*Game On: Teaching Cybersecurity to Novices Through the Use of a Serious Game**

Devorah Kletenik, Alon Butbul, Daniel Chan, Deric Kwok, Matthew LaSpina
Department of Computer and Information Science
Brooklyn College, City University of New York
Brooklyn, NY 11210
kletenik@sci.brooklyn.cuny.edu

Abstract

We report on the creation of an educational serious game to teach basic cybersecurity concepts. *Cyber Secured* uses engaging gameplay and challenges to educate students about concepts such as phishing, malware, encryption and passwords. This game was evaluated on introductory students in three sections of an e-commerce course. Our analysis demonstrated statistically significant learning gains as well as continued retention of the material. We also saw evidence of increased interest in cybersecurity, and reports of positive attitudes towards the use of this game to teach and assess cybersecurity material. The results of our work suggest that *Cyber Secured* is a useful tool to educate about cybersecurity, and we have made our game freely available.

1 Introduction

Cybercrime poses a threat to both our society and economy. An increasing awareness of human users as the "weakest link" compels building awareness and educating Internet users about cybersecurity. Many different types of training sessions and exercises have been conducted on a variety of Internet users. In this work, we discuss our use of a serious game to educate college students who are new to the field of cybersecurity.

Over the past two decades, there has been a growing interest in creating educational "serious games" that help students learn by offering an engaging alternative or supplement to traditional lectures. Research suggests that serious games are superior at teaching subject matter compared to traditional means of instruction and increase long-term retention and student motivation (e.g. [7, 12]). A number of serious games have been created to teach cybersecurity concepts, including digital games, card games and Capture the Flag competitions. These games offer engaging ways to teach about cybersecurity and increase student interest.

However, many of these games are geared towards those who are already knowledgeable about cybersecurity. When novices to the field are overly challenged by cybersecurity games, they may have poor learning outcomes and possibly exhibit counteractive decreased interest in cybersecurity [8]; as a result, it is important to achieve game balance by matching the game topics to the players' backgrounds. We address this problem by creating a game geared specifically to cybersecurity beginners; in fact, to students who may not have any computer science background at all. Our goal is not to educate the next generation of security professionals, but to inform lay people about online risks, spark interest in the topic and motivate learning more.

2 Related Work

Perhaps the most well-known cybersecurity game is the *CyberCIEGE* game. Players assume the role of an IT decision maker for a small business in a 3D office environment. Scenarios challenge the players to make security decisions and depict realistic tradeoffs and risk management. The scenarios educate about concepts such as encryption, DMZ, and patches [5]. *CyberCIEGE* has been tested in a number of computer security courses (e.g. [10]).

Another cybersecurity game, *Cash City*, teaches about cybersecurity in a digital Monopoly-style game. The game was evaluated on first-year IT students and showed modest improvement for the game-playing group over a control group [6]. [d0x3d!][1] is a tabletop card game that is open-source and available for downloading and remixing. It has been assessed in a number of field tests and has received positive feedback [2]. Several games have been created to specifically focus on phishing awareness, e.g. [9, 11, 1]. A survey of cybersecurity games, both those reported about in academic literature and those created by private industry, is discussed in [4].

3 The Game

In the game, which is loosely based on the Game *Spent*[2], the player has been hired as an IT specialist. S/he must then navigate through routine challenges and learn along the way: each "month" in the game contains specific learning modules which the player must successfully navigate, based on the learning goals summarized in Table 1. Players are given a brief tutorial and then have to use the information to succeed at a related quiz or challenge: for example, crafting a password and then seeing how strong it is, determining whether an email is a phishing scheme, encrypting and decrypting using a variety of encryption methods, and making various security choices for the company (e.g. choice of backups for sensitive data), as well as short multiple-choice quizzes.

Along the way, the player is also informed about random events that happen to the company, both negative and positive. In addition to making the game more fun,

[1] `http://d0x3d.com/d0x3d/welcome.html`
[2] `http://playspent.org/`

Table 1: Learning Goals of the Game

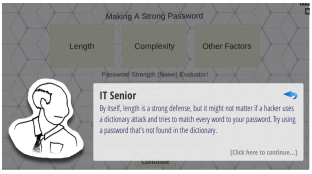
passwords	creation of passwords that are robust against dictionary attacks
data backups	importance of, different methods and advantages and disadvantages
phishing	ability to discern between safe and unsafe emails
malware	basic types of malware, characteristics, and what to do
encryption	basic idea, Caesar cipher & drawbacks, one-time pad and RSA

the events serve as extra learning tools. For example, the hard drive may fail, and the impact of that event will depend on whether the player had previously selected to backup the data. Similarly, players who have chosen Dropbox as cloud storage may be randomly informed of a Dropbox hacking that steals their data. Some of the random events include: firmware updates to patch security holes; hard drive failure; a simulated Equifax data breach.

