



GAP: A Game for Improving Awareness About Passwords

Harshal Tupsamudre¹(✉), Rahul Wasnik², Shubhankar Biswas²,
Sankalp Pandit¹, Sukanya Vaddepalli¹, Aishwarya Shinde¹, C. J. Gokul¹,
Vijayanand Banahatti¹, and Sachin Lodha¹

¹ TCS Research, Pune, India

{harshal.tupsamudre,pandit.sankalp1,sukanya.vaddepalli,
aishwarya.ashinde,gokul.cj,vijayanand.banahatti,sachin.lodha}@tcs.com

² IIT Bombay, Mumbai, India

{rahulwasnik,shubhankarbiswas}@iitb.ac.in

Abstract. Text-based password is the most popular method for authenticating users on the internet. However, despite decades of security research, users continue to choose easy-to-guess passwords to protect their important online accounts. In this paper, we explore the potential of serious games to educate users about various features that negatively impact password security. Specifically, we designed a web-based casual game called *GAP* and assessed its impact by conducting a comparative user study with 119 participants. The study results show that participants who played *GAP* demonstrated improved performance in recognizing insecure password features than participants who did not play *GAP*. Besides having educational value, most of the participants also found *GAP* fun to play.

Keywords: Serious games · Passwords · Security · Human factors

1 Introduction

Security studies show that users choose predictable passwords to protect even their important accounts [10, 16]. Majority of passwords are either short or composed using dictionary words, lowercase letters and digits *e.g.*, *princess*, *password* and *123456*. As a result, many websites including banking and social-networking services mandate users to include capital (uppercase) letters, symbol and digits in their password for improved security. However, users respond to this requirement by placing capital letters, digits and symbols at predictable positions, mostly at the beginning or at the end of the password, thus affecting the password security [7, 25, 28]. We refer to passwords resulting from such popular strategies as “insecure passwords”.

Several studies in the past have shown that serious games can be effective tools for training and encouraging behaviour change. For instance, Sheng *et*

al. [26] designed an online game called *Anti-Phishing Phil* to teach users to recognize phishing websites while Denning *et al.* [8] designed a card game called *Control-Alt-Hack* to raise awareness about computer security concepts. An evaluation of both these games indicate that educational games are not only more effective in terms of learning, but they are also more engaging and fun as compared to traditional approaches such as reading training materials.

Playing computer games is linked to a range of perceptual, cognitive, behavioural, affective and motivational impacts and outcomes [6]. Games provide situated experiences where players are immersed in complex, problem solving tasks [27]. Games are more engaging as they incorporate a number of strategies and tactics in gameplay [9]. Games facilitate procedural learning by providing the player appropriate and immediate feedback through game elements such as game points, progress bar and messages [24]. Further, games seem to have an advantage when it comes to retention of newly gained information as compared to conventional methods [30].

The use of games as a security training tool is an emerging idea not only in academia but also in the industry [13]. In fact there are commercial games developed by Wombat [21], NPS [19] and others to educate users about various security threats including virus, Trojan horse and phishing. However, relatively less work has been done in the context of passwords. In this work, we explore the use of serious games to educate users about insecure passwords. Since what characteristics constitute a secure password is not fully agreed upon [4], we focus only on educating users about insecure password creation strategies. We designed a web-based casual password awareness game called *GAP* and gauged its effectiveness by conducting a study with 119 participants. The study results indicate that participants who played *GAP* performed much better in identifying insecure password practices than those who did not play the game.

The organization of this paper is as follows. First, we describe the design and mechanics of the *GAP* game. Subsequently, we explain our study methodology and survey results. Finally, we conclude the paper by proposing an extensible and modular game framework for creating educational games for passwords.

2 GAP: A Password Awareness Game

In this section, we describe the design and rationale of *GAP*, a game to educate users about insecure password creation strategies. First, we explain how we derived the educational content for the game. Next, we illustrate the gameplay followed by the justification for choosing the casual game genre. Later, we describe the design principles and technology used to develop the *GAP* game.

