Self-Efficacy-Based Game Design To Encourage Security Behavior Online

Tianying Chen
Carnegie Mellon University
Pittsburgh, PA, USA
tianyinc@andrew.cmu.edu

Jessica Hammer
Carnegie Mellon University
Pittsburgh, PA, USA
hammerj@andrew.cmu.edu

Laura Dabbish
Carnegie Mellon University
Pittsburgh, PA, USA
dabbish@cs.cmu.edu

ABSTRACT

Eliciting cybersecurity behavior change in users has been a difficult task. Although most users have concerns about their safety online, few take precautions. Transformational games offer a promising avenue for cybersecurity behavior change. To date, however, studies typically focus on entertainment value instead of investigating the effectiveness and design potential of games in cybersecurity. As a first step to filling this gap, we present the design of Hacked Time, a desktop game that aims to encourage cybersecurity behavior change by translating self-efficacy theory into the game's design. As cybersecurity games are a relatively novel area, our design aims to serve as a prototype for mapping specific behavior change principles relevant to this area onto game design practice.

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5971-9/19/05
https://doi.org/10.1145/3290607.3312935

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; • **Human-centered computing** → *HCI theory, concepts and models.*

KEYWORDS

Cybersecurity; games; game design; self-efficacy.

ACM Reference Format:

Tianying Chen, Jessica Hammer, and Laura Dabbish. 2019. Self-Efficacy-Based Game Design To Encourage Security Behavior Online. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI'19 Extended Abstracts), May 4–9, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3290607.3312935

INTRODUCTION

The rapid development of online spaces has been accompanied by an alarming increase in cybercrime. Despite the fact that a majority of the general public shows great concern about their security online, people do not actively take precautions to protect themselves [9]. Therefore, inducing security behavioral change in the general public is instrumental in promoting a safer online space for everyone. Recently, researchers have been experimenting with using games to promote cybersecurity behavior change. These games show great promise, but studies of their effectiveness often report only participant enjoyment instead of measurable learning goals or behavior change outcomes [1, 8]. There is also a lack of cause-and-effect connection between theory and design choices. In this paper, we present the design of Hacked Time, a desktop game that aims to encourage cybersecurity behavior change by applying design principles derived from self-efficacy theory. As a first step to address the research gap, this paper contributes to the literature on theoretically informed game design approach by introducing a set of practices for mapping specific behavior change principles onto game design decisions. We also discuss future plans to investigate the effectiveness and measurable outcomes from our design.

BACKGROUND

Cybersecurity behavior change and games

While it is hard to make people change their security behavior online, several existing works show that under certain circumstances, such as social influences, trust, and cost efficiency, people are motivated to take security advice, and even more, change their behavior. Fagan et al. [7] and Redmiles et al. [11] pointed out that people accept security advice when they feel the advice makes sense to them, or when it is from a trusted security source. They reject advice when the behavior is costly or inconvenient, e.g. going through the various steps required to use two-factor authentication (2FA) [7, 11]. Das et al. [5] finds social influences to be a strong motivating factor for behavior change. A

majority of recent security behavior changes in their study were prompted by social influences, for example, after hearing about someone's negative experience, or having been pranked by a friend [5].

Researchers have explored the effectiveness of different types of interventions for increasing cybersecurity awareness. Recent approaches for cybersecurity awareness and behavior change include delivering just-in-time notifications using browser plug-ins [6], and raising awareness using games [1, 8]. Some commonly used formats for these games include but are not limited to role-playing, puzzle, interactive narratives, and attack-and-defend games [1, 8]. Although these approaches provide inspiration on designing games for cybersecurity, we still lack concrete evidence-based guidelines about how to design these games effectively. The games themselves are exploratory, largely testing the general concept of games as an education vehicle. Studies of the effectiveness of these games have focused primarily on the entertainment or engagement value of the games (e.g. how much participants enjoyed the game), instead of gauging what they learned or measure predictors of behavior change [1, 8]. This means we do not know what aspects of the game contribute to security behavior change or what game design approaches are more effective than others. In this work, we begin to draw an explicit connection between theories of behavior change and how such theories can manifest in-game.

Self-efficacy theory

Self-efficacy refers to one's belief in their own ability to accomplish a certain goal [3]. Self-efficacy has, since its creation, been thoroughly studied and implemented in a variety of settings. Bandura [3] outlined design strategies for a self-directed health program to be successful, inspired by his previous publication on self-efficacy. The design strategies involve four components: information that increases knowledge of health risk (risk information); skill development to translate concerns into preventative actions (skill development); guided practice for skill enhancement and to apply these skills in the high-risk situations (skill enhancement and application); and enlisting social support for desired changes (social support). These strategies serve as a practical guide for how to employ self-efficacy principles in practice. More recently, Yin et al.[13] and Backlund et al. [2] have shown positive results from game design practices guided by self-efficacy literature.

