

“Smells Phishy?”: An Educational Game about Online Phishing Scams

Malak Baslyman
School of Electrical and
Computer Engineering
University of Ottawa
Mbasl071@uottawa.ca

Sonia Chiasson
School of Computer Science
Carleton University
chiasson@scs.carleton.ca

Abstract—We propose *Smells Phishy?*, a board game that contributes to raising users’ awareness of online phishing scams. We designed and developed the board game and conducted user testing with 21 participants. The results showed that after playing the game, participants had better understanding of phishing scams and learnt how to better protect themselves. Participants enjoyed playing the game and said that it was a fun and exciting experience. The game increased knowledge and awareness, and encouraged discussion.

I. INTRODUCTION

Online phishing scams in which criminals trick users into revealing their personal details such as credit card information remain a serious concern [1]. The Anti-Phishing Working Group (APWG) reported that 630,494 unique phishing websites were detected in the first three quarters of 2015. It also reports that banking and financial services are among the most-targeted industry sectors [2]. In 2013, the estimated loss from phishing attacks was USD \$5.9 billion [3]. Advances in automatic detection of phishing have had significant success, but can lack contextual information necessary to detect more sophisticated attacks [4]. End-users remain instrumental in fighting online phishing since they are often the only ones with this contextual knowledge, but users need security awareness to recognize and avoid threats [5].

To address this online interaction issue, we designed and developed *Smells Phishy?*, a board game to expose users to phishing risks, reveal common phishing tricks, and provide players with security advice and strategies to protect their personal information online. The game demonstrates phishing scams in the context of online shopping. Players navigate the board while completing their shopping list, facing potential phishing attacks, and deciding how to handle them. Correct decisions lead to rewards while errors result in an in-game penalty. Both situations include a brief explanation of the risk and appropriate action.

End-users tend to believe that phishers are highly skilled technical cybercriminals [6]. The game aims to show users that they can still outwit phishers and protect their personal information. The game boosts people’s confidence to beat phishers, by showing them that detecting scams is often achieved through close attention to what the others say or

present. These skills are necessary for secure online interaction.

Our main contribution is the *Smells Phishy?* board game, along with its design rationale and preliminary empirical evaluation. 21 participants played the game in small groups. The results of the study showed that participants who did not know anything about online phishing scams before playing the game could define what phishing scams and explain how to protect themselves after playing the game. Even technically inclined participants showed increase knowledge and reflection on the topic. Furthermore, participants felt that playing the game was a pleasing, exciting and rich experience.

II. RELATED WORK

A. Phishing

Online phishing scam is kind of social engineering where criminals fool users to reveal sensitive information, typically for the purposes of identity theft or financial gain [1], [7]. Phishers send fraudulent emails to users asking them for help or offering business or inheritance, and asking them to click on a link, or open an attachment [3], [7]. The communications usually include a sense of urgency to distract users’ attention from carefully examining the contents of the message. Sometimes, they exploit users’ emotions by offering free rewards or asking for help due to natural disaster, or the exploit users’ trust by impersonating popular brands and sending users to fraudulent sites. More sophisticated approaches reach users by phone, by SMS, through social network websites, or even through multiplayer online games [7]. Phishing attacks not only target home users, but also target organizations, such as corporations and financial institutions. Some phishing attacks have stolen sensitive security information or caused significant financial losses for organizations [8].

Modern browsers include features to help users detect phishing, and phishing sites often display characteristics that could alert a vigilant user of the potential scam. However, many users still fail to recognize phishing sites.

Anti-phishing approaches, such as email filtering [9], malicious URL detection tools [10], and taking down phishing websites [11] are useful to fight against phishing attacks, and these automated methods should be the first line of defense. Automated methods have improved significantly in recent

years, with popular browsers eventually catching as many as 90% of phishing sites [12].

However, a secondary line of defense, provided by users, is still necessary in cases where automated tools fail or have not yet detected a new attack [1], [7]. Human recognition to phishing emails and website is necessary to handle these risks, but users are quite poor at recognizing phishing attacks [1], [13]–[15].

Educating and training users about examining URL and domain names, inspecting website contents (e.g., for spelling mistakes, poor GUI, and unbelievable offers) and handling phishing emails is essential to tackle this problem [1], [3], [7], [16].

B. Phishing Education

Education about phishing risks is recognized as an important aspect of phishing protection. Its effectiveness in raising users' awareness has been demonstrated in several studies [17]–[19] and takes three forms: online training tutorials, embedded training systems and educational games.

Many websites offer guidelines and advice to help users distinguish between spoof and safe websites. For example, eBay released an article illustrating how to differentiate the real eBay website from fake ones [20]. Government websites [21], [22] provide essential information to stay safe online, while international organizations such as the APWG exist to combat cybercrime and raise awareness through comprehensive educational material [2]. Embedded training systems aim to teach users within the context where they may normally be attacked. One of the most significant works in this area is PhishGuru [18], [23]. The system periodically sends fake phishing emails to users and presents immediate feedback according to users' behavior. A user study showed that PhishGuru helped teach users about phishing attacks and how to avoid them.

C. Security Games

Games have long been recognized as an effective and engaging educational strategy. Within the realm of computer security and privacy, this approach has been followed to teach several non-phishing topics. Some are designed for traditional tabletop use and multiple players, while others are digital single-player games.

d0xd3 is an open-source tabletop game that teaches players about network security by taking on the role of white-hat hackers [24]. The game is collaborative; players win or lose as a group against the game itself. Preliminary user testing was conducted with middle school, high school, undergraduate, and adult groups. The authors received positive feedback from users. They also observed discussion and strategizing relating to security, indicating engagement with the material, but no pre/post assessments directly measured learning.