2.1 Game Content

Previous password studies show that users place capital letters, symbols and digits at predictable positions in the password. For instance, a study [25] that surveyed university students, faculty and staff found that 55.8% of the users place

symbol at the last position, 74.2% of the users place capital letter at the first position and 34.9% users place digit at the last position of their password. Similarly, another study [7] that surveyed users at different universities to understand their password composition found that 44% of the users place capital letters at the beginning, 44% users place symbol at the end, 13% users place symbol at the beginning, 54% users place digits at the end, and 16% users place digit at the beginning of the password. Typical examples of such passwords are *football!*, **football*, *basketball1* and *2basketball*.

To emphasize the fact that composing passwords using a single character class does not provide enough security, we consider an additional insecure strategy where all letters of a password are capital, *e.g.*, BASEBALL. Therefore, in the current version of the game, we focus on educating users about the following six insecure password creation strategies.

1. *use of capital letters at the beginning of the password*
2. *use of only capital letters in the password*
3. *use of digits at the beginning of the password*
4. *use of digits at the end of the password*
5. *use of symbols at the beginning of the password*
6. *use of symbols at the end of the password*

We analysed publicly available password databases [3] to learn about the popular symbol and digit that users add at the beginning and at the end of the password. Our analysis revealed that ‘!’ is the most popular symbol used at the end and ‘*’ is the most popular symbol used at the beginning of the password. Further, ‘1’ is the most popular digit that is used at the beginning as well as at the end of the password. Since the passwords in the RockYou dataset were not created using any composition policy, we estimate the popularity of each of these operations by referring to the findings of a real-world password study [25].

2.2 Game Mechanics

The game world of *GAP* consists of a tank and barriers interspersed on the maze as shown in Fig. 1. Each barrier is labelled with an insecure password obtained by modifying the baseword *princess* with operations listed in Table 1. Presently, the game world consists of six barriers, one corresponding to each insecure operation. The goal of the player is to exit the maze by destroying all six barriers (insecure passwords) along the path.

The controls used in the game are simple (Fig. 2). The movement of the tank is controlled using left and right arrow keys and the movement of the turret is controlled using the mouse. The player rotates the turret to aim at the barrier and clicks the left-button of the mouse to release the ammunition. There are three types of ammunitions out of which the player has to choose the right one depending on the password label of the barrier. For instance, to destroy the barrier labelled with a password that starts or ends with a digit, the right ammunition is loaded by pressing letter **D** on the keyboard. If a wrong

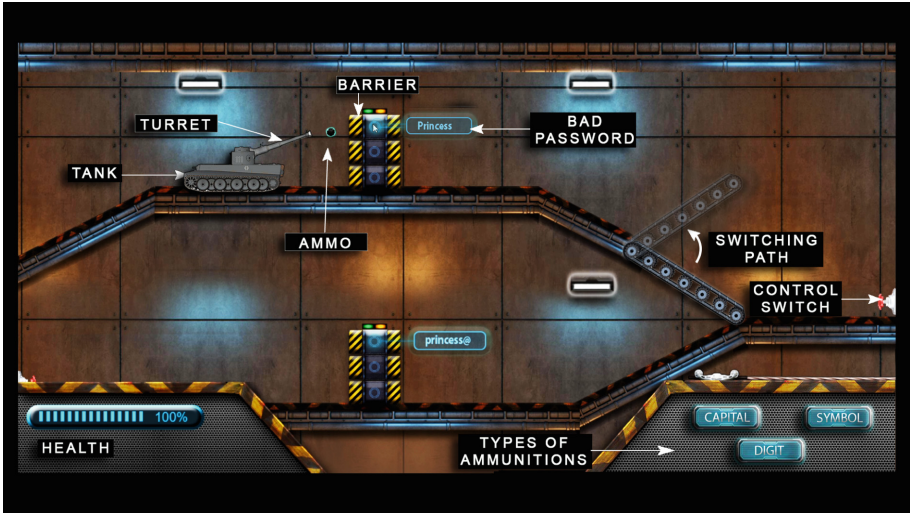


Fig. 1. The interface of GAP, a web-based game to educate players about insecure password creation strategies. The labels in this image are not part of the game and are for understanding purposes only.