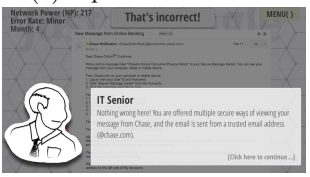
Player success is calculated through a combination of "network power," which is the quantitative scorekeeping system, and error rate. The error rate influences the probability of negative events happening to the player and can be decreased through successful completion of learning challenges. To be extra-friendly to novices, we allow them to select the challenge level of the game (Figure 2a). An "IT Senior" provides advice as necessary (e.g. Figures 2c and 2d). The game is published as a WebGL, so that it is playable in the browser with no need for installation.

(a) Choose challenge level

(b) Equifax data breach



(c) IT Senior provides hints



(d) IT Senior corrects mistakes

Table 2: Game pictures

4 Impact of the Game

4.1 Overview

Cyber Secured was piloted in the Electronic Commerce course offered at our US urban public college. The course is co-listed under the Computer Science and

Business departments and the students are fairly evenly divided between the two departments. Most of the CS students (and typically all of the Business students) are new to the field of computer science, and specifically to cybersecurity.

The course covers the basic technological and business background of e-commerce, including the development of the Internet and the WWW, business strategies, cybersecurity, and marketing. In the cybersecurity portion of the course, the goal is to give a general overview of the insecurity of the Internet, educate about security threats and explain the high-level concepts behind encryption. *Cyber Secured* was designed to help teach these basic topics to this pool of beginners.

To determine the potential of *Cyber Secured* to improve students' knowledge of cybersecurity and to get student feedback about the game, students taking the e-commerce course were offered the opportunity to play *Cyber Secured* for extra credit on a homework assignment. In total, 118 students were presented with this offer, comprising three sections of the e-commerce course, one online and two traditional in-class courses: an in-class section in the Spring (henceforth, Class1), and an in-class section (henceforth, Class2) and an online section (henceforth, Online), both in the following Fall. The students were briefed on the study and informed consent was obtained. They were then asked to take a pre-test measuring their knowledge of basic cybersecurity concepts, play the game, and take a post-test. The pre- and post-tests consisted of 13 questions covering passwords, phishing, malware, and encryption; to save space, we give only a sample of the questions in Figure 1. Questions on pre- and post-tests were highly similar. The pre- and post-tests were administered through Google Forms. The game was posted online[3].

Some changes were made to the game between the Spring and Fall semesters, including adding content about one-time pads and RSA encryption. To keep this study consistent between the cohorts, we used the same pre- and post-tests in the Fall semester as in the Spring, omitting questions about the new content.

4.2 Participants

In Class1, 40 students were offered the opportunity to participate. Of the 40 students, 23 took the pre-test, played the game and took the post-test (12 male and 11 female). We denote this group as Game (G). The other 17 students are our Control group (C); of these, 14 did not take the pre-test or play the game and three took the pre-test but did not play the game or take the post-test. Class 2 had 40 students. Of these, thirty chose to participate by playing and taking both tests (Game, 21 male and 9 female) and ten students did not take the pre-test or play the game (Control). Finally, of the 38 students in the Online course, 22 were in group Game (12 male, 10 female) and 16 did not take the pre-test or play the game (Control).

[3] `https://cybersecured.itch.io/cyber-secured-2020`

Figure 1: Sample post-test questions (correct answers are underlined)

1. Which of these passwords is the strongest?
   (a) ILoveSchool!
   (b) hello!8
   (c) monkey
   (d) YaThink?
   (e) I don't know

   Briefly explain your answer.
2. A phishing email is:
   (a) an email that has a virus inside
   (b) an email that tries to solicit sensitive information from you
   (c) an email that has spyware attached
   (d) an email that automatically gets sent to all of your email contacts
   (e) I don't know
3. If you're unsure if an email from a specific site is a phishing attempt, you should
   (a) click on the link provided
   (b) type the URL of the site directly into your browser
   (c) reply to the email to see if it bounces back
   (d) open the attachments provided
   (e) I don't know
4. Encrypt the following text, using a Caesar cipher with a key value of 2: `hello`. jgnnq
5. Decrypt the following text, using a Caesar cipher with a key value of 3: `fbehu`. cyber.
6. Is a Caesar cipher a strong encryption method? Explain your answer briefly.