Another good example of a game to raise awareness is Control-Alt-Hack [17]. The players take on the role of white-hat hackers and perform several missions for “client” companies looking to improve the security of their systems. User

testing with over 400 players shows increased awareness of security and change in security attitude. Other games, such as Protection Poker [25], EOP [26] and OWASP Cornucopia [27], are designed to teach software developers to consider security risks from the very early phases of software development.

In terms of digital games, there are two significant titles. Anti-Phishing Phil [28] teaches players to recognize illegitimate websites through presenting URLs in the context of an underwater game where the player must protect Phil the fish from falling for phishing bait'. A similar game has also been developed for the mobile platform [29]. The second game is CyberCIEGE [30] that was designed to teach network security students through simulated attack scenarios. Players have to defend their workstation from attack. The game has been incorporated into the curriculum of some academic institutions. None of the current games focus on specific end-use activities, or covers a range of tricks relating to phishing from the viewpoint of users (such as asking for social insurance numbers). Smells Phishy? is intended for end-users and provides education in the context of a popular real-life scenario, namely online shopping.

III. DESIGN OBJECTIVES

When designing educational games, the challenge is to fulfill the educational requirements while providing an enjoyable playing experience [31]. We conceptualized Smells Phishy? with several design objectives in mind. In this section, we briefly describe these primary goals.

Educational: The main purpose of the game is to teach players about phishing scams, how to protect themselves from these risks, and about the importance of vigilance. We assumed little-to-no pre-existing knowledge about phishing, but assumed that players were familiar with the basics of web browsing and the concept of online shopping. Beyond recognizing suspicious URLs, our intention was to promote self-reflection and encourage players to understand the consequences of their actions with respect to phishing, whether positive or negative. We intended to impart the following specific lessons:

- Verify the URL for suspicious content
- Notice the presence (or absence) of SSL indicators
- Follow basic password rules
- Recognize common characteristics of phishing websites or emails such as spelling mistakes or making unrealistic offers

Entertaining: Our second goal was to make the game fun and entertaining to promote engagement with the material. Another major motivation was to promote a fun and safe environment in which to test their knowledge. We wanted to encourage players not to feel ashamed about their mistakes because the idea is to make users fall victim to phishing tricks within the game so that they learn about them. Entertainment is also essential to encourage players to continue playing and absorb security knowledge without feeling bored [31].

Conversation-provoking: We want the game to promote reflection and discussion around the subject of phishing and

making more secure choices. We also want it to motivate players to link the presented security concepts to their real life experience and share their stories and experiences regarding these concepts with other players. These reflections enrich learning experience and help players realize that others also struggle with identifying phishing at times. Ideally, the game is memorable enough that players also share their game-playing experience and learning with others after playing the game.

IV. GAME MECHANICS

With these objectives in mind, we turned to the game mechanics — the components, rules, techniques and tools used to build and design games [32], [33]. In our project, this included four critical factors: choosing the game context and format, choosing how to demonstrate the security concepts, providing educational messages, and ensuring funny and enjoyable learning experiences.

The premise of the game is that users need to make purchasing decisions as they shop at several e-commerce stores. We chose online shopping due to its popularity, its obvious need for requiring personal information (including credit cards), which exposes users to potential threats, and its generalizability since tasks are similar across different stores.

Players face the challenge of handling phishing risks within the game; our intention is to help people to link these security concepts to real life scenarios. A positive or negative consequence follows each decision, demonstrating the potential risks and secure behaviors.

As part of the designing game mechanics, we included several attributes to increase players' engagement:

Turn-based: We selected a turn-based board game format to encourage players to interact with each other and learn from the actions of others as well as their own.

Achievement: Each player is tasked with purchasing items on an individualized shopping list, which acts as a scorecard. Successful purchases advance the player within the game.

Resources: Players also track their progress within the game through the balance of their credit card. Players must find a way to safely purchase all items in their shopping list while finishing with the most money. Unwise decisions can result in a financial penalty, while smart moves sometimes result in bonuses. Hints, which can help avoid unfavorable outcomes, cost money so players must weigh the trade-off between spending a small sum to potentially avoid worse consequences.

Rewards and punishments: Some successful decisions result in bonus rewards. These occur at variable times; a correct decision always results in achievement, but sometimes it also results in a bonus added to credit cards by the bank. Players making unwise decisions may unexpectedly find themselves in jail to reflect upon their actions while others move ahead.

Competition: Players compete against each other to be first to purchase all items on their shopping list with the highest balance left on their credit card.

Feedback loop: At each turn, players must make purchasing decisions. Each decision is directly linked to a consequence

with in-game ramifications and feedback that is meaningful within the game and when faced with real-life decisions relating to phishing online.

Cascading information theory: Players receive phishing advice throughout the game, but rather than offering all details at once, tips are uncovered one at a time as a direct result of the players' actions. By cascading information in such a way, players have time to assimilate the advice in context, before moving on to the next task.

Cards: To add variability to the game, cards are used at each turn to describe the obstacle faced by the player, along with the associated consequence and security advice.

Narrative: Besides the general narrative of online shopping, each task has a short scenario and explanation for the challenge to help players imagine themselves faced with a similar scenario in real-life. The hints, consequences, and security advice follow the same narrative thread.

Humor: Humor is included within the scenarios by placing players in funny situations, or within the consequences by describing silly outcomes for the players' actions.

