Hacked Time: Design and Evaluation of a Self-Efficacy Based Cybersecurity Game

Tianying Chen
Carnegie Mellon University
tianyinc@andrew.cmu.edu

Margot Stewart
Carnegie Mellon University
erstewar@andrew.cmu.edu

Zhiyu Bai
Carnegie Mellon University
zoebai@cmu.edu

Eileen Chen
Carnegie Mellon University
ezchen@andrew.cmu.edu

Laura Dabbish
Carnegie Mellon University
dabbish@cs.cmu.edu

Jessica Hammer
Carnegie Mellon University
hammerj@andrew.cmu.edu

ABSTRACT
A major reason why people don't use security tools online is that they perceive them as difficult and challenging, resulting in the lack of self-efficacy. Previous research has looked at improving user security attitude and practices through a variety of interventions, including transformational games. These games, targeted at improving security attitude and promoting change through gameplay, offer a new perspective on cybersecurity education. In this research we present the design and evaluation of *Hacked Time*, a desktop game that uses an integrative approach that incorporates Bandura's self-efficacy design framework to improve player self-efficacy. Using a randomized control trial (n=178), we demonstrate that our game is effective in improving player's security attitude and self-efficacy for using cybersecurity tools. We discuss how our design pattern can serve as an exemplar to enhance player self-efficacy in other fields.

CCS Concepts
•**Security and privacy** → **Social aspects of security and privacy;** •**Applied computing** → *Computer games;*

Author Keywords
Cybersecurity; games; game design; self-efficacy.

INTRODUCTION
Cyber-crimes are on the rise. In 2018 alone, it is reported that about 12 billion personal data records were stolen, and by 2018 nearly 60 million Americans experienced identity theft [43]. In spite of this imminent threat, however, most people do not take precautions to protect themselves online [31]. A recurring theme in this inaction is the misunderstanding of security tools and an inaccurate perception of the cost versus benefit of these tools [26, 52], resulting in the lack of self-efficacy in users. Recent research has attempted to educate people and improve attitude about cybersecurity through games [1, 25]. While these games are reported to be enjoyable, we do not know whether or how they affect players' attitude or self-efficacy related to cybersecurity [1, 25]. Moreover, game interventions in cybersecurity seldom draw and evaluate cause-and-effect connections between theory, design practice, and outcome. At the same time, transformational games in cybersecurity tend to influence players through micro-lenses, affecting one sub-construct of a framework at a time, instead of employing a more holistic approach. For instance, [8] designed separate mini-games to target individual constructs of self-efficacy in addressing cybersecurity through self-efficacy based transformational games. Even though this approach enables designers to understand the effect of individual elements, a successful intervention program should aim to affect users in a comprehensive manner to make a meaningful impact [7].

To address the aforementioned gaps in cybersecurity game research, we present the design and evaluation of *Hacked Time* [11], a desktop game that embeds Bandura's self-efficacy design framework [7] in its design to improve player's security attitude and cybersecurity self-efficacy: a person's belief in their capacity to accomplish a certain goal [6]. In this work we map self-efficacy principles onto game design decisions, demonstrating the effective use of theory-informed game design practice. With these design practices we collectively address elements of risk awareness, skill development, and guided practice proposed by the design framework from [7]. Building on previous literature, our method integrates a range of design decisions guided by [7] to influence player self-efficacy in a holistic way.

In a quantitative evaluation, we examine whether we successfully incorporated theory-driven design principles into our game and increase player self-efficacy, frequently framed as the first step in behavior change [7, 48]. We conducted an experiment with 178 MTurk comparing the effectiveness of our game against providing security information in a non-game format or providing no security information (a control group). We found that playing *Hacked Time* significantly increased self-efficacy and security attitude post-intervention compared with non-game controls. This paper contributes to the field of human-computer interaction, and the cybersecurity game

DIS '20, July 6–10, 2020, Eindhoven, Netherlands.

ACM ISBN 978-1-4503-6974-9/20/07 ...$15.00.
http://dx.doi.org/10.1145/3357236.3395522

research literature in particular, by demonstrating an effective integrative approach to designing with self-efficacy theory. Additionally, we provide design patterns that can be extended to game creation in other fields where increased self-efficacy is desired.

BACKGROUND

User security behavior

Data has shown that users are not particularly good at protecting themselves online: As of 2017, only 12% of online users in the US use password management software, one of the protection methods most recommended by experts [39, 26]. There are many reasons why this is the case. For one, they do not recognize the importance of the issue: people often do not perceive themselves as vulnerable to online threats; they underestimate the benefit while overestimating the cost of protection methods [52]. On the other hand, attempts to convey the seriousness of cybersecurity threats can backfire. When users perceive security threats to be over-sensationalized, they also become unconvincing [23].

Another challenge to secure online behavior is that users lack knowledge of what they can do to protect themselves. Even when users believe they have information on how to appropriately protect themselves online, it is often misguided. Ion et al. [26] demonstrated a severe mismatch between general population beliefs about the most important cybersecurity protection methods versus security expert recommendations. Security experts recommend updating systems, using a password manager, and enabling two-factor authentication (2FA) as the most effective protection methods, while users believe using antivirus software and strong passwords to be the most effective. Finally, even when users know what to do, they do not always follow through. For example, people tend to reject security advice when it is inefficient or inconvenient, such as going through the process of 2FA [20, 38]. In addition, people often assume that they are not able to obtain and effectively use information on online protection [52].

A key theme across these challenges is self-efficacy. As described more fully below, self-efficacy theory refers to a person's belief that they are able to accomplish their goals. When users do not know what to do to protect themselves, they cannot set appropriate goals. When they believe that protecting themselves is impossible, they lack belief in their ability to accomplish those goals. These are core self-efficacy problems [52]. For cybersecurity-related behaviors, self-efficacy has been shown to be a strong predictor for behavior change: for example, self-efficacy specific to internet usage and online protection predicts people's actual adoption of online protection methods [40, 49]. The impact of self-efficacy has also been explored together with response efficacy (person's beliefs as to whether the recommended action step will actually avoid the threat) from the Protection Motivation Theory (PMT) framework [41]. A study by Zhang et al.[58] demonstrated that both self-efficacy and response efficacy not only predict whether users adopt security behaviors but also contribute to the perception of the ease of use of technology, with self-efficacy more strongly predicting perceived ease of use which in turn relates to perceived usefulness of the intervention. Therefore, affecting self-efficacy can also lower the mental barrier that users encounter when presented with security information.

