Addressing Human Factors in the Design of Cyber Hygiene Self-Assessment Tools

Jacob Esparza[1], Nicholas Caporusso[2] and Angela Walters[1]

[1] Department of Informatics,
Fort Hays State University, 600 Park Street,
67601 Hays, United States
[2] Department of Computer Science,
Northern Kentucky University, Louie B Nunn Dr,
41099 Highland Heights, United States
jtesparza@mail.fhsu.edu, caporusson1@nku.edu

Abstract. As cybersecurity (CS) threats become more sophisticated and diversified, organizations are urged to constantly adopt and update measures for contrasting different types of attacks. Particularly, as novel techniques (e.g., social engineering and phishing) are aimed at leveraging individual users' vulnerabilities to attack and breach a larger system or an entire company, user awareness and behavior have become key factors in preventing adverse events, mitigating their damage, and responding appropriately. As a result, the concept of Cyber Hygiene (CH) is becoming increasingly relevant to address the risk associated to an individual's CS practices. Consequently, self-assessment tools are becoming more important for evaluating user's literacy, implementing measures (e.g., training), and studying the effectiveness of interventions. In this paper, we propose a framework for including human factors in the design of self-assessment tools and for accurately modeling CH aspects that the root cause in CS issues.

Keywords: Cybersecurity · Human Factors · Phishing · Social engineering · Risk assessment · Cyber Hygiene · Knowledge-Attitude-Behavior

1 Introduction

In the last decade, the widespread adoption of personal communication technology and connected devices changed the scenario of CS: despite the increasing effort of companies and governments to prevent breaches and protect critical business information and organization resources, novel types of CS threats (e.g., ransomware, phishing, and social media engineering) directly aimed at exploiting individuals pose new challenges for entire organizations [1]. In the recent years, most of the work focused on enforcing security of cyber-physical systems aimed at protecting the entire organization: unfortunately, this is not enough to prevent breaches caused by incorrect behavior of their employees and users. Several recent events demonstrated that traditional CS frameworks, including the development of guidelines especially designed to instruct users about their CS practices, are not enough to prevent attacks that directly target individuals via indirect methods (e.g., social engineering) and threats (e.g., phishing and ransomware) that leverage poor adherence to good security practices. Also, as detailed by research studies and incident reports, users are prone to making mistakes and to reiterating incorrect CS behavior, such as reusing the same password for several accounts and generating weak usernames and passphrases, which creates entry points for hackers and, consequently, weaken or void any security measures taken [2] [3]. Therefore, companies are increasingly diversifying CS strategies: awareness campaigns, required training, and informational events, which were demonstrated to lead to a better understanding of the risks and how to avoid them. As users and their practices are the last line of defense and, simultaneously, the first entry-point of the most dangerous attacks [4], the concept of CH, that is, user's CS behavior with specific regards to practices that can increase risk for others, is gaining interest among CS organizations [5] [6]. Particularly, self-assessment questionnaires can be utilized to identify items in which users lack knowledge or are prone to misbehavior and, consequently, design interventions aimed at increasing their awareness.

In this paper, based on previous literature, we introduce a new model that takes into consideration human factors to exactly identify the root cause of individuals' malpractices. By doing this, we aim at supporting the development of initiatives that specifically target the characteristics of the single user, and thus, could lead to better outcomes.

2 Related Work

In addition to protecting their systems, organizations have begun to address security concerns caused by individuals' weaknesses, by implementing training programs aimed at improving the awareness of their employees, with the objective of reinforcing their ability to recognize, avoid, and report threats. Although most studies in the literature have demonstrated the effectiveness of training initiatives in increasing individuals' CS literacy, the authors of [6] found that in several cases previous training does not result in any significant improvement in terms of adoption of more secure practices, unless the strategy, design, and delivery of courses are aligned with assessment policies that enforce correct CS conduct on a continuous basis. As discovered by [7], different factors might influence individual's behavior, which, in turn, makes it difficult to define a holistic framework for addressing the diverse aspects that contribute to neutralizing threats.