A. Game Overview

Players start with money on a prepaid credit card. With each turn, players attempt to buy items from a shopping list by making careful purchasing decisions. Each choice results in either a positive or negative consequence such as successfully buying the item or having to deal with being phished. Hints can be purchased to help with decision-making, and post-decision feedback offers security advice. The game continues until all players except the last have completed their shopping list (since the remaining player cannot play alone) and the completed player with the most money remaining wins.

B. Game Components

The main components of the game are summarized below.

Board: consists of a 18"x18" square board illustrating a neighborhood map with many storefronts, a police station, and a bank. Each is depicted with a cartoon representation of its physical counterpart, intended to have a clear parallel with online shopping components.

Cards: there are five types of cards, as follow.

- Task cards: provide a task description and corresponding challenge. Each store has its own task cards. The tasks describe the obstacle faced by the user while purchasing an item. The tasks are intended to test players' procedural knowledge relating to online purchases and phishing.
- Police cards: reveal the consequences of the player's action based on how they chose to answer the challenge; task cards and police cards are paired. Each police card has two sections: 1) The punishment or reward resulting from the player's response to the Task challenge. For example, if the player has fallen for a phishing scam, they may be sent to jail for a turn or lose money. If they took appropriate action, they are congratulated and may receive an additional reward such as extra money. 2) The security advice provides additional feedback and

tips about the specific risk and teaches how to avoid this risk in future. The security advice is the main educational resource providing feedback on players' performance.

- Hint cards: help players safely accomplish their task; each Task card has a corresponding hint card. They offer hints about what actions to take and provide motivation behind the suggested actions. Unlimited access to the Hint cards may be purchased for \$5 at the start of the game, or individually for \$1 at each turn. The Hint cards simulate security software that might alert users to potentially dangerous situations.
- Credit cards: are initially filled with \$100. Each player receives one credit card for purchasing the items on their shopping list. Tokens are used to represent additions/subtractions from the total.
- Shopping lists: contain items to purchase. For each item, the store where the item is available and its price is also indicated. Each player receives a different shopping list.

Movement tokens: used to represent players on the board. Die: determines who starts the game and to determine who is responsible for reading a Task card for the current player.

Booklet: contains the game instructions and links to online resources to learn more about phishing safety.



Fig. 1. Game board and card placement.

C. Game Description

In its present configuration, the game can be played by 2 to 4 players. At the beginning of the game, each player receives a credit card with \$100. They may purchase unlimited access to the Hint cards, or choose to buy-as-you-go. The game unfolds as each player in turn attempts to purchase the items on their shopping list and deal with the consequences of their actions. Each Task and Police card is read aloud so that everyone can consider the task and benefit from the feedback and security advice provided in response. For each potential behavior, there is a consequence. The consequence may involve sending the player to jail to be punished, sending the player to the bank to claim bonus money or reimbursement after being phished, or forwarding the player to another store. If a player fails to make a purchase, they must return to the store on their next turn, pick a new Task card, and attempt to purchase the item again. When the player passes a security challenge and successfully purchases the desired item, the item is crossed from the shopping list, the financial transaction takes place, and the player may pursue the next item at their next turn. The game runs until all players, but one, have purchased all required items or run out of money. The winner of the game is the player who buys all the required shopping list items and has the most money remaining.

Figure 1 illustrates the board game with the neighborhood stores, bank and jail, as well as the Tasks cards, Police cards, Hint cards. Figure 2 shows the other game components. Figure 3 gives examples of each type of card in relation to each other.

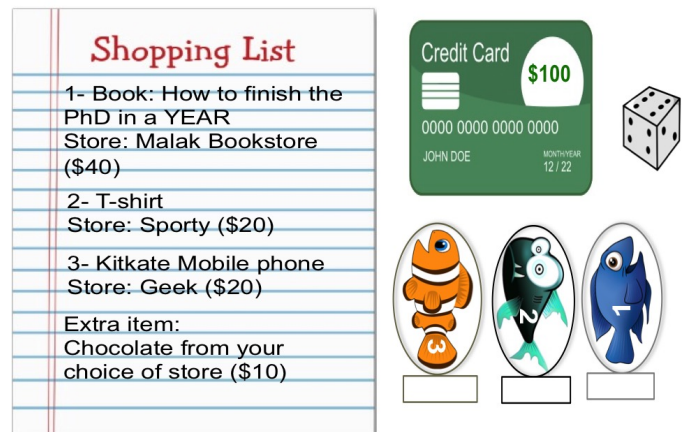


Fig. 2. Game components include a shopping list, credit card, die, and movement tokens.

D. Intended Audience

The game is intended to provide general advice about phishing protection, giving players a reasonable level of literacy about the subject. Players may have varying levels of knowledge before playing the game, but the information will be most novel and useful to those with low phishing literacy. One strategy to promote discussion among players is to include a more advanced player who can act as a mentor and expand upon the tips provided by the game. While we tested the game with adults, we believe that the content of the game could be equally suitable for children 12 and up (see Section VI-E).



Fig. 3. Sample Task, Hint, and Police cards.

V. USABILITY STUDY

We carried out a formative in-lab user study to evaluate the effectiveness of the game. The study was reviewed and approved by our Institutional Review Board.

A. Methodology

Participants: There were 21 participants (9 male and 12 female, aged 24-44 years). We recruited three experts in computer security to get their feedback on the game concept and material, and to see if their presence would enhance the game experience. Four participants were computer scientists and the others were non-experts with various non-technical backgrounds. The majority were university students. Participants spent an average of eight hours daily using a computer. Their activities included browsing websites and checking emails. All participants indicated that they were very comfortable using a computer.

