CYBER SECURITY EDUCATION THROUGH GAMING

CYBERSECURITY GAMES CAN BE INTERACTIVE, FUN, EDUCATIONAL AND ENGAGING *

Ian Cullinane, Catherine Huang, Thomas Sharkey
Computer Science Department
MassBay Community College
i_cullinane, c_huang,
t_sharkey@post.massbay.edu

Advisor: Shamsi Moussavi
Computer Science Department
MassBay Community College
781-239-2240
smoussavi@massbay.edu

ABSTRACT

Cyber security is an active and evolving field. Among its many challenges are educating minors in the safe and responsible use of the Internet. To date, many computer games have been developed which seek to teach these concepts. Through a grant funding from The National Science Foundation, students at MassBay Community College have researched and evaluated currently available games. With an end goal of developing new game platforms to teach cyber-security, current games were evaluated based on their effectiveness in imparting the material and keeping students engaged. After research and evaluation of games currently available to help understand the current market, this project is focusing on the development of new games designed to teach cyber security concepts to minors aged 11-14.

INTRODUCTION

Every year Internet technologies become more ingrained in our daily life. As those systems become more and more complex, they start to become environments and communities in and of themselves. Just like our real world environment we must be mindful and cautious how we interact with those communities. Much like the real world we need to teach minors about dangers and possibilities in online environments. Today,

the average child can start accessing the Internet unsupervised at the age of eight [1]. As they start to use more complicated systems and social networks, the need safe usage becomes critical.

In order to properly develop games to educate, the behaviors and motivations of minors online must be understood. According to Madden, et al, 95% of minors aged 12-17 use the Internet in some capacity, eight in ten use some kind of social media [4]. Facebook alone attracts 77% of all Internet users aged 12-17 [4]. Other common activities include email and browsing, and many students engage in the use of local networks at their school. All of these environments, and the implications of their use, should be understood by today's students.

Current trends indicate a typical minor using the Internet should know how to be safe online by age twelve. A minor should be able to understand the implications of using a social network, how to identify malicious emails (e.g. spam, phishing, and viruses), and how to protect their privacy and identity. The games being developed focus on minors aged 11-14. The goal is to create a fun and engaging game platform, which will give students the necessary tools for safety, as well as engage them in a fun interactive way.

GOALS

The goals of this project are to produce games that:

- Teach basic cyber security concepts to minors
- Are easily available
- Provide an engaging environment
- Provide continuity and a sense of progression in learning

The top goal for this project looks to increase one's understanding of cyber security, and the potential risks with inadequate security safeguards through computer gaming [3]. Lessons will be about phishing, viruses, malware and other topics that have been identified as important through the research phase. In order to reach the maximum audience the games are being developed to run online through a browser. In this way the games can be played by anyone with a computer and Internet connection.

The design of the game calls for a general story the user can play through which mimics their everyday student life and technologies they will interact with. Through this story the player will interact with various games, which represent real world systems, threats, and concerns. Choices in the game will mimic real world consequences.

METHODOLOGY

Current research is a continuation of work completed by a previous M-STEM scholar during the 2013-2014 academic year that led to a presentation of works at the 2014 CCSCNE conference. The need for engaging and effective cyber security education tools became more apparent during the MassBay Community College summer bridge program. This program features a section teaching cyber security concepts to high school students.

Current research began by identifying games currently available in the category of cyber security. Many games were tested and the best ones were selected to be scored and ranked. The researchers played each game separately and scored based on set criteria: replay value, progression qualities, and interface accessibility. Then each game was also given an overall score.

