Cyber Secured: A Serious Game for Cybersecurity Novices

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

ABSTRACT

We developed an educational serious game to teach basic cybersecurity concepts to novices. An evaluation of the game on introductory Computer Science and Business students suggests that playing the game resulted in both short-term learning gains in cybersecurity as well as longer-term retention of the concepts. We also saw evidence that students who played the game had increased interest in cybersecurity, and students self-reported interest in playing the game to learn more about and assess their knowledge of cybersecurity.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; • **Applied computing → Computer games**;

KEYWORDS

cybersecurity, serious games, game-based learning

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. Due to the potential for games to engage and motivate learning, a number of serious games have been created to teach cybersecurity concepts. However, many of these games are geared towards those who are already knowledgeable about cybersecurity and may actually decrease the interest of novices in learning about cybersecurity by overly challenging them [1]. 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.

2 OVERVIEW / METHODS / RESULTS

We developed a game called *Cyber Secured* using the Unity 2D environment to teach and assess basic cybersecurity concepts to beginners. In the game, 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 educational goals of the game, for example, for example, 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. Random events, such as hard drive failures and Dropbox hacks, reveal the impact of the choices that players made.

Cyber Secured was piloted in the Electronic Commerce course offered at our college. The course includes both (introductory) Computer Science and Business students; most of the students are new to the field of computer science, and specifically to cybersecurity. Students in three sections of the course (two in-class and one online) were offered the opportunity to participate in a study of *Cyber Secured* for extra credit. In total, 64% (75/118) students chose to participate. Students were asked to take a brief pre-test, play the game, and take a brief post-test.

Some outcomes of the study include:

- **Post-test scores:** Average scores on the post-tests demonstrated statistically significant increases compared to the pre-tests (on average, about 17%).
- **Final exam:** Scores on the security questions on the final exam were significantly higher than scores on the pre-tests for participants, as well as higher than scores on those questions for non-participants.
- **Interest in cybersecurity:** Students who played the game were significantly more likely to say that cybersecurity was the most interesting/useful topic that they learned in the course, compared to both non-participants and students from previous semesters. This suggests that playing the game increased student interest in cybersecurity.

Over 80% of students said that they would play the game to learn about cybersecurity or to assess their knowledge.

3 CONTRIBUTIONS AND FUTURE WORK

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. Our plans for the future include making the game more fun, adding analytics so that we can see with which concepts students struggle, and conducting a study of its effects on a larger sample of students.

REFERENCES

[1] Portia Pusey, David H Tobey, and Ralph Soule. 2014. An Argument for Game Balance: Improving Student Engagement by Matching Difficulty Level with Learner Readiness.. In *3GSE*.