Security behavior change interventions

Existing cybersecurity behavior change interventions use a range of theories to drive design. For example as mentioned in the previous section, PMT is a theoretical framework used to promote behavior change in cybersecurity. PMT includes understanding threat severity and the individual's vulnerability, as well as appraising the cost and efficacy of the coping mechanisms for the threat [41]. Researchers have used concepts in PMT to successfully understand and predict user's security behaviors online, as well as to elicit behavior change by targeting these concepts [54, 46]. Another approach is to use "nudging," a concept from behavioral economics that leverages systematic biases in decision making to elicit behavior change [50]. Previous studies have demonstrated that nudging can create effective interventions by framing the messages and visualizing privacy indicators to encourage users to stay away from privacy-invasive mobile applications [10]. As an expansion on the idea of "nudging" users into certain behavior, the MINDSPACE approach specifies a set of nine common methods that can be used to encourage behavior change in cybersecurity [19].

Researchers have also applied theory from social psychology, successfully implementing the concept of social proof in notification design in order to increase adoption of a security technique within a social media platform [17]. Das et al. identified a set of social triggers for security behavior adoption, such as having heard about someone's negative security experience or having been pranked by a friend [16]. According to Fagan et al. [20] and Redmiles et al. [38], people tend to accept security advice when they feel that it is logical or the source of the advice is trustworthy.

These theories have been instantiated in a range of interventions. These interventions include traditional cybersecurity training and awareness campaigns [5], and more novel approaches such as using browser plug-ins to deliver just-in-time notifications [30], using visible social influence tactics to motivate users [17]. However, the majority of these approaches less adequately address two important issues: the users' perception that cybersecurity a dull subject [23], as well as the recurrent theme of lack of self-efficacy stemming from user's perception of the difficulty of tool usage. To address the two issues, we first discuss research on transformational games for cybersecurity attitude and change. Then we discuss how we can use Bandura's design framework to support user's self-efficacy.

Transformational games for cybersecurity

Transformational games focus not just on the gaming experience, but on eliciting behavior change in players that persists beyond the game itself [14]. Designing games to succeed as games (i.e. to be fun and engaging) while striving to accomplish their transformational goals (i.e. behavior change) is a difficult process [53]. Current transformational game design frameworks highlight the importance of building games based on validated research [14]. Transformational games

have multifaceted impacts on the player, including on their perception, cognition, behavior, mood, and motivation: the most frequently studied and reported outcomes include knowledge acquisition as well as affective and motivational outcomes [13]. Although game development requires a different set of skills and resources from traditional instructional methods, research demonstrates that under the right circumstances, transformational games can be more effective for knowledge acquisition and information retention when compared to traditional instruction [56].

Transformational games in cybersecurity are gaining more and more research attention. The games designed include genres such as role-playing, puzzle, interactive narrative, and tower defense games [1, 25]. However, cybersecurity game interventions in the literature are frequently designed based on *learning* theories, which provide players with necessary knowledge; few go further to incorporate theories of behavior change that encourage players to act upon this knowledge and protect themselves [1, 25, 45]. Furthermore, existing work rarely draws explicit connections between theory and design decisions, making it difficult to derive generalizable principles or comprehensive best practices [1, 25]. Finally, evaluations of these games focus on enjoyment rather than learning outcomes or predictors of behavior change [1, 25]. Even though player enjoyment is essential to games, especially since cybersecurity is often perceived as a dull subject [23], enjoyment alone does not predict learning [28], nor is it a direct assessment of whether players change their behavior. Therefore, to provide convincing evidence that serious games in cybersecurity research are effective for motivating change, it requires assessing not only enjoyment value, but evidence for change or for antecedents of change. Our work seeks to address this gap by applying and assessing the effect of a behavior change theory, specifically self-efficacy theory, on cybersecurity game design.

Designing with self-efficacy theory

Self-efficacy refers to people's belief in their own ability to accomplish a certain task or goal [6]. In a meta-review of 34 studies of health behavior change, Joseph et al. [29] found that Bandura's was the most widely studied and implemented behavior change theory in healthcare, and that interventions built on this theory showed behavior change over the longest term compared to those built on other theories. Bandura in [6] outlined four dimensions of self-efficacy: performance accomplishments, vicarious experience, verbal persuasion, and physiological states. Later, drawing on his previous work, Bandura in [7] presented a framework that defined four specific principles of healthcare program design to encourage behavior change: (1) information that increases knowledge of health risk (risk information); (2) skill development to translate concerns into preventative actions (skill development); (3) guided practice for skill enhancement and application of these skills in high-risk situations (guided practice and skill enhancement); and (4) enlistment of social support for desired changes (social support). Compared to the four dimensions initially proposed, these principles are directly actionable, while still building on the original four dimensions. We believe that they provide an integrative approach to behavior change and is appropriate to adapt into the digital game design space.

Self-efficacy theory has started receiving attention in transformational game design and research practice. Research in self-efficacy and transformational games have produced positive preliminary evidence [4, 57]. However, more specifically in cybersecurity, there are fewer examples of transformational games designed with self-efficacy principles. Those that do exist have not been validated and focus on individual components of self-efficacy rather than presenting an integrative approach. Baral and Arachchilage outlined specific ways of designing for self-efficacy by affecting individual dimensions of self-efficacy with separate games [8]. However, they did not validate their design recommendations with quantitative evidence that the game interventions actually affected self-efficacy. In addition their approach focuses on how to influence individual components of self-efficacy, by using mini games to change individual constructs one at a time, instead of taking an integrative approach treating the game as a unifying component, as Bandura proposed in his sefl-efficacy design framework [7].

In this research we address the limitations of prior studies in this area; previous work on self-efficacy and cybersecurity often applied self-efficacy theory as an explanation, instead of experimentally manipulating self-efficacy and assessing the outcome of the intervention quantitatively. We lack validated guidelines for designing games with self-efficacy principles that influence a user's actual cybersecurity self-efficacy. In the next section we present the design of *Hacked Time* and our method of integrating separate elements of self-efficacy using Bandura's design framework into a unifying game body for a coherent transformational experience.

DESIGN AND PLAYTESTING

We believe that self-efficacy theory can not only be used as a tool to understand and predict behavior, but also more importantly, serve as a convincing theoretical background for designing cybersecurity interventions. Because existing cybersecurity game interventions do not adopt this approach, we began our research by designing *Hacked Time*, a transfor-

Figure 1. Escape room - finding clues.