ammunition is fired, the health of the tank decreases and the barrier remains unaffected. To make the game more challenging, the maze consists of switching paths that can be re-positioned using a control switch. The player is required to open a new path for navigating the tank through the maze by hitting the control switch with the tank. The information about the rules and controls is provided to the player before the start of the game.



Controls	Action Performed
→	Move the tank Right
←	Move the tank Left
C key	Select Capital Ammunition
S key	Select Symbol Ammunition
D key	Select Digit Ammunition
	To Aim the at the Barrier
	To Shoot the Barrier

Fig. 2. Controls for navigating tank and selecting ammunition in the GAP game.

In short, the game requires the player to look at the password label (*princess1*), identify insecure operation (digit at the end) and choose the right ammunition (key D) to destroy the barrier. Shooting barriers labelled with

Table 1. The list of insecure operations and corresponding examples along with the correct key for loading ammunition.

Insecure operation	Example	Ammunition
Capital at start	Princess	C key
Capitals only	PRINCESS	C key
Symbol at end	princess!	S key
Symbol at start	*princess	S key
Digit at end	princess1	D key
Digit at start	2princess	D key

insecure passwords signify to the player that such passwords should never be used to protect their online accounts.

2.3 Training Messages

When the player destroys the barrier with the right ammunition, we display certain facts about the insecure password with which the barrier was labelled (Figs. 3 and 4). The purpose of the facts is to make the player aware of how insecure the particular operation is. For instance, if the barrier is labelled with a password that begins with a capital letter (*e.g.*, *Princess*), we display the fact: “More than 70% of the users keep a capital letter in the first position of their password. Hence, it is an insecure practice” and if the barrier is labelled with a password that ends with a symbol (*e.g.*, *princess@*), we display the fact: “More than 50% of the users keep symbol in the last position of their password. Hence, it is an insecure practice.” For the current version of the game, we borrowed these facts from the findings of a real-world password study performed by CMU researchers [25].

**Fig. 3.** Fact presented when barrier labelled with insecure password *princess* is shot.



Fig. 4. Fact shown when barrier labelled with insecure password *princess@* is shot.

2.4 Game Genre

As passwords are created by users with diverse backgrounds, making a suitable choice of game genre that teaches users about insecure passwords is critical. We wanted the game to be simple, yet capable of teaching the concept in an impactful manner. Therefore, we designed *GAP* to be a slow-paced casual game that simulates an “escape situation”, where the player controls a tank and the objective is to navigate the tank through the maze by demolishing barriers (labelled with insecure passwords) placed along the way. The *GAP* game is web-based (can be played using a web browser), uses simple game controls, has a short gameplay time (less than five minutes) and does not assume any prior experience in gaming.

Casual games are one of the fastest growing segments within the industry [1, 17]. These games are characterized by less complex game controls, faster rewards and shorter gameplay time [15]. As casual games are easy to learn and simple to play, they appeal to users with different age-groups [5]. Further, according to one report, 50% of the casual game players are females [18]. Casual games are mostly available in web-based or mobile-based versions and come in a wide range of genres. Typical examples of casual genre are Pacman, Tetris, Solitaire and Candy Crush. Casual games have been successfully explored in the healthcare domain [11, 12]. In this work, we explore the potential of casual games in the security domain.