4.3 Pre-test to Post-test

We give the mean and median for both tests for the 75 students who played the game below in Table 3. Both the pre- and post- tests were scored out of 13 points, and the scores are given both as raw scores and as percentages. Scores are presented for each of the individual sections as well as the combined group of all students. The average scores on the post-test demonstrate statistically significant increases compared to the pre-tests (using a paired t-test, $\alpha = .05$, $p < .001$ for all three sections).[4]

4.4 Final Exam Scores

To measure retention and transference, we looked at performance on the final exam. All sections of the course had questions on the final exam that related to the cybersecurity concepts covered in the game (e.g. malware, phishing, and encryption). The two Class groups had similar finals, with the questions about security (Class Security-Questions, or C-SQ) worth 26 points total; the online final had Online-

[4]We note that the scores on the pre- and post-tests were significantly less for the Online group than the corresponding scores in both Class groups ($p < .01$ for all). We do not offer conjectures to explain this, particularly due to such a small sample size.

Table 3: Game Quizzes, Group Game

		Average Score	Median
Class1 ($n=23$)	Pre-test	7.7/13 (59%)	7.3/13 (57%)
	Post-test	10.6/13 (82%)	12/13 (92%)
Class2 ($n=30$)	Pre-test	9.0/13 (69%)	9/13 (69%)
	Post-test	10.6/13 (81%)	11/13 (85%)
Online ($n=22$)	Pre-test	6.0/13 (46%)	6/13 (46%)
	Post-test	8.2/13 (63%)	8/13 (62%)
Combined ($n=75$)	Pre-test	7.7/13 (59%)	8/13 (62%)
	Post-test	9.9/13 (76%)	10/13 (77%)

Security Questions (O-SQ) worth a total of 17 points. The questions on the final give us a way to measure the impact of the game on longer-term retention and knowledge, despite not corresponding closely to the questions in the pre-/post-tests.

In Table 4, we give the average scores of the pre-tests and the security questions on the final for each section, given as percentages of total possible points. We also calculated the difference between the pre-test score and the score on the final security questions; the average of those differences is given in the last column on the table. We analyzed the pre-test score and final SQ score for each student in the Game groups using a paired t-test. The final SQ scores were significantly greater than the pre-test scores ($p \leq .001$) for each Game group, indicating retention of the material taught (though, of course, other factors may also have contributed).

Table 4: Average Pre-test and SQ Scores

	Pre-test	Final SQ	Difference
Class1 ($n=23$)	59%	76%	+16%
Class2 ($n=30$)	69%	79%	+10%
Online ($n=22$)	45%	77%	+32%

We also compared the final SQ scores of those who played the game to their classmates who did not. In Table 5, we give the average scores for the security questions (SQ) for the Class and Online groups. The last column gives the grade for the "Rest of the Final" (ROF): the non-cybersecurity questions on the final (as a percentage of the remaining 74 and 83 points, respectively), to serve as a control group for the SQ.

In both the Class and the Online Control groups, the scores on the SQ lag considerably behind the scores on the ROF. This is consistent with our observation that students find cybersecurity of the most difficult topics in the course. In contrast, scores on SQ for the Game groups were similar to their ROF scores, in addition to being significantly higher than Control-SQ scores. This suggests that the game helped students understand and retain the material.

However, it is difficult to draw any concrete conclusions about the effect of the game. The differences in scores for the SQ were not statistically different between the Game groups and Control groups for the Class groups and likewise, the ROF

scores were also not significantly different. In the Online group, on the other hand, there was a statistically significant difference between the SQ scores of Game and Control groups, but also a statistically significant difference between ROF scores ($p < .001$, $p = .003$, respectively). Hence, while we find the results of the final questions encouraging, we see possible evidence of a selection bias indicating that the differences in SQ scores may have been (at least partially) caused by underlying differences in the Game and Control groups. It is also possible that our small sample size does not allow us to adequately study the effects on the final.