The concept of CH aims at introducing a new approach in CS that combines established practices from healthcare domain to refer to individual's CS posture [5] [6]. As experts are still shaping its scope, in this paper, we adopt the definition of [5], that describes CH as *the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet enabled devices from being compromised in a cyber-attack*. Both the definition and its explanation are especially effective in assimilating preventive approaches in CS to measures adopted in healthcare standards. Also, [5] proposed the Cyber-Hygiene Inventory (CHI), that is, a model that enables categorizing questions regarding several items of concern into standard risk dimensions, such as storage and device (S), authentication and credentials (A), Facebook and social media (F), e-mail and messaging (E), and transmission and browsing (T). In general, easy-to-adopt tools in the form of questionnaires and surveys are convenient and versatile instruments for assessing, screening, and monitoring individual's practices on a regular basis, eliciting potential risks, and addressing them with appropriate follow-up interventions. Unfortunately, they lack longevity and require continuous updates to cope with the constantly changing scenario of CS. Conversely, the top-down design of the CHI and its abstraction level render it more robust compared to other questionnaires and scales: the specific risk factors can be further customized to take into account new threats and to change the depth, scope, and content of questions based on the context of application. However, the current design of the CHI only tests subject's knowledge about CS without considering any human factors, such as, behavior, attitude, perception, other intrinsic and extrinsic aspects (e.g., gender, age, and facilitating conditions) that have been demonstrated to be crucial in implementing effective measures. Consequently, the questionnaire offers very limited insight on individual's general attitude with respect to CH as well as on their actions and situational responses in presence of a potential threat. For instance, as showed by previous research, despite knowing how to generate secure passwords and being aware of the risks of reusing the same username for multiple websites, individuals might decide to compromise their standard to a level that results in better convenience [2] [3] [4]. Similarly, the CHI does not support identifying the underlying factors impacting individual's intention to implement a correct behavior, despite of their general attitude to CS practices. As a result, two users assessed with a questionnaire designed using the current CHI model could very well obtain the same CH profile despite their actual actions might result in very different outcomes in terms of risk. For instance, users could adopt strict measures in regard to sharing information via social media, because they take their privacy into consideration for reasons that are not related to any potential implications in terms of CS. Moreover, the current CHI lacks aspects that support updating questionnaires and incorporate new questions aimed at measuring individuals' progress over time and analyze the impact of CS interventions on their CH posture.

3 Incorporating Human Factors in the Inventory

In this paper, we propose a novel framework for designing self-assessment tools in the context of CH. Specifically, our work aims at improving the inventory described in [5], so that human factors can be taken into consideration in the CHI in designing questions, administering assessment tools, and designing interventions. To this end, in addition to the risk contexts considered by [5], our work incorporates the Knowledge-Attitude-Behavior (KAB) model introduced by [8] to address risk in the healthcare domain, which was not included in the original version of the CHI. The KAB approach has been utilized in several CS frameworks and self-assessment scales in the context of CS, such as the Human Aspects of Information Security Questionnaire (HAIS-Q) [9].

3.1 The importance of Knowledge, Attitude, and Behavior

In our work we expand the KAB model to better fit the concept of CH: as shown in Fig. 1, we define *knowledge* as subject's level of training and awareness of the risk concerning specific aspects in the CS field, that is, technical competence (e.g., authentication and credentials) that is already taken into consideration in most questionnaires, including the CHI; we use *attitude* to refer to individual's general approach to CS based on their perceived level of severity and to recurring patterns in their habits; finally, we consider *behavior* any aspect related to their situational response, that is, the security score associated with actual actions realized by users in order to prevent or address threats in the dimensions considered by the CHI. By doing this, we separate CS concerns related to human factors into three specific domains and, thus, we make it possible to precisely identify the areas in the process that are more prone to potential flaws, so that they can be addressed with targeted intervention. As a result, an individual's CH profile can be obtained by evaluating the risk contexts in combination with human factors. This, in turn, facilitates designing CH inventories that better integrate within a workflow where an improved and more accurate assessment of an individual's CH score results in the prescription of CH interventions especially targeted at the root cause of the CS concern. Furthermore, categorizing risk dimensions into their atomic components is expected to enhance evaluating the effectiveness of CH interventions.