GAP also exhibits certain characteristics of escape-the-room genre, as the goal of the player is to escape the maze by overcoming obstacles placed along the path. Research shows that escape rooms (maze) are experiential, encourage players to think creatively and engage in critical thinking. The escape-the-room games often consist of puzzles that run in a simple game loop [29]. In the case of *GAP*, the loop consists of the following three steps:

1. Challenge (shooting barrier labelled with insecure password using right ammunition)
2. Solution (a feedback message indicating the potential risk of using insecure password)

3. Reward (the ability to move forward thereby closing in towards the end of the maze)

Escape-the-room genre games make use of (horror) elements to add a sense of urgency to escape. On the contrary, we designed *GAP* to be slow paced where players have a chance to stop and reflect on the new knowledge they have learned.

2.5 Design Principles

We applied two principles from the learning sciences theory to design the *GAP* game: reflection and contextual-procedural.

- *Reflection Principle*. According to this principle [2], learning increases if the learners are given an opportunity to stop and think about what they are learning. This principle is employed in the *GAP* game as we display appropriate factual training messages to the player after destroying the barrier and also after the end of the game.
- *Conceptual-Procedural Principle*. According to this principle [23], conceptual and procedural knowledge influence one another in mutually supportive and integrated ways. This principle is employed in our game since we label each barrier with distinct example (*e.g.*, *princessI*) to teach players about the concept of insecure passwords. To destroy the barrier, the player has to identify the insecure operation (*e.g.*, digit at end) and choose the right ammunition (*e.g.*, **D**) as shown in Table 1. To reinforce the learned concept, we also provide clear procedural tips to the player (*e.g.*, “adding digits at the end of the password is an insecure practice”) after the barrier is destroyed.

2.6 Technology Used

We created static images and sprite sheets for the *GAP* game using Adobe Photoshop. The two popular options for creating web-based games are Flash and HTML5. However, Flash is a proprietary software, it is not supported on all devices (*e.g.*, iPhones and iPads) and it has potential security issues. On the other hand, HTML5 and javascript are open standards and supported by all browsers and devices [22]. Therefore, the entire game was developed using HTML5, CSS3 and Phaser javascript library [20]. All the images, libraries and assets required for playing *GAP* were fetched from the server only once before the start of the game to give an uninterrupted gameplay experience to the players. The survey responses of participants were captured using J2EE application server and stored in PostgreSQL database.

3 User Study

To assess the impact of the *GAP* game, we designed a survey questionnaire which consists of the following two parts.

1. In *part 1* of the survey, we asked participants questions related to demographic characteristics *i.e.*, gender, age, education and specialization.
2. In *part 2* of the survey, we asked participants to identify *insecure positions* for adding a symbol, a digit and a capital letter in the password. These questions are listed below.
 - (a) *When adding a capital letter to the password, which of the following is/are insecure practices? (Check all that apply)*
 - *Adding a capital letter at the beginning*
 - *Adding a capital letter at the end*
 - *Adding a capital letter in the middle*
 - *Using only capital letters*
 - *Other*
 - (b) *When adding a symbol to the password, which of the following is/are insecure practices? (Check all that apply)*
 - *Adding a symbol at the beginning*
 - *Adding a symbol at the end*
 - *Adding a symbol in the middle*
 - *Other*
 - (c) *When adding a digit to the password, which of the following is/are insecure practices? (Check all that apply)*
 - *Adding a digit at the beginning*
 - *Adding a digit at the end*
 - *Adding a digit in the middle*
 - *Other*

3.1 Experiment Groups

We conducted a comparative user study to evaluate the impact of *GAP* on the performance of its users. All participants were randomly assigned to either of the two experimental groups: *control group* or *game group*.