Sessions: We grouped participants into nine sessions. Sessions lasted between 30 to 60 minutes, and each session included two or three participants. We ensured that only one expert was included per session, therefore three sessions were a mix of experts and non-experts and six sessions consisted of only non-experts.

We introduced the purpose of the session, had participants sign consent forms, and described how the test sessions would be organized. We informed them that they could withdraw from the session at any point and the data collected about their performance would be discarded.

There are two major aspects of the game that we wanted to test. The first was whether the game instructions were clear and understandable. The second was playing the game. We wanted to see if the game strategy makes sense to the players, whether the game was fun and enjoyable, and whether it helped players learn about phishing attacks.



Fig. 4. The test environment.

Tasks: To test these aspects, we asked the participants in each session to perform two main tasks:

- Read and explain the game instructions. We asked participants to read the two pages of game instructions individually. Then we asked them as a group to explain the game to us. This allowed us to explore whether the written instructions were appropriate and to ensure that everyone understood the game correctly before playing.
- Play the game. We asked participants to play the game and provide feedback while they were playing. We gave them two options to finish this task: play to the end and declare a winner, or stop the game after 15 minutes if they did not want to continue.
- Setup: The experiment took place in our research lab, as shown in Figure 4. We set up the game board, cards, tokens, and die before the test sessions started. We provided paper and pens for note-taking, and we offered snacks to encourage a comfortable game-playing environment.

B. Data Collection

As this was our first test of the game, we were primarily concerned with collecting qualitative data about the experience and data indicating whether participants' knowledge of phishing had improved from playing the game. Four methods were used to collect the data.

Pre-test interview: We collected demographic information and the participant's levels of knowledge about phishing scams. Plus, the interview was used as an icebreaker to greet them and make them feel comfortable.

Observation: We observed participants while they read the instructions and played the game, and we asked them to provide any feedback as it occurred to them. We took notes of any comments made. We were interested in collecting data about the time they spent reading the game instructions, the time spent performing (understanding) the card tasks, the phishing scams that tricked them, and the phishing signs of which they were aware. We were also interested in gathering their

TABLE I
PRE-TEST KNOWLEDGE OF PHISHING.

Question	n	Response
Define phishing scam	8	Knew phishing related to identity theft
	5	Vaguely knew it was a security threat
	9	Were unable to define phishing
Identify protective actions against phishing	4	Use anti-phishing tools, pay attention to URLs and website content
	8	Use anti-virus
	9	Did not know how to protect themselves

feedback on the game components and how they interacted with them.

Post-test interview: We asked participants to reflect on their experience with the game, and their opinion of the tasks and instructions. In addition, we repeated the pre-test questions asking them to define phishing scams and identify protective behaviors to see if the game had enriched their knowledge. At the end of the interview, we asked for any additional comments or questions.

Questionnaire: We gave participants a questionnaire after the post-test interview. The questionnaire consisted of Likert-scale questions and was divided into three sections. The first section investigated perceived knowledge of phishing scams after playing the game; the second collected participants' feedback about the game; and the third gathered data about the different emotions the participants felt while playing the game and in different situations within the game. The questionnaire ended with two open-ended questions asking for suggested improvements to the game and asking to identify the best part of the game.

VI. RESULTS

A. Pre-test

The pre-test responses provided an idea of their pre-existing knowledge of phishing scams. As shown in Table I, participants initially had limited knowledge of phishing and how to protect themselves against this online threat.

B. Reading Instructions

We explored how long it took participants to familiarize themselves with the game, whether the instructions were understandable, and qualitative feedback for improvement.

Time: Participants spent an average of 10 minutes reading and understanding the game instructions.

Understandability: Out of nine groups, five were able to completely explain the instructions after reading them. Four groups understood the majority of the instructions but needed small clarifications. For example, one group missed the instruction detailing how to start the game but then knew how the turn-playing took place.

Feedback: 13 participants believed that the game instructions were straight-forward; however, they thought the instructions were quite long which made them hard to remember (two participants used scared and buzzed to express what they felt when they were reading them). One participant suggested having shorter sentences to facilitate understanding

and memorability, while three suggested offering a video demonstration of the game. Two suggested including diagrams. The six participants who were accustomed to playing board games said the instructions were fairly fine, clear and simple to follow.

While there are clearly improvements that could be done to the instructions on the next iteration, participants overall understood the game with little intervention and participants accustomed to turn-based board games thought that the instructions were adequate.

C. Playing the Game

Similarly, we looked at time and understandability in playing the game, the game's effectiveness with respect to the security content, and users' feedback.

Time: Groups played the game for 30-45 minutes and each challenge (Task card) took 60 to 90 seconds to complete.

Understandability: Seven groups were slightly confused about the starting point and determining who plays next. However, after the first round, they understood how to play and the game unfolded smoothly. Two groups played the game from start to finish without issue.

Four participants were confused about the role of the die within the game. The die was used to determine who is responsible for reading a Task card to the current player, rather than determining movements on the board. One group of participants ignored the die entirely and devised their own strategy for reading the cards.

Hint Cards: Response to the Hint cards was mixed. Three participants in three different sessions chose to pay for unlimited access to the Hint cards. Two participants each bought one pay-as-you-go Hint card. Two other participants did not understand the benefit of the Hint cards and chose to ignore them. The remainder strategically did not want to spend money paying for the Hint cards.

Police Cards: Three participants were particularly interested in the security advice and carefully explored the Police cards after each task. The others were primarily interested in the security advice to explore the reason for the punishment when they fell victim to phishing.