Table 5: Average Scores on Final SQ

	SQ	ROF
Class1: Control($n=17$)	63%	73%
Class2: Control ($n=10$)	63%	67%
Combined Class Control: ($n=27$)	63%	70%
Class1: Game ($n=23$)	76%	79%
Class2: Game ($n=30$)	79%	77 %
Combined Class Game: ($n=53$)	77%	78%
Online: Control($n=16$)	53%	66%
Online: Game ($n=22$)	76%	77%

4.5 Interest in Cybersecurity

In addition to increasing *knowledge* about cybersecurity, another goal of our game was to increase *interest* in cybersecurity, with the goal of students finding the topic intriguing and relevant. We attempted to ascertain whether that goal was met. All three finals contained a two-point question that asked "*In your opinion, what was the most interesting / informative / useful topic that we covered? Briefly explain your answer.*" This question solicits general feedback about topics that interested students. We use the responses to estimate student interest in cybersecurity.

Table 6: Cybersecurity response rate

	Control	Game
Class1	44%	54%
Class2	25%	56%
Online	23%	53%
Combined	33%	54%

Out of the 118 students in the three sections of this course, 108 responded to the question. For each of the responses, we tallied up which students chose cybersecurity, or any of its sub-topics (e.g. malware, phishing, encryption) vs. other topics in the course. We give the cybersecurity response rates for each section in Table 6. In each section of the course, more than half of the Game group chose cybersecurity as their "favorite" course topic. The same was not true of the Control group, whose cybersecurity responses were much less frequent. The difference in the response rate was statistically significant ($p=.04$). We see this as an indication that playing the game increased interest in cybersecurity. (Some of the Game responses made that explicit, e.g. "*The game really helped me delve into the topic.*")

We also looked at response rates to this question from a previous semester, in which cybersecurity was taught but the game was not offered as a resource. That rate gives a baseline of cybersecurity interest among our students. The response rate of cybersecurity topics in the past was 38%; the difference between that rate and the response rate of the Game groups was statistically significant ($p = .049$). This suggests that the game actually increased interest in cybersecurity, and that the effects that we observed between Game and Control groups were not merely selection bias.

4.6 Qualitative Survey Results

The post-test also included qualitatives survey questions. The first four were based on [3] to measure the levels of intrinsic motivation of the students. The second three questions measured the students' engagement with the game. All seven questions used a 5-point Likert scale, labeled from "strongly disagree" (1) to "strongly agree" (5). An additional two questions asked for students' feedback on the game. The results of the rating questions are shown in Table 7. (To save space, we condense the intrinsic motivation questions.) In the second column, we give the average scores, across all sections. In the third column, we give the percentage of responses that indicate agreement; i.e. either "agree" or "strongly agree" (≥ 4).

Table 7: Qualitative Survey Responses

Question	average	percent agreeing
I played this game because I found it interesting	3.6	55%
I would play this game for fun	2.9	29%
I would play this game to learn about security	4.3	82%
I would play this game to help assess my knowledge of security	4.2	82%

The average score across all four intrinsic motivation questions was 3.3, indicative of slightly above-average motivation. Although students were neutral about the "fun" qualities of the game, the responses indicate strong agreement with the educational and assessment qualities of the game; over 80% of the students said that they would play this game to learn about and assess their knowledge of security.

The survey also included two-open ended questions for feedback: *Please tell us at least two things that you did not like about the game or think should be changed* and *Please tell us at least two things that you liked about the game – things we should not change.* These questions were not required fields; 67 (89%) of students chose to answer them. We hand-tagged the comments to identify common themes between answers; comments could be tagged with multiple tags. In total, we identified 16 "don't like" and 15 "like" tags. On the "like" end, 45% of students who answered commented about the educational benefits of the game, with comments such as *"I like that it taught you about the different topics while having fun; A great way to learn about the topic. Different in a good way; The content was very informative!; The game was very interesting and informative. It would be great if there were*

more games like this to teach students about the topics in e-commerce." 18% of the responses commented on the fun aspect of the game: *"I enjoyed playing until the 12 months were over; It felt very much like a regular game; The game was creative and unique unlike most browser games."*