1. *Control group*. In this group, participants were asked to answer the survey questionnaire without being exposed to any kind of training.
2. *Game group*. In this group, participants were asked to answer the survey questionnaire after playing the *GAP* game. In addition to the *part 1* and *part 2* of the survey, participants in the game group were also asked the following open-ended questions regarding the game.
 - *How much fun was the game?*
 - *Did you have any trouble or difficulties while playing the game?*
 - *Are there any possible improvements in the game?*

We measure the impact of *GAP* by comparing the survey responses of participants in the control group and game group. As described earlier, the *part 2* of the survey asks participants to identify insecure positions for adding a digit, a symbol and capital letter in a password. Participants in the game group, responded to the *part 2* of the survey after playing the *GAP* game whereas participants in the control group responded to the *part 2* without playing the game. Therefore, we can observe whether the training messages embedded in the game improved the performance of participants in identifying insecure password practices.

Table 2. Participant demographics in the control group and game group.

	Control	Game
Gender		
Male	65.57%	70.69%
Female	34.43%	29.31%
Age		
18–24	75.41%	75.86%
25–34	24.59%	24.14%
Education		
Bachelors	54.10%	51.72%
Masters	40.98%	44.83%
Doctorate	4.92%	3.45%
Major		
CS	49.18%	51.72%
Non-CS	50.82%	48.28%
#Participants	61	58

3.2 Demographics

We recruited 119 participants within our organization through the use of internal mailing lists. They were assigned randomly to either control group or game group. Table 2 summarises the demographics of participants in each group. Most participants were young and had a bachelor’s degree. We found no significant difference in gender, age or education between the control group and game group.

4 Results

After analysing survey responses, we found that participants who played the *GAP* game performed better in correctly identifying insecure password practices than participants in the control group. In particular, participants in the game group performed much better in correctly recognizing that adding a capital letter in the beginning, using only capital letters, adding a symbol at the end and adding a digit at the end are insecure practices. In the remaining cases, participants in the game group performed at least as good as participants in the control group.

To determine whether the difference between the performance of participants in the control group and game group is significant, we perform a two-tailed Fischer’s Exact Test (FET). In this case, the variable of interest is whether participants correctly recognized insecure password operations or not. We claim the result to be statistically significant if $p < 0.01$ and we indicate possible significant interest if $p < 0.10$. The results of statistical tests are summarized

Table 3. Proportion of participants who correctly identified insecure password creation practices. The results of statistical tests (FET) are also given.

Question	Control	Game	p-value
Capital - adding at beginning	57.38%	93.10%	<0.0001*
Capital - only capital letters	62.30%	82.76%	0.0147**
Symbol - adding at beginning	70.49%	81.03%	0.2051
Symbol - adding at end	63.93%	79.31%	0.0711**
Digit - adding at beginning	55.74%	68.97%	0.1855
Digit - adding at end	54.10%	87.93%	<0.0001*

in Table 3. We marked the entry with value $p < 0.01$ in the table using (*) and $p < 0.10$ using (**).

We found highly significant difference between the performance of control group and game group participants in recognizing two insecure operations, adding a capital letter at the beginning and adding a digit at the end ($p < 0.0001$). Further, we found significant interest in the performance of control group and game group participants in recognizing two other insecure operations, adding a symbol at the end and using only capital letters ($p < 0.10$). We note that adding capital letter at the beginning and adding digit (or symbol) at the end are the most popular operations [7, 25, 28]. The difference in performance between the two groups in recognizing these insecure operations was either statistically significant ($p \ll 0.01$) or had significant interest ($p < 0.10$). There was no statistical difference between the performance of the two groups in recognizing remaining two insecure operations, adding a symbol at the beginning or adding a digit at the beginning ($p \geq 0.10$), but the proportion of participants who answered correctly is higher in the game group as compared to the control group.

4.1 Game Feedback

The average time required to complete the GAP game was about 3.5 min. The analysis of the game feedback revealed that 81.03% of the participants found the game to be fun while 6.90% of the participants felt otherwise. The remaining 12.07% of the participants remained neutral. When it comes to difficulty, 77.59% of the participants felt that the game was not difficult to play while 18.97% participants reported difficulty in playing the game. Of these 18.97% participants, 12.07% participants reported difficulty in understanding the game instructions and 6.90% participants reported difficulty in understanding the game controls. The rest 3.45% of the participants remained neutral (Table 4).