D. Recognition of threats

In each session, up to 18/24 Task cards were played. In total, 59 instances of Task cards containing phishing risks were played (with some repetition across sessions). Figure 5 illustrates the phishing characteristics that participants should have identified while playing the game. The horizontal axis represents these tricks while the vertical axis represents how many participants fell to or were aware of these tricks across all sessions. The red bars identify how many participants fell victim and failed to recognize the phishing attempt. The green bar indicates the number of participants that recognized the phishing trick and were able to take appropriate evasive action. For example, 13 task challenges relating to a change in domain name were played. Six participants fell victim to it, while seven participants correctly identified the threat.

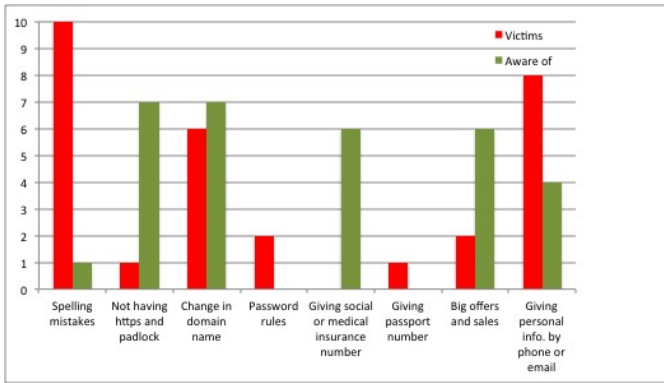


Fig. 5. Number of participants able to detect specific phishing characteristics.

Reassuringly, participants never fell victim to social insurance number or health insurance number tricks, although one participant shared their passport number. Most participants were also aware of having a secure https connection before giving their personal information.

Looking at the most effective phishing scams, 10 out of 11 participants who were exposed to spelling mistakes in the content of the Task card fell victim to it. Participants expressed surprise that this could be a sign that the website is illegitimate. The second most effective trick was a request to give personal information by phone or email, with 8 out of 12 participants unwittingly sharing information with an attacker.

In terms of the effectiveness of the game, approximately half of challenges resulted in participants falling victim, giving lots of opportunity for education and discussion surrounding the topic of phishing and protective behaviors. We view this as an indicator that the game difficulty is at an appropriate level. We observed increased engagement with the game and material as a result of the incorrect responses to challenges, especially when a player with high technical skill fell victim to an attack; the victim expressed disbelief while the other players found the situation quite humorous.

E. Participant feedback

We asked participants for feedback during and after game play. We received overall positive feedback about the game as well as some suggestions for improvement.

Almost all participants were satisfied with the game. They said it was fun, very good, educative, realistic, instructive and exciting. Given that this was the first iteration of the game, we feel that this is encouraging feedback.

Participants thought that the task challenges were feasible, easy to understand, and got directly to the point. Interestingly, one participant said that being in jail was very exciting because you have to wait for a round to know what kind of mistake you had made. This offers evidence that our game mechanics had some success at generating engagement and excitement.

Some participants expressed interest in an expanded version of the game. Six participants wished for more stores and a wider variety of tasks. One participant, who was a security

expert, said that the game demonstrates the real world challenges, while a second suggested different levels of challenges to more accurately simulate real life scenarios.

The majority of participants suggested that the game was suitable for players aged 12+ or 14+. Five participants thought that the game suited all ages and would be appropriate for anyone needing to learn the basics of phishing scams. Two participants believed that the game was appropriate for even young children because it could raise awareness of the risks associated with online shopping. However, we feel that the game requires a level of reading comprehension and digital literacy that may elude younger players; a modified version based on similar concepts could be possible for younger audiences.

We had carefully selected the name of our game and displayed it in several locations on the board, hoping it would resonate with players and that they would notice the spelling and play on words. However, most participants did not notice the meaning behind naming the game *Smells Phishy?* nor the way it was spelled (*\$me11s Ph!shy?*). Only three recognized the parallel with phishing and common phishing characteristics, such as having spelling mistakes and using numbers or other symbols instead of letters to imitate legitimate sites. We also observed the results of this inattention within the game — nearly half of participants fell victim to phishing scams involving spelling mistakes and a change in domain name.

F. Pre and Post Phishing Knowledge

Participants (including computer scientists) initially had fairly low levels of understanding of phishing and protective behaviors (Table I). After playing the game, all participants could define phishing as a way of tricking people to steal their identity and personal information for illegal use. When questioned about protective behaviors, participants now had much more complete answers. They mentioned paying close attention to the contents of websites and their domain names, looking for signs of SSL, and having anti-phishing tools. All participants had at least partial knowledge of appropriate protective actions. Participants were said to have accurate knowledge when they mentioned both tools to protect against phishing and specific user behaviors such as paying attention to the URL, SSL, and website content. We classified them as having partial knowledge when they mentioned either tools or user behaviors. Figure 6 highlights the improvement in knowledge.

G. Questionnaire

The post-test questionnaire contained Likert scale and open-ended responses. The focus of the questionnaire was to assess participants' perception and opinion of the game as well as collect further feedback about potential improvements. Likert-scale questions used a 5-point scale ranging from 1 = strongly disagree to 5 = strongly agree.

1) *Educational features:* The first section of the questionnaire inquired about the educational features of the game. The questions and their mean response out of 5 are available in

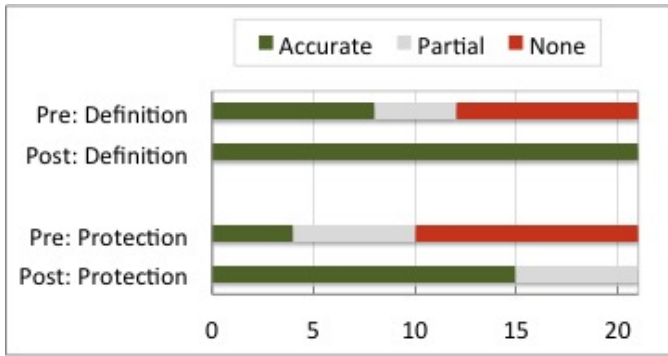


Fig. 6. Number of participants able to define phishing and identify protective actions before and after playing the game.

