participants cautioned that such competition could run counter to the organization’s culture and risk alienating colleagues.

Statistics. The Statistics feature was well-liked. We believe that the appeal stems from the usefulness of the information for comparing one's practices with the larger picture as well as its visual presentation that made it easy to comprehend.

Personalization. Participants found it difficult to understand the Personalization feature and its connection with information security. These difficulties appeared to be driven largely by the one-time nature of the study and the non-functioning nature of this feature in the Prototype.

Risk Communication. While participants appreciated the contextual nature of Risk Communication, they complained about its disruption and obtrusiveness. Moreover, participants were frustrated because the dialog did not offer concrete guidance on achieving the task in a secure manner. These reactions reveal that effective Risk Communication needs to balance a variety of tensions, such as whether to interrupt the user or provide feedback in the background and whether to block user actions completely or allow users to proceed with a policy violation.

These observations could serve as useful guidelines for improving the studied persuasive features and applying them in systems. For instance, Statistics could benefit from the addition of a larger set of security-related behaviors and enabling an understanding of security that considers nuance, such as severity and risk. Similarly, Risk

Communication needs to minimize disruption and guide the user toward the secure alternative, instead of serving a purely informational and/or access control function.

7 Limitations

We must also point out several important limitations. There were interdependencies among the persuasive features. For instance, Security Points were incorporated in the Security Quiz, Challenges, Personalization, and Risk Communication. These interdependencies might have led to overlapping effects among the features. Additionally, the application of randomization in order to avoid order effects may have created somewhat unnatural sequencing, thus hampering a full understanding of a feature. For example, successful completion of a Challenge was rewarded with Security Points. However, due to random feature ordering, it was possible to encounter Challenges prior to being introduced to the concept of Security Points. At the same time, it is also likely that the potential errors of such peculiarities were canceled out owing to the random ordering. As explained in the Method section, Risk Communication was placed at the end, which may have introduced an order effect for this feature.

Our study examined a single usage instance using an interface prototype lacking back-end functionality. Moreover, study participants had no prior exposure to the prototype. A longitudinal study with a functioning system is needed to study how these findings are affected by usage experience and learning.

8 Conclusion

Our research goal was to investigate if a Behavior Change Support System with persuasive features could be a promising mechanism for raising employee awareness of an organization's information security policy and helping prevent work practices that violate the policy. To achieve this objective, we applied eight persuasive strategies to design and implement six persuasive features in an interactive prototype. A user evaluation of the features via an online study suggests that the features hold promise but their persuasive power could be enhanced by design refinements. A functioning deployment in a real-life setting is needed to study the longitudinal impact of the persuasive features. We hope these findings spur further exploration that investigates how additional persuasive strategies could be employed to develop persuasive system features.

9 Acknowledgements

This work was partially funded by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement 318508 (MUSES – Multiplatform Usable Endpoint Security).

References

1. Al-Omari, A., El-Gayar, O., Deokar, A., and Walters, J. Security Policy Compliance: User Acceptance Perspective. *45th Hawaii International Conference on System Sciences*, IEEE, (2012).
2. Busch, M., Wolkerstorfer, P., Hochleitner, C., Regal, G., and Tscheligi, M. Designing a Persuasive Application to Improve Organizational Information Security Policy Awareness, Attitudes and Behavior. Extended Abstract. *Symposium on Usable Privacy and Security*, (2014).
3. Chiasson, S., Stobert, E., Forget, A., Biddle, R., and Van Oorschot, P.C. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transactions on Dependable and Secure Computing,* 9, 2 (2012), 222–235.
4. Drozd, F., Lehto, T., and Oinas-Kukkonen, H. Exploring perceived persuasiveness of a behavior change support system: A structural model. *Persuasive Technolo*gy, (2012).
5. Forget, A., Chiasson, S., Oorschot, P.C. Van, and Biddle, R. Persuasion for stronger passwords. *Persuasive Technology*, (2008).
6. Gabrielli, S., Forbes, P., Jylhä, A., Wells, S., Sirén, M., Hemminki, S., Nurmi, P., Maimone, R., Masthoff, J., and Jacucci, G. Design challenges in motivating change for sustainable urban mobility. *Computers in Human Behavior*, 41, (2014), 416-423.
7. Gamberini, L., Spagnolli, A., Corradi, N., Jacucci, G., Tusa, G., Mikkola, T., Zamboni, L., and Hoggan, E. Tailoring feedback to users' actions in a persuasive game for household electricity conservation. *Persuasive Technology*, (2012), 100-111.
8. Kaptein, M.C. Personalized persuasion in ambient intelligence. *Journal of Ambient Intelligence and Smart Environments*, (2012), 43-56.
9. Lehto, T., Oinas-Kukkonen, H., and Drozd, F. Factors Affecting Perceived Persuasiveness of a Behavior Change Support System. *Thirty Third International Conference on Information Systems*, (2012).
10. Merhi, M. and Midha, V. The Impact of Training and Social Norms on Information Security Compliance: A Pilot Study. *Thirty Third International Conference on Information Systems*, (2012).
11. Munson, S.A. and Consolvo, S. Exploring goal-setting, rewards, self-monitoring, and sharing to motivate physical activity. *PervasiveHealth*, (2012).
12. Oinas-Kukkonen, H. and Harjumaa, M. A systematic framework for designing and evaluating persuasive systems. *Persuasive Technology*, (2008).
13. Oinas-Kukkonen, H. Behavior change support systems: A research model and agenda. *Persuasive Technology*, (2010).
14. Thomson, M.E. and Solms, R. von. Information security awareness: Educating your users effectively. *Information Management & Computer Security,* 6, 4, (1998), 167–173.
15. Uffen, J. and Breitner, M.H. Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions. *46th Hawaii International Conference on System Sciences*, IEEE, (2013).

16. Venkatesh, V. and Bala, H. Technology Acceptance Model 3 and a research agenda on interventions. *Decision Sciences,* 39, 2, (2008), 273–315.
17. Yeo, A., Rahim, M., and Ren, Y. Use of Persuasive technology to change end user's IT security aware behavior: A pilot study. *International Journal of Human and Social Sciences*, (2009), 673–679.
18. Zuckerman, O. and Gal-Oz, A. Deconstructing gamification: Evaluating the effectiveness of continuous measurement, virtual rewards, and social comparison for promoting physical activity. *Personal and Ubiquitous Computing*, 18, 7, (2014), 1705-1719.