Self-efficacy Principle	Design Implementation	Design Details
Informaiton of risk factors	Empathy building	We introduced character customization to enocurage empathy building
	Friend narrative	The player interacts with a "friend" in game to make the risks more observable and relatable
Skill development	Hidden object / escape room	Allows players to interact with the environment and diagnose which behaviors put security at risk
	Smart watch consultant	Smart watch provides players with security information and what to do to protect themselves
	Time energy questions	Allows players to reflect on their security knowledge and proper diagnose how they can implement what they learned
Guided practice	Mock implementation of tool	Allows players to actually go through the implementation experience and practice the skills they learned with guidance

Figure 2. Summary of Bandura's self-efficacy design framework [7] and corresponding design implementations.

mational game designed to promote improved cybersecurity practices by increasing player self-efficacy.

Game overview

In *Hacked Time*, the player is a time-traveling detective who helps a college student deal with a security breach. These fictional choices align with the game's goals. Detectives learn by making sense of clues, just as we hope players will look for clues to discover real-life security threats. The time-travel element allows us to show an observable and causal impact of effectively using security tools. In their detective role, the player alternates between two key activities: talking to the student as they might in an interactive novel, and exploring their space as they might in a hidden object game. When players speak with the student, they can learn more about what happened from the student's perspective, teach the student about cybersecurity, and give them advice. To advance the game, the player selects from among available dialogue choices. When players explore the space, they can learn more about how the security breach actually occurred, regardless of the student's personal perspective. Players can click on certain objects and gain insight on their relevance to the student's security problem (Figure 1).

At the beginning of the game, the player is given several options for both their own appearance and that of a "friend" in-game who they are tasked with helping. Directly after this initiation, the game also introduces the player's time-traveling smart watch, which offers in-game help as well as supplementary dialogue on cybersecurity concepts. Finally, players are directed to the main part of the game which combines interactive novel and hidden object game techniques with time travel. The player has a dialogue with the student to find out about what happened and has the opportunity to select dialogue options that help the student resolve their issue. In *Hacked Time*, the player also inspects the student's bedroom to see if anything in the room could give insight about how the security breach occurred.

During the main phase of the game, the player collects "time energy" by helping the student solve their security problems (Figure 4). Once the player has enough time energy, the game enters its ending phase when the detective travels back in time to before the security breach occurred. The player can choose what preventative security measures the student can take, help the student implement those measures, and then return to the game's present to see the effect of their actions on the student's situation. In the end, the players are presented with the time energy they earned for their actions.

Transformational games provide a platform for us to offer players enactive attainment at low risk as the experience of learning by doing in real life might be scarce, or too risky for players to experiment. By designing these activities with the interactivity that games can offer, we link together Bandura's concepts of *enactive attainment* (experiencing mastery) and *vicarious experience* (experiencing through another, e.g. a character) [6].

Iterative design process

Hacked Time was created by an interdisciplinary team at Carnegie Mellon University. The team consisted of five people with backgrounds in psychology, HCI, computer science, and game design. The team also included a faculty advisor who is an security expert. The design, development, and iteration process lasted 8 months. The team implemented Bandura's design framework for self-efficacy outlined in [7], and used them to shape the game design throughout the iterative process. A summary of specific principles and the corresponding design decisions is presented in Figure 2. Based on these principles, members brainstormed preliminary game ideas and received expert feedback [53, 14]. Once the team agreed on an approach, we created both low-fidelity and high-fidelity prototypes for playtesting [12, 22]. Low-fidelity prototypes were created in a range of mediums, from paper to interactive Powerpoint. High-fidelity prototypes were created in Unity. Based on our playtest results, we identified additional areas for iteration and made improvements accordingly. The game

went through a total of three iterations prior to the evaluative study described later in this paper.

We conducted internal playtesting with colleagues with expertise in cybersecurity, both to evaluate the playability of the game and to improve our implementation of the design principles. We collated their feedback, discussed with the team, and iterated the game based on player suggestions. For example, at this stage we added character customization and generalized the process for implementing security tools. Next, we moved to external playtesting with students from our university, to help us understand whether the game's manifestation of the design principles was being understood by players. Playtesters were asked to play *Hacked Time*, and for each participant one observer took notes on their interaction with the game. After playing the game, participants were asked to respond to a written questionnaire about their experience. In the sections below, we report the design process and key insights from the external playtests that supported the iterative design process.

Risk information

Bandura's first principle in his design framework discusses the necessity of revealing the potential consequences that result from high-risk behavior [7]. This component emphasizes the importance of knowledge and awareness. In the context of online security, people often receive this information from family members and friends [38, 16]. It is also a common trigger for people to start taking security precautions through social influences [16]. Therefore, we emphasized the importance of empathy and relatability in our game, opening the game with an interaction between the player and a friend (the "student" referenced above). The player's friend tells a story of being hacked and the consequences that followed. This corresponds with research showing hearing about friends or family members' negative security experiences can lead to increased protective behaviors, and replicates a more natural and convincing information acquisition process [38, 16].

After addressing the player's awareness and knowledge of a cybersecurity threat they could encounter in their daily life, throughout the game we provide them with factual information about the nature of password leaks, potential causes of information breach, consequences that follow, actionable suggestions on how to protect their online information, and hands-on experience with protective tools. From finding clues to providing helpful suggestions to the student, the player walks through a proactive and reflective process from problem-finding to problem-solving. By communicating risk information to the players through dialogue, we also try to address the barrier of the perceived dullness of cybersecurity, and to lower the potential aversion that player could develop with dry and straight-to-the-point security warnings [23].

Playtest insights

From our preliminary testing, we found that in order to effectively communicate risk, as well as to make the player feel risk is imminent and relatable, the player needs to be able to empathize with the in-game characters. Earlier iterations of the game failed in this aspect: players reported that they skimmed through the opening text because there was not much interaction with the in-game character and nothing that they cared about. On top of that, most players indicated that the in-game characters did not look like them, which also made it hard for them to relate to the characters. In order to address this issue, we worked with a professional game narrative writer to improve the dialogue quality, and gave players more customization options for the playable characters. (Figure 3).

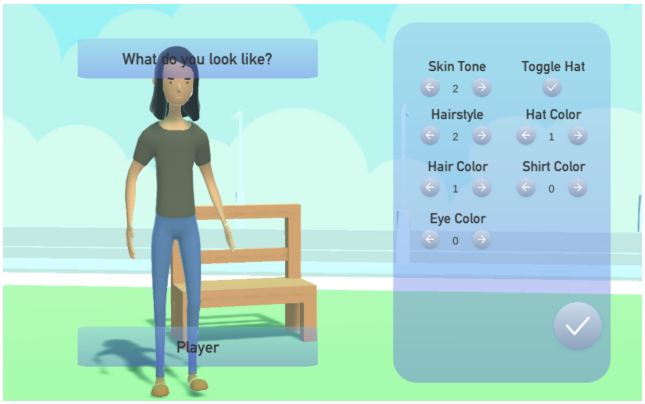

Figure 3. Character customization process.