On the "don't like" side, 15% of the responses noted that the game was confusing in some way (*"Make the instructions a bit clearer; the game error level was confusing at first"*); 12% wanted the graphics to be improved (*"I wish the game was a bit more colorful; the graphics could be improved"*) while 12% could not think of any improvements necessary (*"Nothing that I didn't like; None. I liked the game"*). The most frequent comment (16%) was that the game was too long (*"The game felt long; it was kinda long; I think the game is a little bit too long to play"*). As noted in Section 4.1, we added two new encryption modules between Class1's participation and that of Class2/Online. Responses about length were far more prevalent in Class2/Online surveys, and slightly lower levels of interest in the game were reported in those surveys as well. We suspect that the additional modules may have made the game too long for students and decreased their interest in playing. One of our plans is to make these modules optional, so that students can choose to skip them.

5 Discussion and Conclusions

Although our sample size is small, our results are encouraging and show that students who play *Cyber Secured* demonstrate educational gains compared to students who did not play. Moreover, student feedback suggests that students themselves recognize the value of the game as a tool for learning about cybersecurity and several students asked for us to create similar games for other course topics. We think that this game has potential to be helpful to students who are new to cybersecurity and plan to continue to develop the game by making some modules optional as well as by making the game more visually appealing and fun to play by speeding up slow-loading text, clarifying instructions and improving the graphics. We would also like to add analytics so that we can see with which topics students struggle, and we plan to then conduct a larger study of its effects on a larger sample of students.

This game was created by a team of undergraduate CS students. This project was doubly enriching, offering educational benefits for both the students who created the game and those who played it. Besides improving their skills in Unity game programming, the students who developed the game learned to manage a complex code base, to work as a team, and to design a pleasing user experience. This game is thus a strong representation of "of students for students."

The game is available for free online at `https://cybersecured.itch.io/cyber-secured-2020` as a resource for other instructors who teach cybersecurity to novices. Because of the introductory nature of the game, it can be used in a variety of courses, including General Education courses, CS0 courses and other CS courses for non-majors. The game can also be a meaningful addition to high school CS courses. *Cyber Secured* can be used as a standalone course activity to raise

awareness about cybersecurity, as a means of assessing student knowledge, or as an introduction to the topic. It can also be used to motivate class discussions about cybersecurity, as well as debates about the ethical issues that surround cybersecurity.

References

[1] Nalin Asanka Gamagedara Arachchilage, Steve Love, and Konstantin Beznosov. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, 60:185–197, 2016.

[2] Mark Gondree and Zachary NJ Peterson. Valuing security by getting [d0x3d!]: Experiences with a network security board game. In *6th Workshop on Cyber Security Experimentation and Test*, 2013.

[3] Frédéric Guay, Robert J Vallerand, and Céline Blanchard. On the assessment of situational intrinsic and extrinsic motivation: The situational motivation scale (SIMS). *Motivation and Emotion*, 24(3):175–213, 2000.

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

[5] Cynthia E Irvine, Michael F Thompson, and Ken Allen. CyberCIEGE: gaming for information assurance. *IEEE Security & Privacy*, 3(3):61–64, 2005.

[6] Thomas Monk, Johan Van Niekerk, and Rossouw von Solms. Sweetening the medicine: educating users about information security by means of game play. In *Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists*, pages 193–200. ACM, 2010.

[7] Marina Papastergiou. Digital game-based learning in high school computer science education: Impact on educational effectiveness and student motivation. *Computers & Education*, 52(1):1–12, 2009.

[8] Portia Pusey, David H Tobey, and Ralph Soule. An argument for game balance: Improving student engagement by matching difficulty level with learner readiness. In *3GSE*, 2014.

[9] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth 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*, pages 88–99. ACM, 2007.

[10] Michael Thompson and Cynthia Irvine. Active learning with the CyberCIEGE video game. In *Proceedings of the 4th Conference on Cyber Security Experimentation and Test*, 2011.

[11] Shian-Shyong Tseng, Kai-Yuan Chen, Tsung-Ju Lee, and Jui-Feng Weng. Automatic content generation for anti-phishing education game. In *Electrical and Control Engineering (ICECE), 2011 International Conference on*, pages 6390–6394, 2011.

[12] Pieter Wouters, Christof Van Nimwegen, Herre Van Oostendorp, and Erik D Van Der Spek. A meta-analysis of the cognitive and motivational effects of serious games. *Journal of Educational Psychology*, 105(2):249–265, 2013.