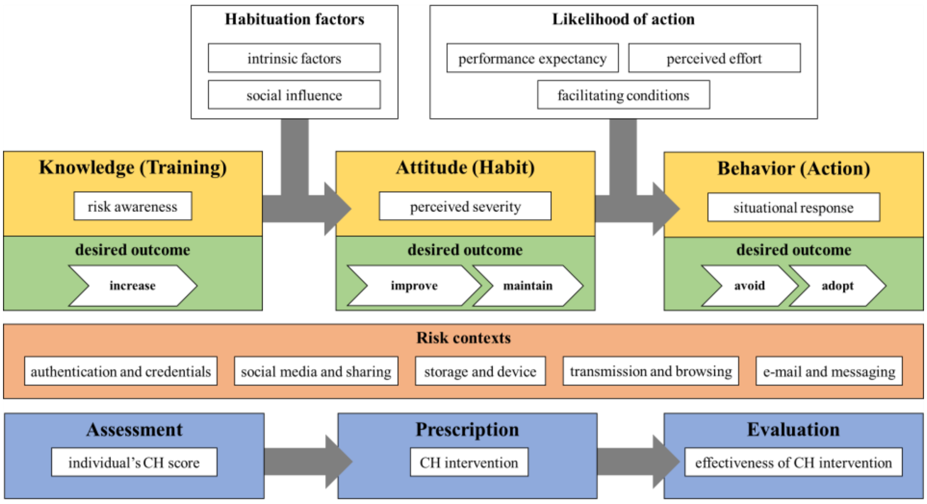

Fig. 1. An overview of our proposed framework. We incorporate the KAB model in the design of CH self-assessment tools to highlight the importance of accounting for human factors that have an impact on individuals' risk awareness, perception of the severity of threats, and on their situational response in different contexts. Also, our framework includes aspects that influence user's attitude and behavior and suggests specific dimensions that need to be considered when designing questionnaires and updating them by considering the desired outcome in terms of CH improvement in the user posture.

3.2 Desired CH outcomes

Moreover, in our framework we divide each component of the KAB model into specific actions that individuals are expected to realize depending on their current and desired level of CH. Particularly, we take into consideration if they are able to: (1) *increase* their knowledge and awareness, (2) *change* an incorrect attitude in terms of CS so that they can build and (2) *maintain* a high CH profile, and (3) *avoid* potentially dangerous actions and *adopt* strategies that are expected to result in a proactive and improved behavior with respect to detecting and reporting potential threats. As a result, in addition to providing insight on the root cause analysis of CH issues, our framework supports updating data collection instruments by designing questions that specifically evaluate users' growth over time in terms of their level of CH.

3.3 Human factors influencing Knowledge, Attitude, and Behavior

Indeed, surveys and questionnaires, such as the CHI, are designed with a two-fold purpose, that is, (1) screening individual's and identifying their CH posture to prevent risk associated with their CS behavior, and (2) measuring the effectiveness of CS interventions, such as training programs, which have the objective of enhancing individuals' knowledge, in order for an increased awareness habituates them to correctly align their perception of risk with its actual severity, so that they can adopt a correct behavior when realizing their tasks. Nevertheless, several intrinsic and extrinsic human factors play a crucial role in the KAB model and they have an impact in correctly translating CS knowledge (risk awareness) into a responsible attitude; also, they intervene in specific situations in which users are required to take appropriate actions. Therefore, our model takes into consideration *habituation factors*, that is, aspects that shape users' habits over time and impact their attitude; also, we suggest elements that modify individuals' *likelihood of action* in accordance with the expected CH behavior. The former includes background, beliefs, and prior experiences that can result in different attitudinal approaches towards CH. For instance, users who have experienced a breach in the past might show better CH habits, because the incident might result in an increased perception of the severity of CS threats. Also, social factors, such as practices adopted by user's groups (e.g., their milieu and organization) can influence the individuals' attitude and lead to the development of habits that can improve or be detrimental for their CH. For instance, limiting the maximum length of passwords in authentication forms might induce users to always produce shorter passphrases.