To understand the impact of the risk information design, we looked for signs that players were able to relate to potential risks. In our external playtests, we found that our game elicited strong feelings about the consequences of the breach. Players could also think of the "worst cases possible" associated with risky behaviors, for instance, one participant said "my nudes could leak." Moreover, social consequences seemed to motivate our participants to engage with the topic of cybersecurity and helped them relate the in-game experience to potential real-life risks.

Skill development

To encourage skill development, we employed several game mechanics that allowed players to identify security concerns and translate them into preventative actions: a puzzle system, a teaching agent, and a teachable agent where players must offer appropriate suggestions to the student who they are helping. The puzzle system requires players to carefully observe their environment in order to discover potential risks in the student's situation. The player first explore the student's room to find possible clues by investigating every day objects, such as the student's backpack, desk drawer, and computer. The computer in this case needs to be unlocked by a password. The player can find the password in the student's drawer written on a sticky note. After finding the sticky note, the computer unlocks and allows the player to get into the student's various social media sites. We embedded three security concerns into the gameplay: the student used a weak password, shared the password across different accounts, and stored the password in an unsafe place 1. After discovering the password and seeing that it works on all of the student's social media accounts, the player informs the student about ways they can protect themselves (a strong password, two-factor authentication, and a password manager). The student is then offered three options that can address the threats outlined above, and has the option to combine them if they feel one approach is not good enough to address the problem.

Figure 4. Advising the student about security.

The teaching agent Travis the smartwatch is available throughout the game, providing information necessary for players to understand each protection method and its utility. It also provides feedback on the appropriateness of the player's preventative action suggestions to their friend, who functions as a teachable agent for each security concern. Feedback from Travis is given in the form of time energy, which is visualized as an energy bar in the upper left corner of the screen. As described in the game overview, time energy is needed for game progression and is gained by helping the student. The more helpful the answer given in dialogue, the more time energy is obtained by the player (Figure 4). With no single correct answer for the time energy questions, *Hacked Time* attempts to simulate everyday scenarios where personal judgment is needed depending on the specific security concern and context. For example, a password manager may be safe and helpful for web-based login activities where many passwords are used. However, two-factor authentication and a strong password may be vital to protecting a bank account. In *Hacked Time*, certain options are more useful than others in the students' particular situation. Bandura suggests [7] that people develop skills through modeling. People tend to judge their own abilities to exercise control over situations based on the abilities of those they regard as similar to themselves. In *Hacked Time*, the player suggests preventative actions to the student; the effectiveness of the suggestion is reflected in the time energy gained and how the student responds to their choice. The player can see what happens to the student and realize that they could be in a similar situation to the student's. Throughout the game, players learn the effects of different actions taken to remedy the situation for each security concern encountered.

Playtest insights

The first iterations of our game allowed the players to only learn about and implement one security feature in response to each security concern. However, in our preliminary testing, many players reported that they wanted the opportunity to learn about all the ways they could protect themselves. Therefore in the next iteration of the game, we allowed the players to learn about multiple security tools that they can use. At the same time, due to the added information presented to them, we also included a brief recap at the end of the skill development module so the information about the translation between security concern and preventative action is repeated to the player and can help them better retain what they learned.

To examine the effectiveness of the skill development component of our game, we looked at whether participants could identify the security concerns and corresponding preventative actions we outlined in-game and whether they could extend these skills into real-life situations. In external playtests, we found that participants were able to develop skills to solve in-game situations as well as identify solutions to real-life risky situations. Most playtesters were able to identify either a real-life security concern that could expose their account to being compromised, or the consequence that could follow. For instance, most playtesters identified that using the same passwords across accounts in real life put them at risk and conceptually understood how to address those concerns with the methods they learned. One playtester said, "I use the same password for everything. I should probably set up 2FA for my bank account."

Guided practice and skill enhancement

The third self-efficacy design principle focuses on guided skill practice and application in high-risk situations. The goal of this design guideline is to induce self-efficacy through modeling and repeated practice. In our case, after obtaining knowledge about the effectiveness and situated usage of cybersecurity protection methods, people require guidance to practice and perfect these skills. Bandura suggested that the value of guided practice is not only due to skill improvement, but also stems from the increased belief in their capacities [6]. In the case of cybersecurity, the increased belief is especially important as the skills themselves are not complicated to perform, but rather players perceive them to be complex because of negative perception and poor knowledge of feasibility of the implementation.

Our design goal was to guide the player through a high-risk situation and help them gain protection skills by going to the past to correct the student's actions. One of the reasons people do not engage in secure behaviors is they tend to overestimate the cost of protection [52]. The lack of knowledge about and practice with less commonly implemented methods, such as a password manager, may contribute to these misconceptions. Therefore, we strove to change players' belief that implementing security mechanisms are too difficult by guiding them through the process. When they go back in time to help the student, the player sets up a protection method for the student, such as initializing two-factor authentication for Facebook (Figure 5). The player can also explore and implement other security measures to increase the student's security, which lets them walk through other methods of protection. Finally, we show the positive outcome of protecting their account: when the player returns to the present time, the student's account was never hacked and all of their information stayed safe.

Playtest insights

In our first prototype, we guided the players through the implementation process with specific tools such as Facebook for 2FA and Roboform for password manager. From our preliminary testing, we found that players thought only showing

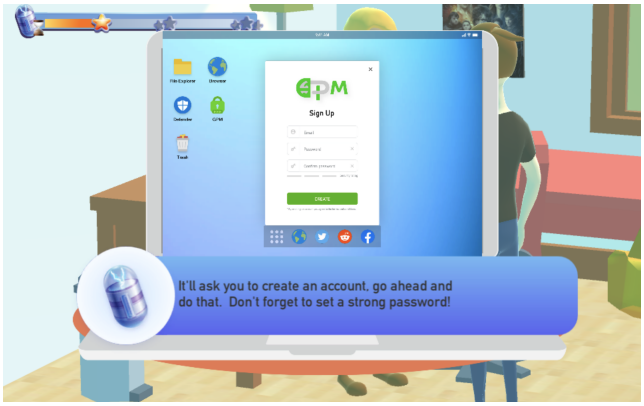

Figure 5. Guided practice - setting up password manager.

specific tools for implementation was limiting. Players responded they would like to learn an overview process for the security tools currently available so this knowledge can be applied to not only one tool, but security tools in general. For our next iteration of the game, we searched for the most commonly used security tools, and summarized the process needed to properly set them up. We then created a mock-up process based on the generalized set-up process. The goal was to allow the players to feel empowered not only using one specific tool, but also in adapting this knowledge to other similar tools.