Overall, we got positive response from the participants for using the game as a training tool. One participant remarked, “*The idea of educating people with the help of game was a very good idea.*” Another participant remarked, “*An interesting way to teach what is important and what is not*”. We also received few

Table 4. Feedback about the *GAP* game.

Question	Yes	No	Neutral
Game is fun	81.03%	6.90%	12.07%
Game is difficult	18.97%	77.59%	3.45%

suggestions from participants for improving the *GAP* game. These suggestions mainly include replacing text instructions with a demo video and adding more challenging tasks to the game.

5 Conclusion and Future Work

In this paper, we developed a web-based casual game called *GAP* with an objective of educating users about various insecure password practices. We also assessed its impact by conducting a user study with 119 participants. Our study results show that participants who played *GAP* showed improved awareness of the insecure password practices. Specifically, about 93% of the participants who played the game correctly identified that adding capital letter at the beginning of the password is an insecure practice, about 81% of the participants correctly identified that adding symbol at the beginning is an insecure practice and about 88% of the participants correctly identified that adding digit at the end is an insecure practice. Further, most participants found the game to be fun and completed the gameplay within a short duration of time (less than four minutes).

Currently, the educational content used in the game is derived from external sources (mostly from password research studies [7, 25]). Another possibility is to tap into real-world publicly available password sources [3, 14] to learn about emerging popular passwords and patterns, and extend *GAP* with more insecure operations. However, the *GAP* game in its current state require changes to the code to support new insecure operations. We plan to make our game code more modular and flexible so that it can be extended to support other insecure operations with minimum effort. This would particularly benefit organizations that may want to customize the *GAP* game to train their employees.

Many organizations enforce stringent password expiry policies mandating employees to change their password after few months. Employees typically circumvent such policies by appending the current month (01–12) to their password. Consequently, the organization wishes to educate their employees about the negative consequences of using month in their password through the *GAP* game. To support a new insecure operation, the code of the *GAP* game needs to be altered with an example of insecure password, training message, new type of ammunition and new control key, this can be restrictive. We envision a separate data module which can be configured with an insecure password (e.g., *Princess07*), appropriate training message, ammunition (e.g., MONTH) and control key (e.g., M) before playing the game. Instead of using the same baseword *princess* every-time, the data module can also choose a new baseword at random from the list

of breached lowercase alphabetic passwords. Upon initialization, the *GAP* game accesses the data module, reads the game content and configures the gameplay accordingly. We aim to explore this framework further in our future studies.