Furthermore, additional human factors intervene when users actually realize actions (e.g., opening an attachment, changing the privacy settings of their social media account, and creating a password): their behavior can be influenced by the perceived effort and the expected performance, which refer to the difficulty and to the benefits (in terms of CH) of adopting a secure behavior in accomplishing a task, respectively. Moreover, external factors can have an impact on users' actions: facilitating conditions refer to elements that make it easy for users to implement CS principles (e.g., tools for reporting spam and phishing emails), enforce their correct behavior (e.g., scheduled antivirus updates), and prevent potentially dangerous actions (e.g., requiring user's confirmation before opening a suspicious file). For instance, the trade-off between convenience and strength in password creation represents the relationship between performance expectancy and perceived effort; conversely, an example of facilitating conditions is the automatic password generation provided by certain browsers that proactively suggest and memorize secure passphrases without any overhead for the user.

In our model, we consider factors related to social influence as different from aspects pertaining to facilitating conditions: the former refers to practices that result in attitudinal changes (e.g., as users become familiar with password management systems, they develop the habit of using it for every passphrase), whereas the latter indicates adoption of policies or instruments that prevent users from adopting an incorrect behavior by making it more convenient to adopt secure measures (e.g., requiring users to change their passwords every three months or adopting two-factor authentication systems).

4 Conclusions and Future Work

As reports found that a large number of attacks leverage vulnerabilities at the individual user level and use them as entry points, organizations are increasingly adopting assessment tools that help them evaluate individual's awareness with respect to CS and implement interventions, such as training programs, aimed at addressing risk proactively by improving the CH profile of their users.

In this paper, we introduced a novel framework that takes into consideration relevant human factors that have an impact on individual's CH. By doing so, we aim at enhancing the design of self-assessment tools, so that organizations can create better questionnaires that achieve a more in-depth picture of the respondent and enable identifying the types of threats together with their root causes. To this end, we modeled the underlying behavioral aspects that influence user's motivation in perceiving and addressing CS risks properly. The advantage of our model is that, in addition to risk contexts, it suggests dimensions that have to be taken into consideration without detailing individual questions or specific implementation details, which makes it consistent with the strategy adopted by [5] for developing their CHI. This is to maintain a top-down approach that supports evaluating human aspects that are associated with habituation factors and with the likelihood of action separately from users' knowledge about risk items.

References

1. Caporusso, N., Chea, S. and Abukhaled, R., 2018, July. A game-theoretical model of ransomware. In International Conference on Applied Human Factors and Ergonomics (pp. 69-78). Springer, Cham.
2. Stainbrook, M. and Caporusso, N., 2018, July. Convenience or strength? Aiding optimal strategies in password generation. In International Conference on Applied Human Factors and Ergonomics (pp. 23-32). Springer, Cham.
3. Stainbrook, M. and Caporusso, N., 2019, July. Comparative Evaluation of Security and Convenience Trade-Offs in Password Generation Aiding Systems. In International Conference on Applied Human Factors and Ergonomics (pp. 87-96). Springer, Cham.
4. Fandakly, T. and Caporusso, N., 2019, July. Beyond passwords: enforcing username security as the first line of defense. In International Conference on Applied Human Factors and Ergonomics (pp. 48-58). Springer, Cham.
5. Vishwanath, A., Neo, L.S., Goh, P., Lee, S., Khader, M., Ong, G. and Chin, J., 2020. Cyber hygiene: The concept, its measure, and its initial tests. Decision Sup-port Systems, 128.
6. Cain, A.A., Edwards, M.E. and Still, J.D., 2018. An exploratory study of cyber hygiene behaviors and knowledge. Journal of information security and applications, 42, pp.36-45.
7. Neigel, A.R., Claypoole, V.L., Waldfogle, G.E., Acharya, S. and Hancock, G.M., 2020. Holistic Cyber Hygiene Education: Accounting for the Human Factors. Computers & Security.
8. Bettinghaus, E.P., 1986. Health promotion and the knowledge-attitude-behavior continuum. Preventive medicine, 15(5), pp.475-491.
9. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T., 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security, 66, pp.40-51.