To understand the effect of guided practice, we looked for signs demonstrating playtesters' familiarity and understanding of how to use the security tools. In our external playtests, playtesters were able to learn through our example and exhibited a sense of control. One playtester said: "I think it helped demonstrate the process of using these tools, and it is also step-by-step, and there is a quiz-like question to make sure whether the student knows why we need to use these methods".

EVALUATION

Our iterative design and playtest process left us confident that our game successfully incorporated Bandura's self-efficacy design framework. Not only were players able to complete the game and connect it to their own life experiences, the specific design decisions we made were understood by players. However, playtesting is a design method, not an evaluation method so we next wanted to compare our game to other potential methods for inducing cybersecurity self-efficacy. We therefore ran a randomized controlled experimental study to understand the impact of the game on player self-efficacy compared to a) cybersecurity information presented as text and b) a control condition without any cybersecurity content (a length-equivalent article on an unrelated topic).

Participants

We recruited 300 participants from the US on the Amazon Mechanical Turk (AMT) platform for baseline assessment. Participants were paid an hourly rate of 10 dollars. We chose the AMT platform because it provides an effective way of recruiting a large sample of participants, and the bias of AMT samples has been well studied by previous research. Of the 300 participants who completed our pre-experiment assessment, 191 returned for the experiment. We included attention check questions in the questionnaire, which ensure that participants actually engage with the material presented to them. These questions include instructions such as "select 'strongly disagree' for this question" and are embedded in the questionnaires throughout. This strategy is commonly implemented in Amazon-Turk-run studies to ensure participants do not respond randomly just to receive compensation, and has been demonstrated to be an effective strategy for maintaining data quality [15, 24]. After discarding participants who failed the attention check, we had 178 valid responses. Participant demographics are presented in Figure 6. There was no significant difference between baseline scores for participants who dropped out compared to participants who returned.

Procedure

Participants were first asked to fill out a baseline assessment survey online to measure their cybersecurity self-efficacy with [55]. Participants were then instructed to come back two days later for the experiment. In the experiment, participants were given a survey in which they were randomly assigned to one of three conditions and given specific instructions for their condition: 1) game, in which they were instructed to play *Hacked Time*; 2) information, in which they were instructed to read the equivalent to the text information on cybersecurity protection methods we presented in the game, delivered in a browser with proper formatting, headings, and paragraphs to facilitate reading of the information; and 3) control, in which participants were instructed to read a paragraph on an unrelated topic presented similarly as in condition 2. After the experimental manipulations, the participants were asked

		Control		Info		Game	
		n	%	n	%	n	%
Gender	Male	31	56.4	33	54.1	36	58.1
	Female	23	41.8	28	45.9	26	41.9
	Not disclose	1	1.8	0	0.0	0	0.0
Age	18-24	3	5.5	4	6.6	3	4.8
	25-34	26	47.3	22	36.1	26	41.9
	35-44	17	30.9	20	32.8	19	30.6
	45-54	4	7.3	8	13.1	8	12.9
	55-64	4	7.3	6	9.8	4	6.5
	65+	1	1.8	1	1.6	2	3.2
Race	Caucasian	42	76.4	42	68.9	44	71.0
	Black/Af. Am.	4	7.3	5	8.2	8	12.9
	Native Am.	0	0.0	2	3.3	0	0.0
	East Asian	3	5.5	1	1.6	5	8.1
	Pac. Islander	0	0.0	0	0.0	0	0.0
	S.E. Asian	1	1.8	0	9.8	1	1.6
	South Asian	2	3.6	2	3.3	1	1.6
	Hispanic	2	3.6	4	6.6	1	1.6
	Mixed Race	1	1.8	4	6.6	1	1.6
	Other	0	0.0	1	1.6	1	1.6
Total		55	100	61	100	62	100

Figure 6. Demographics

to fill out the same self-efficacy outcome assessments they completed in baseline again.

Measures

To measure self-efficacy related outcomes, we adapted Witte's Risk Behavior Diagnosis Scale [55]. This scale includes four sub-scales that measure elements of Bandura's concept of self-efficacy: severity of threat, susceptibility to threat, self-efficacy, and response efficacy. As a construct closely related to self-efficacy, response efficacy measures the player's perception of how well a tool works instead of how well they could do something themselves and is an important predictor for technology acceptance [58]. We also included the Security Attitude scale (SA-6) for evaluating cybersecurity attitude-related outcomes [21]. To control for participants' prior experience with technology, we asked for their comfort with technology on a scale of 1 (extremely uncomfortable) to 7 (extremely comfortable) in the baseline assessment. For the pre-experiment baseline assessment, participants completed the Risk Behavior Diagnosis Scale, SA-6, comfort with technology, and demographic questions. For the post-experiment assessment, participants completed all the same measures except the comfort with technology and the demographic questions. All the measures used 1 (strongly disagree) to 7 (strongly agree) Likert scale response format.

Statistical Analysis

We used analysis of covariance (ANCOVA) for each of our five variables: severity of threat, susceptibility to threat, self-efficacy, response efficacy, and security attitude. ANCOVA is a statistical analysis tool that evaluates the effect of the independent variable on the dependent variable while statistically controlling for the effect that other variables not of primary interest (covariates) might have on the dependent variable [33]. We employed ANCOVA as it allows us to adjust for the effect of baseline assessment score as well as participant's familiarity with technology on the post-test assessment score. For our model, condition was treated as the categorical fixed factor. Post-experiment assessment was treated as the dependent variable. We included participants' self-assessment of their familiarity with technology, as well as their pre-experiment baseline assessment score, i.e. self-efficacy and security attitude, as the covariates. Results from the ANCOVA are presented in Figure 7.

RESULTS

Severity and susceptibility to threat

There was no significant change in participants' response for severity or susceptibility to threat in any of the conditions (Figure 7).

Self-efficacy and response efficacy

The result from ANCOVA (Figure 7) indicated that participants in different conditions showed significant change in their self-efficacy as well as their response efficacy. A post-hoc analysis showed that participants in the game condition scored significantly higher in both self-efficacy and response efficacy in comparison to the information only and control groups.