Transformational game design

Compared to traditional games, transformational games (sometimes referred to as "serious games") are designed to invoke behavior change in players that persists beyond the game [4]. Designing games that achieve their transformational goals, while still succeeding *as games*, is a challenging process [12]. Existing design frameworks for creating transformational games emphasize the need for games to build on validated bodies of research. For example, the Tandem Transformational Game Design Process transforms concepts from the research literature into goals and constraints for design [12], while Kaufman et al.[10]'s work on embedded design shows how research on psychological influence can inform a specific design philosophy.

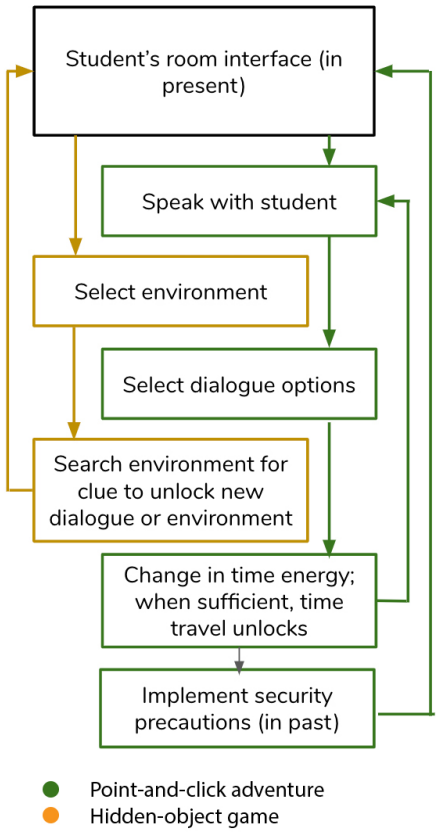

Figure 1: Game flow.

Figure 2: Player receiving information on security risks.

DESIGN

Hacked Time was designed at Carnegie Mellon University by an interdisciplinary team. The team brainstormed ideas for an engaging gameplay narrative, then presented the ideas to peer lab members for feedback and evaluation. Design principles for self-efficacy were extracted for a literature review and were used to guide game design decisions during the iterative process. Low-fidelity prototypes were used to explore the effect of these design decisions on player experience and on gameplay.

Game overview

Hacked Time combines elements of interactive novels and hidden object games with time-travel. In interactive novels, the player converses with computer-controlled characters, selecting dialogue and other choices to advance through a branching narrative. For example, in Hacked Time, the player takes the role of a detective, helping a college student deal with a security breach (Figure 2). The player can speak with the student to learn more about their situation, and select dialogue options to give them advice about what they should do. In hidden object games, players inspect a visual environment for meaningful objects. In Hacked Time the player must inspect the student's environment to identify clues related to the security breach (Figure 3). Player can click on the clues to gain helpful information to discover the cause of the breach (Figure 4). Finally, players acquire "time energy" through their dialogue options (Figure 5). The more helpful their answer, the more energy is acquired. When the player acquires enough time energy, they can travel back in time to before the security breach occurred. They can choose what security precautions to help the student practice and implement and then return to the game's "present" to see the impact of their actions on the student's situation (Figure 6).

Information on risk factors

The first design principle outlined by Bandura [3] is an information component that discloses the potential consequences resulting from a high-risk behavior. In a digital security context, this information is often acquired through reports of negative experiences from family and friends [5, 11]. To make this information acquisition process more natural and convincing, we designed the game to start with an anecdotal story of a friend messaging the player about a security breach they experienced, and the consequences that followed (Figure 2). The game narrative is structured around helping the friend with their problems. This narrative structure makes the game easier to relate to and briefs the player on the potential consequences of security breaches.

Development of skills

Time energy, which is needed for time travel, is given only to the most altruistic would-be time travelers. Players can therefore obtain time energy from being as helpful as possible to the student in improving their security choices (Figure 5). The player must analyze the situation using clues that are situated in the student's environment. The player then learns about all the security options and

Figure 3: Player can search through the student's room for clues.

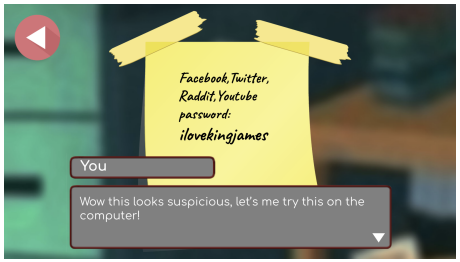

Figure 4: Successfully finding the cue.

Figure 5: Player gets time energy when giving solutions to the student.

their applications, and are asked to choose the *most effective* response. In this case, the student's security problems stems from three factors: writing down the password, using a weak password, and sharing password across accounts. While some security options are more effective, all options are an improvement over the student's current choice: password manager creates and manages unique strong passwords for different online accounts, which would be the most secure; even though 2FA and strong password each solves one aspect of the problem, they improve on the student's current practice. This approach tries to imitate real life situations in which no answer is "correct", but are relatively more or less effective depending on context. The amount of time energy acquired reflects the relative value of the choice. Bandura [3] suggests that development of skills come from modeling: people judge their own capabilities based on how well those whom they regard as similar to themselves perform. In this case, by offering solutions to the student, the player can gain insights on the effectiveness of the security behavior based on its effect on someone similar to their situation.