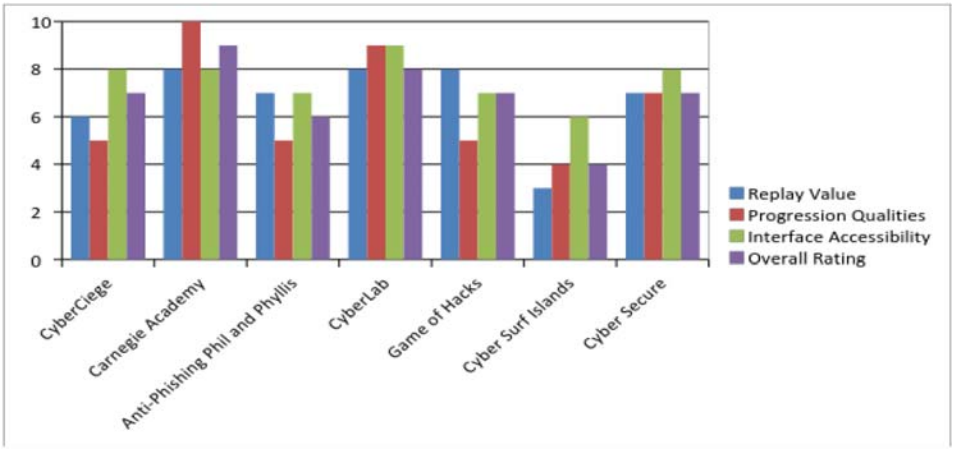

Fig 1, analysis of current Cyber Security Games

Replay value represents how much the user would be willing to play the game again. If the games were identified as monotonous with little engagement then the game received a low score. If the there was a high level of engagement that left the user wanting more, high marks were given.

Progression qualities identifies if the game had new levels for the user to unlock or if the game had some sort of narrative that would keep the user interested and wanting to continue their gameplay to see what they could do next.

Interface accessibility is rated on the game's ability to teach the user how to play the game and ease of navigation through the menus so the user can understand what to do in each situation and be able to accomplish their task.

RESULTS

The data shown in Fig1, made it possible to see the traits that successful and unsuccessful games had in common. Many games were found to have elements that proved to be either appropriate or inappropriate for the age group and goals of the project.

The game mechanics that were common to successful games, mechanics common to all games, and mechanics of an unsuccessful game were also identified. A game mechanic is any number of design elements the game developers have used. An example would be the pattern-matching mechanic common to almost all games tested, where a player is shown a pattern and then expected to identify the pattern in a challenge.

Strong Gameplay Elements

Games that were viewed as an overall success displayed patterns in design that lower scoring games failed to utilize. Games that contained a narrative to

accompany learning especially achieved a high score in overall quality. Carnegie Cadets, the overall best scoring game, also featured the most complicated narrative and progressive elements. CyberSecure, and Cyber Lab also ranked highly overall and included a complex narrative. Progression in general showed to be a positive trend including level progression and progressive difficulty.

Game Name	Tester Experience	Topics Covered
CyberCiege	+ Simple instruction + Good real life situations - Situations unrelated to our audience	Spam emails, worms, identity theft, password protection.
Carnegie Academy	+ In-depth information and comprehensive + Nice interactive world + Tracks player data	Spam email, password protection, cyber bullying, personal information, website dangers.
Anti- Phishing Phil and Phyllis	+ Simple Design - Situations unrelated to our audience - No progression	Phishing, fake website identification.
Cyber Lab	+ Good design and interesting story + Harder levels to unlock + Video content - Instruction contains Extensive text	Passwords, phishing.
Game of Hacks (http://www.gameofhacks.com/)	+ Allows for user-generated content + Tracking high scores + Player can compete against friend's scores - Looks into hacking, instead of security	Identifying vulnerable code.
FBI Cyber Surf Islands	+ Polished user interface + Contain levels to be unlock + Resource section for Instructor - Extensive text - Lack of variation in gameplay types	Online predators, passwords, privacy, cyber bullying, social networking, reputable sites, chat rooms.
Cyber Secure	+ Clear narrative story and setting. + Good interface with 3D models + Has glossary of terms to help players + Audio content - Only ask multiple-choice questions. - Large amount of Text	Protecting company information, passwords, encrypted networks.

Fig 2, User experiences with given games

Weak Gameplay Elements

Variety of gameplay was shown to be very important. Games that featured repetitive gameplay elements ranked lowest. Cyber Surf Islands, the lowest ranking game, featured a lot of "levels" but they all used the same gameplay mechanics. An extremely simple game that prompted a lot of text the player

had to read. This game became boring extremely quickly. All games that scored poorly had at least one of two common traits: Repetitive gameplay or a lack of qualities of scenario progression.