TABLE II
LIKERT QUESTIONS RELATING TO PHISHING EDUCATION; HIGHER MEANS INDICATES MORE POSITIVE RESPONSES.

Question	Mean
a) The game showed phishing tricks	4.5
b) I better understood phishing scams after playing the game	4.2
c) I will use the security advice mentioned in the game	4.5
d) It is important to follow the security advice provided in the game	4.6
e) I can better protect my credit card after playing the game	3.7
f) The game taught me how to protect myself from phishers	4.3
g) I learned something new	4.4

Table II. Figure 7 summarizes the distribution of responses for each question relating to security and phishing; responses were very positive. For example, more than half of participants strongly agreed that the game demonstrated phishing tricks and that they will use the security advice in real life.

The second set of questions related to participants' general opinion of the game. The questions are enumerated in Table III. Figure 8 illustrates the distribution of responses for questions (h) through (l) relating to general perception. The majority of the participants strongly agreed that the game was fun and that these types of games are important to facilitate teaching security.

However, responses were mixed in other respects. Most

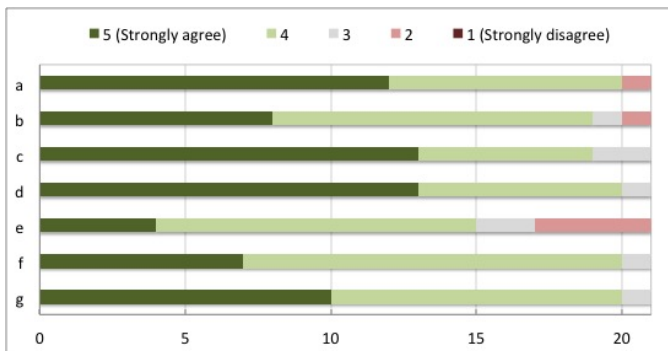


Fig. 7. Likert responses relating to phishing education.

TABLE III
LIKERT QUESTIONS RELATING OPINION OF THE GAME. QUESTIONS (J) AND (K) WERE REVERSE CODED; HIGHER MEANS INDICATES MORE POSITIVE RESPONSES.

Question	Mean
h) The game was fun	4.6
i) I would like to play the game again	4.2
j) The game is complicated	2.8
k) I prefer reading an educational document to playing a game to learn about phishing	3.7
l) Educational games are important to understand security	4.4

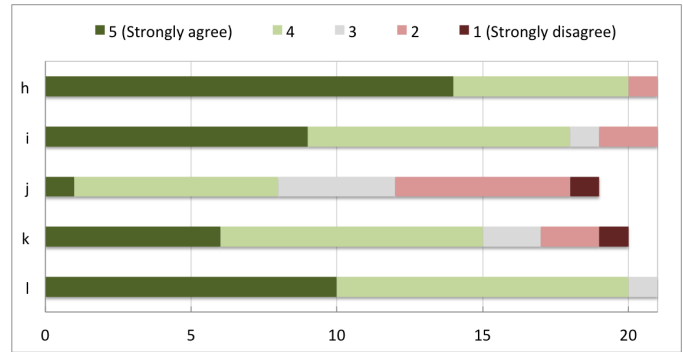


Fig. 8. Likert responses relating to opinion of the game. Questions (j) and (k) were reverse coded; higher means indicates more positive responses.

participants would prefer to play the game instead of reading an educational document about security, but approximately half thought the game was complicated.

2) *Emotional state*: We asked participants about their feelings and reactions at different times in the game. We were looking for a sense of whether participants were engaged. We would expect a variety of emotions, ranging from positive to negative, reflecting the circumstances of the game.

Figure 9 illustrates the participants' feelings while playing the game. All participants were either happy or excited except one who was neutral. After the game, the majority also expressed positive emotions. We note that not all participants responded to the losing money and jail scenarios because it did not necessarily apply to them. Of those who experienced these consequences, participants had mixed reactions. Two reported positive emotions, whereas most felt annoyed, angry,

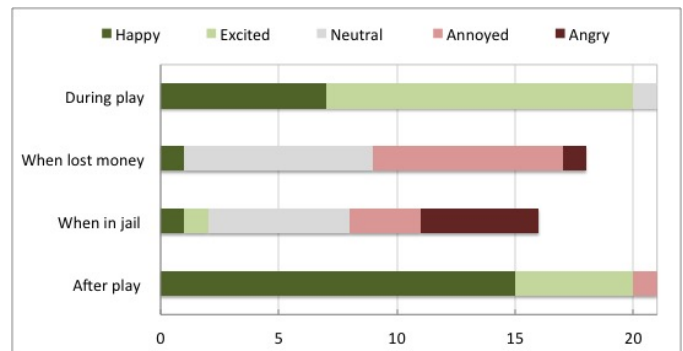


Fig. 9. Participants' emotional responses during play.

or ambivalent about the situation.

3) *Highlights and improvements:* The last section asked participants to highlight the best part of the game and provide any additional suggestions for improvement.

Participants highlighted various parts of the game as their favorite. Some mentioned items directly relating the game mechanics, suggesting that the game itself was appealing. Interestingly, some participants highlighted negative consequences within the game as particularly enjoyable. Three participants said being in jail was the best. Another three participants reported enjoying the feeling of suspense, falling victims to tricky tasks, and losing money.