Skill enhancement and application

This approach aims to provide the players with guided skill enhancement by helping them through the steps that are required to set up a security protection option. By sending the players to the past to correct the student's behaviors, we aim to guide the player through a high-risk situation and show them how their security skills can avert negative consequences. In the past, the player is asked to protect the student's account in the way that is most suitable to them. Moreover, the player is asked to go through the actual process of applying a certain protection mechanism, such as setting up 2FA for Facebook (Figure 6). The player can also choose to implement other security options if they want to heighten their security level even more and/or to practice other methods of protection. By showing the player the actual process of implementing a security mechanism such as 2FA we aim to alter their belief that such processes are convoluted and technologically demanding. At the end of the skill application, we also show the positive outcome of their actions with a happy ending: the friend never got their account hacked and their important information is still safe.

IMPLICATIONS AND FUTURE WORK

Using an iterative design process, we have instantiated Bandura's design principles for increasing self-efficacy in a game. We hypothesize that the skill set and knowledge that players obtain from the game should reduce player's perception that security precautions are unnecessary or difficult to achieve and thus increase their self-efficacy. To evaluate this hypothesis, we plan to conduct a mixed-method study of game effectiveness. First, we will investigate how well each of the game design decisions described above instantiate Bandura's principles using playtests and interviews. We will ask questions such as "Can you describe a scenario in which you could see yourself using one of the security options you used in game?" in order to understand player's take-aways from the game and their skill development. After iterating on the game based on our findings, we will use a

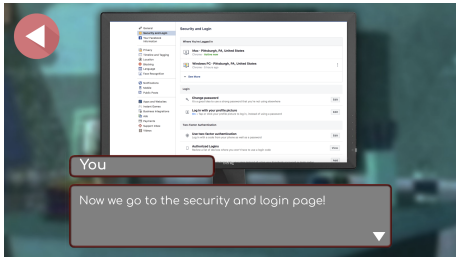

Figure 6: Player are guided through the implementation process of 2FA on Facebook.

randomized controlled study to compare this game to other cybersecurity education methods such as informational fliers and educational videos. Our results will demonstrate whether the extra resources required for game development are justified when compared with more traditional approaches to behavior change. Finally, we will investigate the role of social support as outlined by Bandura in his four design principles [3]. However, it differs from the other three principles in a way that it is an element about external human interaction instead of internal factor. We will conduct a third study comparing outcomes from players collaborating in pairs compared to players who interact with the game alone. In summary, our study was motivated to address the need for a theory-driven design approach to cybersecurity games. If our hypotheses are borne out, it will provide a good model for how to design theory-driven behavior change games in cybersecurity.

REFERENCES

[1] Faisal Alotaibi, Steven Furnell, Ingo Stengel, and Maria Papadaki. 2016. A Review of Using Gaming Technology for Cyber-Security Awareness. *International Journal for Information Security Research (IJISR)* 6, 2 (2016), 660–666.

[2] Per Backlund, Henrik Engström, Mikael Johannesson, Mikael Lebram, and Björn Sjödén. 2008. Designing for self-efficacy in a game based simulator: An experimental study and its implications for serious games design. In *Visualisation, 2008 international conference*. IEEE, 106–113.

[3] Albert Bandura. 1990. Perceived self-efficacy in the exercise of control over AIDS infection. *Evaluation and program planning* 13, 1 (1990), 9–17.

[4] Sabrina Culyba. 2018. The Transformational Framework: A Process Tool for the Development of Transformational Games. (9 2018). https://doi.org/10.1184/R1/7130594.v1

[5] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *Proc. SOUPS*, Vol. 14.

[6] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. 2014. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. ACM, 739–749.

[7] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 59–75.

[8] Maurice Hendrix, Ali Al-Sherbaz, and Bloom Victoria. 2016. Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games* 3, 1 (2016), 53–61.

[9] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy attitudes of Mechanical Turk workers and the US public. In *Symposium on Usable Privacy and Security (SOUPS)*, Vol. 4. 1.

[10] Geoff Kaufman and Mary Flanagan. 2015. A psychologically "embedded" approach to designing games for prosocial causes. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 9, 3 (2015).

[11] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 666–677.

[12] Alexandra To, Elaine Fath, Eda Zhang, Safinah Ali, Catherine Kildunne, Anny Fan, Jessica Hammer, and Geoff Kaufman. [n. d.]. Tandem Transformational Game Design: A Game Design Process Case Study.

[13] Langxuan Yin, Lazlo Ring, and Timothy Bickmore. 2012. Using an interactive visual novel to promote patient empowerment through engagement. In *Proceedings of the International Conference on the Foundations of Digital Games*. ACM, 41–48.