	Control	Info	Game	
	EMM (SE)	EMM (SE)	EMM (SE)	R^2
SE	4.78^{a} (0.09)	5.13^{b} (0.08)	5.44^{c} (0.08)	0.52
RE	5.06^{a} (0.09)	5.24^{a} (0.08)	5.56^{b} (0.08)	0.46
SA6	4.76^{a}(0.10)	4.92^{ab} (0.10)	5.12^{b} (0.10)	0.59
TS	4.29 (0.13)	4.60 (0.12)	4.61 (0.12)	0.32
STT	3.38 (0.15)	3.82 (0.14)	3.55 (0.14)	0.18

1) Means marked with different superscripts differ at $p < 0.01$ significance level. 2) SE - self-efficacy; RE - response efficacy; SA6 - security sensitivity; TS - threat severity; STT - susceptibility to threat; EMM - estimated marginal mean. 3) Independent variable: condition; covariates: pre-test score, self-assessment of technical skill.

Figure 7. Estimated marginal means from ANCOVA by condition for primary dependent variables. Estimated marginal mean represents the mean of the independent variable after adjusting for the effect of covariates.

For self-efficacy, the information only group showed significantly higher self-efficacy compared to the control group. There is no significant difference between response efficacy scores for the information only and control groups. This result showed that playing our game was more effective at increasing player's self-efficacy and response efficacy than simply reading information on cybersecurity. We recognize that making a cybersecurity game takes more time and resources than presenting only security information. However, we believe that presenting only information on the protection methods to players is not particularly effective due to the the public's biased perception of the security tools [26, 52]. This result effectively demonstrated that our game achieved its transformational goal, justifying the increased resources needed to develop such a game.

Security attitudes

The ANCOVA results demonstrated that participants in different conditions had significantly different levels of change in their security scores. A post-hoc analysis further suggested that participants in the game condition had significantly higher security attitude scores compared to control group (Figure 7), suggesting more positive attitudes towards seeking out information about and utilizing security protection methods as a result of game play. This indicated that our game was effective in making the players more conscious of their security behavior and the need to protect themselves online.

DISCUSSION

Expanding on self-efficacy games for cybersecurity

Our results suggest our game design was effective in increasing players' self-efficacy. We believe that our overall game framework could be used by others to design future cybersecurity games to increase players' self-efficacy. We suggest the following design recommendations from our game.

Our overall design followed the general format of an interactive novel, with hidden object elements to accustom the player to thinking about security *in context*. For addressing additional topics within cybersecurity, we recommend creating a character who experiences the cybersecurity breach or challenge, and placing them in an authentic context in which the issue could have occurred.

To encourage understanding of the connection between security concerns and preventative action, we sought to encourage empathy between player and character. We recommend that designers allow players some measure of customization for their character, and that the dialogue be plausible and authentic for the characters being portrayed. This may mean involving a professional writer or having external dialogue readers. Additionally, we faced challenges around the *relationship* between the playable character and the affected character. Having the player's character teach the affected character may have undermined the player's risk perception, but it also may have contributed to the overall positive outcomes of the game. We recommend that during the iterative design process, designers experiment with a range of relationships between characters in the game.

To help players develop their skills, the challenges facing the characters should not be two-dimensional. Real-life scenarios are often complex and multi-dimensional, with no single right answer. We recommend that this truth should be reflected not only in the narrative design, but also in the design of the game's feedback system, which should consider *relative effectiveness* rather than strict right and wrong.

Lastly, for guided practice, we recommend designers implement mock-up processes that summarize and resemble what players could encounter in real life, and provide the players with an opportunity to practice their skills in a controlled environment. Before the player interacts with these processes, they should have multiple positive experiences with the hidden object component of the game that are *not* directly cybersecurity related. By the time the player encounters the guided practice, the game has set norms that hunting for the next action is playful, appropriate, and not shameful.

Information acquisition and self-efficacy

Our study shows that receiving security-related information, without the game delivery mechanism, did affect some post-test outcomes. Participants had increased self-efficacy after receiving security information, but showed no change in response-efficacy or security attitude. In other words, knowing about the security measures made participants believe that they were able to use the security tools. However, it didn't necessarily increase their belief that these tools actually work to protect them. Without this strengthened belief in the effectiveness of the tools, the increased self-efficacy could have a less pronounced impact on the participant's actual behavior and belief [58] due to inaccurate perceptions about tool effectiveness and difficulty of implementation [52].

By comparison, in the game condition, participants' self-efficacy and their belief in the efficacy of the tools increased, over and above what information alone provided. We hypothesize that the core game mechanic of *searching* supported this outcome. When players time-travel to the past, they can experience the implementation process first-hand by exploring a simplified version of the security tool interface. Because the game has previously taught them that searching is a productive game activity, by having them search the student's room for clues, they are primed to explore the tools and discover the needed interactions for implementation. This activity links together Bandura's concepts of *enactive attainment* (experiencing mastery) and *vicarious experience* (experiencing through another, e.g. a character) with the interactivity that games can offer [6]. The experience of learning by doing in real life might be hard to come by, or might be too risky for players to experiment. However, transformational games provide a platform for us to offer players enactive attainment at low risk. Our results suggest that the additional resources needed to develop a cybersecurity game, over and above providing information, did provide increased benefits to the players.

Agency and self-efficacy in game design

Our study provides evidence that integrating self-efficacy principles in a transformational game positively impacts a player's self-efficacy for cybersecurity. *Hacked Time* was more effective in improving constructs related to self-efficacy than either of our control conditions. While this finding is well-supported by the cybersecurity and behavior change literature, it is surprising in the context of game design. Game designers describe good transformational games as ones where content is deeply integrated into the game mechanics [27, 32]. Designers are more skeptical when transformational content does not connect with the systems or mechanisms of the game; in some cases narrative elements may even distract from learning [3, 35]. In *Hacked Time*, the security content is primarily integrated in the narrative, but the game still has an effect over and above presenting the content. Given that game designers have deep expertise in what makes games successful, how can we explain the success of our design?

We understand this finding through the lens of agency. Agency is a core concept in game design. It refers to the user's sense of "being an agent", that they have the capacity to act in a virtual environment and the effectiveness of their action is evident [2]. Agency has been a focal point of HCI research for a long time. Schneiderman [47] pointed out that players desire to be in control of the system with which they are interacting, and for the system to respond to their actions. Designing interfaces and tools that provide players with a sense of agency helps with adoption of technology as well as with the user's sense of control [36]. In games, agency is also an important tool that can be used to create a sense of ownership. Nguyen [37] calls games "agency as art," in which the players' abilities are deliberately matched to game goals in order to create an internal experience of desiring and achieving.