Others focused on their sense of accomplishment and the positive consequences. Six said their favorite part was reading and performing the tasks, and completing the shopping list. One participant highlighted his sense of achievement when he received realistic problems and was able to detect the scam.

Participants had offered constructive feedback that will be helpful in the next iteration of the game. Seven participants suggested adding more tasks and shops with different levels of security challenges to make the game longer. One participant mentioned that if he played the game 2 or 3 times, he would know all the tricks and would not be excited to play again. While this is interesting, we would also see it as a positive result if a player had learned all of the educational material within the game because it would indicate that the game has served its intended purpose. Two proposed adding more variability and competitiveness within the game. They suggested allowing players to spontaneously modify the tasks presented so that it is more difficult for other players to pass the tasks successfully. This is also an interesting suggestion that has potential for increasing engagement, but it would need to be implemented very carefully so that users are still receiving appropriate educational feedback and security tips.

Three participants commented that the game is fun and very nice. Five thought that it was a very good educational tool. One suggested using it in a classroom environment: I can see it used in a school where students playing and learning is fun. Four participants wanted a digital version.

4) *Observations:* Players progressed through the game, we noted that they tended to learn from each other's mistakes. This is a desirable side effect of playing a board game and we hoped to find evidence of this. For example, participants sometimes responded quickly to tasks containing phishing tricks and correctly refused to complete the tasks; they had learnt to easily recognize these particular phishing tricks.

However, in a few instances, this led to unexpected consequences. We noted two participants who refused to fill a form while the domain name was correct and there were signs of a secure connection. Most likely, they chose this response because they saw that other players had accepted to fill forms and were sent to jail (because it was not secure to do so in that instance). As a result, they became suspicious of any task involving forms. While this is a prudent behavior, we hope that most participants would develop more refined critical thinking skills to assess the risk when faced with a new situation. In

these particular instances, the participants stopped accepting all vaguely similar tasks on suspicion that they were phishing traps even if they could not identify the reason why. We do not want to scare users away from all online interactions, but rather teach them to properly assess the situation.

VII. DISCUSSION

We designed and implemented a tabletop board game intended to teach players about phishing in an engaging manner. Overall, we are pleased with the results of this first iteration of the game, and with its ability to convey educational material.

A. Revisiting Our Design Objectives

Our design objectives were to teach about phishing, to do so in an entertaining manner, and to engage players in a dialog about phishing and protective actions.

Education: We saw a dramatic improvement in participants' ability to define phishing and identify protective actions. Initially, half of participants had at least partially correct responses. After playing the game, all participants could define phishing accurately and all could describe at least some countermeasures (Figure 6). Participant opinions also reflected the fact that the game provided useful educational information about security (Table II). Interestingly, the study shows that even skilled computer users learnt about phishing through our game (similarly found in [34]). In this sense, we feel that the educational objective was largely met, within the confines of our limited user testing.

Entertainment: We were pleased to observe participants engaged in the game and responding emotionally to the game mechanics (Figure 9). Participants positively commented on components of the game that were included specifically for their entertainment value, such as the jail and losing money. Participants also noted area of improvement and not all were completely sold on the idea of playing a game to learn about phishing. We feel that the game can be improved, but also note that it is unlikely that this educational format will please everyone.

Conversation-provoking: The sessions with security experts generated more discussion about phishing risks and tricks, after individual tasks and after the game. In sessions with non-experts only, participants seemed to be enjoying playing and having fun more than focusing on the security lessons (they just explored the security advice in the Police cards to see what went wrong). In most instances though, having the participants talk to each other and explain the tasks resulted in enriching the learning experience.

B. Areas of Improvement

Our participants offered suggestions for improvement and we noted others through our observations.

Instructions: One of the main issues, it seemed, is the game instructions. We found that the participants who were used to playing board games were fine with the length of the instructions; they reported that it is normal to have long game instructions and rules. Others, however, felt that the

instructions should be shortened. The security experts were most unhappy at the length of the instructions. We noticed that they tended to over-analyze the instructions and tried to immediately reveal in which ways they may represent the security concerns within the game. As a result of the instructions, participants were initially confused about turn-taking within the game (who is next, which way they should move, and when the game ends). We noticed that these points were not sufficiently and explicitly addressed in the game instructions.

Our game did not follow the conventional model of using the die to dictate movement on the board. Users' mental model clearly suggested using dice to specify how the player should move. A few times, participants rolled the die and wondered where they should move instead of using it to identify who should read the Task cards for them. In our next iteration, we will be revisiting the instructions to simplify them further and may explore the idea of a video demonstration. We will also reconsider the role of the die and may eliminate it to simplify the instructions.

Hint cards: Participants generally preferred taking risks rather than paying for Hint cards. While this may reflect real life attitudes towards security, it led to a potentially undesirable outcome for the game. The three who paid \$5 and got unlimited access to the Hint cards passed all their tasks successfully. However, they lost the game because someone else won a bonus for passing a difficult task. They were annoyed and regretted paying for the Hint cards, saying it is all about luck. We do not want players to leave with a negative impression of paying for external security help (such as anti-malware tools). Addressing this issue will be difficult; we want to leave some results to chance, to reflect the idea that despite your best intentions, sometimes attacks still occur and to keep this compelling element of gameplay (if buying the Hint cards always leads to success, the game will no longer be interesting). However, it may be possible to skew results slightly more in favor of those making smart security decisions.