Knowledge Retention

All games analyzed delivered knowledge in two ways: text descriptions and pattern recognition. The primary difference between the high scoring games and the low scoring games was the context in which the information was displayed. A user playing Cyber Surf Islands will likely learn what they are exposed to. However, they will play the game for so short a time as to not learn more than even one lesson. Conversely players of Carnegie Cadets, Cyber Lab, or CyberSecure are likely to learn a lot more because the games have a much higher level of engagement. This results in more time spent playing, and more opportunity to learn the lessons within.

GAMES IN DEVELOPMENT

The games are currently being developed using the libGDX programming library [2]. This library uses the popular Lightweight Java Game Programming Library to develop and export games, which can be written once and run on multiple platforms. This library provides powerful, professional tools used in game development. Games are being developed with an "online first" mentality.

The development of new games with the intention of releasing them as a web based game playable through the browser, have been started. The games will contain a narrative that is similar to the player's everyday life. Through this narrative the player will be exposed to games and simulations that represent real world cyber security concepts. These games will combine successful design choices found in the games evaluated, targeted towards topics previously discussed. Design choices include but not limited to ideas such as: create an overarching narrative world, interactive interfaces, and deliver information in short comprehensive pieces within various type of games.

NARRATIVE GAME

This game is a representation of a typical middle school environment complete with characters the player can interact with. This game is an overall game, which supplies context and narrative to players interacting with the game. Through this environment the player will learn through interactive instruction, use simulated computer environments, and play games designed to impart valuable lessons in cyber security.

PHISHING GAME

For this game players have access to an email that is given to them from the I.T. character at the school setting narrative. In order for the player to gain access to their email, they must complete a series of brief tutorials that will teach them to identify a phishing attack. These tutorials will be small mini games that will have the player match and identify false emails, or show them what types of information that they should never

share with anyone over the Internet. Later on in the game they will receive emails, which test what they learned. Like real life, their actions will have different consequences.

VIRUS GAME

The virus game will consist of multiple mini-games that are unlock-able as player gain knowledge of this topic. The game begin with the player interacts with certain NPC (non-player-character), the first game will be trigger if the user decide to help the NPC. The first game will focus on teaching the important terms and vocabulary to teach player of the basic knowledge in dealing with computer virus. The later games will orientate around simulated graphics of virus protection software or downloading files from web, where player can play matching game or puzzle game to identify and protect against various viruses.

CONCLUSION

Every year gaming is growing to be a more dominant medium. Virtually all children play video games both educationally and for entertainment. The power of games as a learning medium is a body of research that grows larger every year. The power of gaming can be leveraged to teach important lessons about cyber security to young people who need it the most. By developing games that try and take lessons learned from recent attempts into the field these researchers hope to find new and engaging methods of teaching through gaming.

Planned future work on this research includes development of more games, testing games with the target audience of 11-14 year olds from area middle schools, and use of the games in the MassBay Summer Bridge Program. The games currently being developed will be maintained and built upon by future M-STEM scholars at MassBay Community College.

REFERENCES

[1] Sanchez, Kim. “How Old Is Too Young to Go Online? - *Microsoft on the Issues*.” Microsoft on the Issues. Microsoft, 14 Oct. 2013. Retrieved Web. 01 Nov. 2014. http://blogs.microsoft.com/on-the-issues/2013/10/14/how-old-is-too-young-to-go-online/

[2] Zechner, Mario. *Libgdx*. Computer software. LibGDX. Vers. 1.4.1. N.p., 2013. Retrieved 1 Nov., 2014. http://libgdx.badlogicgames.com/(libgdx)

[3] Denning, Tamara, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. “Control-Alt-Hack: The Design and Evaluation of Statistical Software for Microcomputers.” *Journal of the Royal Statistical Society. Series D (The Statistician)* 34.4 (1985): 391-427. 2013. Web. 1 Nov. 2014. *Proceedings of ACM Conference on Computer and Communications Security* (CCS '13) <http://homes.cs.washington.edu/~lerner/cah-eval-ccs.pdf>

[4] Mary Madden, Sandra Cortesi, Urs Gasser, Amanda Lenhart and Maeve Duggan. "Teens, Social Media and Privacy". Retrieved Web. 22 Jan. 2015. http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/