Along with the original interpretation of sense of control over the medium, some scholars have argued that individual interpretations and social experiences are core to agency in games [51]. The participant's experience of observing, of questioning, or of making sense of a fixed script (such as in literature and theatre) can inform the development of agency [44]. These

arguments support the notion that the sense of agency does not necessarily have to come from direct player control over everything that happens in the game. We therefore suspect that even though we offered limited choices to the players, the experiences they had prior to the game, and their ability to compare, contrast, and extrapolate through the interactions in game, provided a chance for agency to develop. Agency, therefore, describes the ownership of the user toward the game, while self-efficacy describes their ownership of their own actions. The ownership that the participants feel towards the game are likely to provide a comparable guide to extend the ownership towards their actions in real life. Therefore, in future work we aim to explore whether the *experiential* agency that *Hacked Time* provides to the players affects their self-efficacy.

Risk perception and security attitudes

We found that players did *not* increase their perception of security-related risks in the game condition, although their self-efficacy measures did change. This is surprising because risk communication is an important part of Bandura's design framework. We hypothesize that this came about because we made the player a *teacher* for the affected character, instead of having security breaches affect the player's character directly. We made this choice because the literature on teachable agents suggests that having the player teach another character might be more effective than learning from a character due to the self-explanation effect [9, 34]. In our playtesting, we explored whether players *related* to the affected character, and received responses such as "this person is like my mom." While we initially viewed these responses as positive, revisiting them in light of our quantitative results suggests that we may have failed to connect the player's risk to the character's situation. Players did relate to the victim, but not in a way that put themselves in their shoes. Instead, they saw the character from a teacher's perspective that made them believe that they would not make mistakes like these. There might be an inherent trade-off in design, therefore, to let the player be the teacher or the student. For example, giving the players the role of teacher might increase their learning, but make them less susceptible to threat; however giving the players the role of student might make them more susceptible to threat, but less positioned to learn. This is a question that is worth further investigation.

We also note that even though players did *not* increase in their perception of risk, their security attitude was higher after playing the game. Why did players' attitudes change, but not their risk perception? We believe that going through the game experience made players actively think about security practices. At the same time, their increased knowledge and efficacy in both themselves and the tools might contribute to better attitudes. The game decreases the mental barriers that players might have based on an inaccurate perception of the cost and benefit of the tools. Therefore, in-game exposure to security practices may result in a better mental disposition toward security practices.

In summary, in *Hacked Time*, we introduced various game patterns that were closely based on Bandura's self-efficacy design framework. We believe that our design approach can be extended to creating transformational games for other challenges within the cybersecurity field. Additionally, as self-efficacy interventions have been implemented widely in other fields, we believe that our overall design framework can be extended beyond cybersecurity, to areas such as financial literacy or health behavior change.

LIMITATION AND FUTURE WORK

In this study, we focused on self-efficacy as a mediator for player's behavior change instead of directly measuring a player's behavior change outcome. Even though self-efficacy has been repeatedly shown to be a valid predictor for behavior change [18, 42], we believe it is still important to measure behavioral outcomes. This study allowed us to see the preliminary impact of our game, and provided good evidence that our game improves players mindset on security practices. We believe enhancing self-efficacy is an important first step towards behavior change. We plan to conduct future studies that directly measure player's behavioral outcomes in longitudinal follow-ups to understand when and how changes in self-efficacy lead to cybersecurity behavior change.

Another limitation of this study is that we could not differentiate the impact of our game design patterns. It is evident that the game as a whole worked to increase people's self-efficacy. We have hypotheses about which parts of the game had what impact, and we believe as a whole, our game can be modified and adapted into other fields. However, we have yet to isolate specific design decisions that could be extrapolated and used as individual elements in other games. For future studies, we plan to dissect and understand the impact of each individual element of our game.

Lastly, due to practical constraints, we were not able to employ Bandura's social support design principles in this game. We aim to examine the effect of social support on player's self-efficacy in future studies.

CONCLUSION

Games are an increasingly popular intervention to encourage better cybersecurity behaviors online. In this paper we present in detail our design approach to implement self-efficacy theory in a transformational game. We conducted a quantitative study to evaluate self-efficacy outcome as well as security attitudes in players. Our results showed strong support for the effectiveness of our design. Players showed increased self-efficacy, response efficacy, and security attitudes in the game as compared to an unrelated control. In comparison to the group that only received security information, players in the game condition showed increased self-efficacy and response efficacy. Our work suggests that game design based on self-efficacy theory has great promise to encourage better cybersecurity practices. We contribute to the interaction design and HCI literature by showing the promise of using behavior change theory in transformational game design for cybersecurity education, as well as introducing a game design pattern that can be generalized and applied in other fields for self-efficacy motivated interventions.

ACKNOWLEDGEMENTS

This work is supported by National Science Foundation grant CNS1704087.

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] Josephine Anstey. 2005. Agency and the "emotion machine". In *International Conference on Virtual Storytelling*. Springer, 125–128.

[3] Michael B Armstrong and Richard N Landers. 2017. An evaluation of gamified training: Using narrative to improve reactions and learning. *Simulation & Gaming* 48, 4 (2017), 513–538.

[4] 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.

[5] Maria Bada, Angela M Sasse, and Jason RC Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672* (2019).

[6] Albert Bandura. 1977. Self-efficacy: toward a unifying theory of behavioral change. *Psychological review* 84, 2 (1977), 191.

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

[8] Gitanjali Baral and Nalin Asanka Gamagedara Arachchilage. 2019. Building Confidence not to be Phished Through a Gamified Approach: Conceptualising User's Self-Efficacy in Phishing Threat Avoidance Behaviour. In *2019 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 102–110.

[9] Gautam Biswas, Krittaya Leelawong, Daniel Schwartz, Nancy Vye, and The Teachable Agents Group at Vanderbilt. 2005. Learning by teaching: A new agent paradigm for educational software. *Applied Artificial Intelligence* 19, 3-4 (2005), 363–392.

[10] Pamela Briggs, Debbie Jeske, and Lynne Coventry. 2017. Behavior change interventions for cybersecurity. In *Behavior Change Research and Theory*. Elsevier, 115–136.

[11] Tianying Chen, Jessica Hammer, and Laura Dabbish. 2019. Self-Efficacy-Based Game Design to Encourage Security Behavior Online. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–6.