C. Limitations

We conducted a user study with 21 participants, which provided us with important insight into the viability of the game, but further studies are needed to confirm that the results hold in other settings. The usual limitations apply with a sample of this size tested in a lab environment and with relatively well-educated participants. Furthermore, our interpretation of the players' actions may have been biased by our intimate knowledge of the game although we made every effort to remain objective.

VIII. CONCLUSION AND FUTURE WORK

Smells Phishy? is a tabletop board game that educates users about online phishing scams and how to avoid them. The goal of the game is to support secure online interaction by empowering users through knowledge. We made use of several game mechanics to increase engagement, including humor and

competition. The game was evaluated through a usability study with 21 participants who played the game in small groups. Participants found the game enjoyable and educational. Along with positive feedback, we found a significant improvement in participants' ability to define phishing and in identifying protective behaviors to avoid getting scammed. The game increased knowledge and awareness, and started conversations about phishing.

The results of the study were encouraging and we intend to further develop the game. For future work, we are planning to simplify the game instructions to make it easier for players to understand and memorize. We also intend to expand the game by adding more stores, more items to the shopping lists, and more tasks. We will include different difficulty levels for the Task cards to further challenge the security knowledge of the players. In addition, we are planning to improve the evaluation strategy by engaging more participants representing different populations, and to investigate the influence of the game not only on participant's knowledge, but also on their behavior, when compared to a text-based control condition. After refinement, we will explore making a printable version of the game available to the public.

ACKNOWLEDGMENT

We would like to thank Dr. Daniel Amyot and the King Abdullah Scholarship Program (KASP) for supporting this research. S. Chiasson acknowledges funding from NSERC for her Canada Research Chair and Discovery Grant.

REFERENCES

- [1] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006, pp. 581–590.
- [2] "Anti phishing working group," <https://apwg.org>.
- [3] EMC, "2013 a year in review," <http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf>.
- [4] Y. Zhang, S. Egelman, L. Cranor, and J. Hong, "Phishing phish: Evaluating anti-phishing tools," in *Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS)*, 2007.
- [5] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proceedings of the 2009 workshop on New security paradigms workshop*. ACM, 2009, pp. 133–144.
- [6] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 2010, p. 11.
- [7] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, 2012.
- [8] G. Aaron, "The state of phishing," *Computer Fraud & Security*, vol. 2010, no. 6, pp. 5–8, 2010.
- [9] A. Bergholz, J. De Beer, S. Glahn, M.-F. Moens, G. Paaß, and S. Strobel, "New filtering approaches for phishing email," *Journal of computer security*, vol. 18, no. 1, pp. 7–35, 2010.
- [10] C. Whittaker, B. Ryner, and M. Nazif, "Large-scale automatic classification of phishing pages," in *NDSS*, vol. 10, 2010.
- [11] T. Moore and R. Clayton, "Examining the impact of website take-down on phishing," in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*. ACM, 2007, pp. 1–13.
- [12] NSS Labs, "Evolutions in browser security: Trends in browser security performance," <http://www.phishtank.com/>, 2014.
- [13] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007.

- [14] R. T. Wright and K. Marett, "The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived," *Journal of Management Information Systems*, vol. 27, no. 1, pp. 273–303, 2010.
- [15] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Systems*, vol. 51, no. 3, pp. 576–586, 2011.
- [16] J. Epstein, "Phishing our employees." *IEEE Security & Privacy*, vol. 12, no. 3, pp. 3–4, 2014.
- [17] T. Denning, A. Lerner, A. Shostack, and T. Kohno, "Control-alt-hack: the design and evaluation of a card game for computer security awareness and education," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 915–928.
- [18] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, p. 7, 2010.
- [19] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 373–382.
- [20] "Recognizing spoof (fake) ebay websites," <http://pages.ebay.com/help/account/recognizing-spoof.html>.
- [21] "What to do and how," <http://www.consumer.gov>.
- [22] Government of Canada, "Get cyber safe," <http://www.getcybersafe.gc.ca/>.
- [23] P. Kumaraguru, "Phishguru: a system for educating users about semantic attacks," Ph.D. dissertation, Carnegie Mellon University, 2009.
- [24] "d0x3d!" <http://www.d0x3d.com>.
- [25] L. Williams, A. Meneely, and G. Shipley, "Protection poker: The new software security," *IEEE Security & Privacy*, no. 3, pp. 14–20, 2010.
- [26] Microsoft, "Elevation of privilege," <http://www.microsoft.com/security/sdl/adopt/eop.aspx>.
- [27] "OWASP cornucopia," http://www.owasp.org/index.php/OWASP_Cornucopia.
- [28] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "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, 2007, pp. 88–99.
- [29] N. A. G. Arachchilage, S. Love, and M. Scott, "Designing a mobile game to teach conceptual knowledge of avoiding phishing attacks," *International Journal for e-Learning Security*, vol. 2, no. 2, pp. 127–132, 2012.
- [30] M. Thompson and C. Irvine, "Active learning with the cyberciege video game," in *CSET'11 Proceedings of the 4th conference on Cyber security experimentation and test*, 2011, pp. 10–10.
- [31] A. Repenning and C. Lewis, "Playing a game: The ecology of designing, building and testing games as educational activities," in *ED-Media, World Conference on Educational Multimedia, Hypermedia & Telecommunications*, 2005.
- [32] "Gamification," <http://badgeville.com/wiki>.
- [33] T. Fullerton, *Game design workshop: a playcentric approach to creating innovative games*. CRC press, 2014.
- [34] M. Blythe, H. Petrie, and J. A. Clark, "F for fake: four studies on how we fall for phish," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 3469–3478.