References

1. Casual Games Association: Casual Games Sector Report. http://cdn2.hubspot.net/hubfs/700740/Newzoo_Games_Industry_Growth_Towards_2017.pdf. Accessed 10 August 2018
2. National Research Council, et al.: *How People Learn: Bridging Research and Practice*. National Academies Press, Washington, D.C. (1999)
3. Bowes, R.: Passwords. <https://wiki.skullsecurity.org/Passwords>. Accessed 10 August 2018
4. de Carné de Carnavalet, X., Mannan, M.: From very weak to very strong: analyzing password-strength meters. In: NDSS 2014. Internet Society (2014)
5. Chesham, A., Wyss, P., Müri, R.M., Mosimann, U.P., Nef, T.: What older people like to play: genre preferences and acceptance of casual games. *JMIR Serious Games* **5**(2), e8 (2017)
6. Connolly, T.M., Boyle, E.A., MacArthur, E., Hainey, T., Boyle, J.M.: A systematic literature review of empirical evidence on computer games and serious games. *Comput. Educ.* **59**(2), 661–686 (2012)
7. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X.: The tangled web of password reuse. In: NDSS 2014, pp. 23–26. Internet Society (2014)
8. Denning, T., Lerner, A., Shostack, A., Kohno, T.: Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In: CCS 2013, pp. 915–928 (2013)
9. Dickey, M.D.: Engaging by design: how engagement strategies in popular computer and video games can inform instructional design. *Educ. Technol. Res. Dev.* **53**(2), 67–83 (2005)
10. Florencio, D., Herley, C.: A large-scale study of web password habits. In: WWW 2007, pp. 657–666 (2007)
11. Gerling, K., Fuchslocher, A., Schmidt, R., Krämer, N., Masuch, M.: Designing and evaluating casual health games for children and teenagers with cancer. In: Anacleto, J.C., Fels, S., Graham, N., Kapralos, B., Saif El-Nasr, M., Stanley, K. (eds.) ICEC 2011. LNCS, vol. 6972, pp. 198–209. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24500-8_21
12. Grimes, A., Kantroo, V., Grinter, R.E.: Let’s play! Mobile health games for adults. In: Ubicomp 2010, pp. 241–250. ACM (2010)
13. Hendrix, M., Al-Sherbaz, A., Victoria, B.: Game based cyber security training: are serious games suitable for cyber security training? *IJSG* **3**(1), 53–61 (2016)
14. Hunt, T.: Pwned passwords. <https://havebeenpwned.com/Passwords>. Accessed 10 August 2018
15. Kuittinen, J., Kultima, A., Niemelä, J., Paavilainen, J.: Casual games discussion. In: Proceedings of the 2007 Conference on Future Play, pp. 105–112. ACM (2007)
16. Mazurek, M.L., et al.: Measuring password guessability for an entire university. In: CCS 2013, pp. 173–186. ACM (2013)
17. Morrison, C.: Casual Gaming Worth \$2.25 Billion, and Growing Fast. <https://venturebeat.com/2007/10/29/casual-gaming-worth-225-billion-and-growing-fast/>. Accessed 10 August 2018

18. NPD: The NPD Group: 37 Percent of U.S. Population Age 9 and Older Currently Plays PC Games. <https://www.npd.com/wps/portal/npd/us/news/press-releases/37-percent-of-us-population-age-9-and-older-currently-plays-pc-games/>. Accessed 10 August 2018
19. NPS: Cyberciege (2004). <http://my.nps.edu/web/cisr/cyberciege>. Accessed 10 August 2018
20. Phaser: Desktop and Mobile HTML5 Game Framework. <https://phaser.io>. Accessed 10 August 2018
21. ProofPoint: Wombat Security Technologies. <https://www.wombatsecurity.com/>. Accessed 10 August 2018
22. Reimers, S., Stewart, N.: Presentation and response timing accuracy in Adobe Flash and HTML5/JavaScript web experiments. *Behav. Res. Methods* **47**(2), 309–327 (2015)
23. Rittle-Johnson, B., Koedinger, K.R.: Comparing instructional strategies for integrating conceptual and procedural knowledge (2002)
24. Schroth, M.L.: The effects of delay of feedback on a delayed concept formation transfer task. *Contemp. Educ. Psychol.* **17**(1), 78–82 (1992)
25. Shay, R., et al.: Encountering stronger password requirements: user attitudes and behaviors. In: SOUPS 2010, pp. 2:1–2:20 (2010)
26. Sheng, S., et al.: Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In: SOUPS 2007, pp. 88–99 (2007)
27. Squire, K.D.: Video game-based learning: an emerging paradigm for instruction. *Perform. Improv. Q.* **21**(2), 7–36 (2008)
28. Ur, B., et al.: “I added ‘!’ at the end to make it secure”: observing password creation in the lab. In: SOUPS 2015, pp. 123–140. USENIX Association (2015)
29. Wiemker, M., Elumir, E., Clare, A.: Escape room games. *Game Based Learn.* (2015)
30. Wouters, P., Van Nimwegen, C., Van Oostendorp, H., Van Der Spek, E.D.: A meta-analysis of the cognitive and motivational effects of serious games. *J. Educ. Psychol.* **105**(2), 249 (2013)