[12] Judeth Oden Choi, Jodi Forlizzi, Michael Christel, Rachel Moeller, MacKenzie Bates, and Jessica Hammer. 2016. Playtesting with a Purpose. In *Proceedings of the 2016 annual symposium on computer-human interaction in play*. ACM, 254–265.

[13] Thomas M Connolly, Elizabeth A Boyle, Ewan MacArthur, Thomas Hainey, and James M Boyle. 2012. A systematic literature review of empirical evidence on computer games and serious games. *Computers & education* 59, 2 (2012), 661–686.

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

[15] Paul G Curran. 2016. Methods for the detection of carelessly invalid responses in survey data. *Journal of Experimental Social Psychology* 66 (2016), 4–19.

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

[17] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. 2014b. 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.

[18] Hein de Vries, Margo Dijkstra, and Piet Kuhlman. 1988. Self-efficacy: the third factor besides attitude and subjective norm as a predictor of behavioural intentions. *Health education research* 3, 3 (1988), 273–282.

[19] Paul Dolan, Michael Hallsworth, David Halpern, Dominic King, Robert Metcalfe, and Ivo Vlaev. 2012. Influencing behaviour: The mindspace way. *Journal of Economic Psychology* 33, 1 (2012), 264–277.

[20] 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.

[21] Cori Faklaris, Laura A Dabbish, and Jason I Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*.

[22] Tracy Fullerton. 2014. *Game design workshop: a playcentric approach to creating innovative games*. AK Peters/CRC Press.

[23] Julie M Haney and Wayne G Lutters. 2018. " It's Scary... It's Confusing... It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 411–425.

[24] David J Hauser and Norbert Schwarz. 2016. Attentive Turkers: MTurk participants perform better on online attention checks than do subject pool participants. *Behavior research methods* 48, 1 (2016), 400–407.

[25] 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.

[26] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 327–346.

[27] Katherine Isbister, Mary Flanagan, and Chelsea Hash. 2010. Designing games for learning: insights from conversations with designers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2041–2044.

[28] Nina Iten and Dominik Petko. 2016. Learning with serious games: Is fun playing the game a predictor of learning success? *British Journal of Educational Technology* 47, 1 (2016), 151–163.

[29] Rodney P Joseph, Casey L Daniel, Herpreet Thind, Tanya J Benitez, and Dori Pekmezi. 2016. Applying psychological theories to promote long-term maintenance of health behaviors. *American journal of lifestyle medicine* 10, 6 (2016), 356–368.

[30] Yogesh Joshi, Samir Saklikar, Debabrata Das, and Subir Saha. 2008. Phishguard: a browser plug-in for protection from phishing. In *2008 2nd International Conference on Internet Multimedia Services Architecture and Applications*. IEEE, 1–6.

[31] 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.

[32] Christina Kelley, Lauren Wilcox, Wendy Ng, Jade Schiffer, and Jessica Hammer. 2017. Design features in games for health: disciplinary and interdisciplinary expert perspectives. In *Proceedings of the 2017 conference on designing interactive systems*. ACM, 69–81.

[33] Geoffrey Keppel. 1991. *Design and analysis: A researcher's handbook*. Prentice-Hall, Inc.

[34] Yanghee Kim and Amy L Baylor. 2006. A social-cognitive framework for pedagogical agents as learning companions. *Educational Technology Research and Development* 54, 6 (2006), 569–596.

[35] Scott W Mcquiggan, Jonathan P Rowe, Sunyoung Lee, and James C Lester. 2008. Story-based learning: The impact of narrative on learning experiences and outcomes. In *International Conference on Intelligent Tutoring Systems*. Springer, 530–539.

[36] James W Moore. 2016. What is the sense of agency and why does it matter? *Frontiers in psychology* 7 (2016), 1272.

[37] C Thi Nguyen. 2018. Games: Agency as Art. (2018).

[38] 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.

[39] Pew research center. 2017. Password management and mobile security. (2017). `https://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/`

[40] Hyeun-Suk Rhee, Cheongtag Kim, and Young U Ryu. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security* 28, 8 (2009), 816–826.

[41] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91, 1 (1975), 93–114.

[42] Dale H Schunk. 1991. Self-efficacy and academic motivation. *Educational psychologist* 26, 3-4 (1991), 207–231.

[43] Norton security. 2018. 10 cyber security facts and statistics for 2018. (2018).

[44] Joseph Seering, Saiph Savage, Michael Eagle, Joshua Churchin, Rachel Moeller, Jeffrey P Bigham, and Jessica Hammer. 2017. Audience Participation Games: Blurring the Line Between Player and Spectator. In *Proceedings of the 2017 Conference on Designing Interactive Systems*. ACM, 429–440.

[45] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 88–99.

[46] Ruth Shillair, Shelia R Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, and Nora J Rifon. 2015. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior* 48 (2015), 199–207.

[47] Ben Shneiderman. 2010. *Designing the user interface: strategies for effective human-computer interaction*. Pearson Education India.

[48] Victor J Strecher, Brenda McEvoy DeVellis, Marshall H Becker, and Irwin M Rosenstock. 1986. The role of self-efficacy in achieving health behavior change. *Health education quarterly* 13, 1 (1986), 73–92.

[49] Jerry Chih-Yuan Sun, Shih-Jou Yu, Sunny SJ Lin, and Shian-Shyong Tseng. 2016. The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior* 59 (2016), 249–257.

[50] Cass R Sunstein. 2014. Nudging: a very short guide. *Journal of Consumer Policy* 37, 4 (2014), 583–588.

[51] Karen Tanenbaum and Joshua Tanenbaum. 2009. Commitment to meaning: a reframing of agency in games. (2009).

[52] Nik Thompson, Tanya Jane McGill, and Xuequn Wang. 2017. "Security begins at home": Determinants of home computer and mobile device security behavior. *computers & security* 70 (2017), 376–391.

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

[54] Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J Rifon, and Shelia R Cotten. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security* 59 (2016), 138–150.

[55] Kim Witte. 1996. Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of health communication* 1, 4 (1996), 317–342.

[56] Pieter Wouters, Christof Van Nimwegen, Herre Van Oostendorp, and Erik D Van Der Spek. 2013. A meta-analysis of the cognitive and motivational effects of serious games. *Journal of educational psychology* 105, 2 (2013), 249.

[57] 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.

[58] Xiaofei Zhang, Xiaocui Han, Yuanyuan Dang, Fanbo Meng, Xitong Guo, and Jiayue Lin. 2017. User acceptance of mobile health services from users' perspectives: The role of self-efficacy and response-efficacy in technology acceptance. *Informatics for Health and Social Care* 42, 2 (2017), 194–206.