https://doi.org/10.48009/3_iis_2019_28-36

Issues in Information Systems
Volume 20, Issue 3, pp. 28-36, 2019

CYBER-SECURITY INSTRUCTIONAL TECHNOLOGY DESIGN

Billy Carrie, Georgia Southern University bc04045@georgiasouthern.edu
Hayden Wimmer, Georgia Southern University, hwimmer@georgiasouthern.edu
Loreen Powell, Bloomsburg University, lpowell@bloomu.edu
Carl Rebman, University of San Diego, carlr@sandiego.edu

ABSTRACT

As the use of innovative technologies continue to grow at rapid rate, so does the need to protect these technologies from hackers performing breaches to steal user's data. To protect users, cyber-security awareness materials should be readily available to guide users understanding of the vulnerabilities existing in their technological devices; explore the plethora of tactics carried out by hackers to steal their data, and identify measures they can take to ensure their safety as they utilize their devices. The objective of this work is to develop cyber-security awareness materials in Google Classroom using instructional technology design principles to accommodate user learning styles while increasing cyber-security expertise. We create two courses, one focusing on introductory level cyber-security concepts and the other on advanced cyber-security concepts. Topics discussed in the module include threats, attacks, vulnerabilities, risk management, cryptography, software security, and computer networks. Instructional design models and principles such as Universal Design Learning (UDL), Paivio's Dual Coding, Mayer and Anderson's Contiguity Principle, and Howard Gardner's Multiple Intelligences are applied to the development of the module's content in an effort to accommodate user learning styles and technical expertise. Following the completion of the development of the two cyber-security courses in Google Classroom, we concluded that the courses are progressive steps to creating readily available cyber-security awareness materials for the general public.

Keywords: *Cyber-Security, Cyber-Security Education, Instructional Design, Learner Styles, Student Learning Objectives*

INTRODUCTION

Due to the U.S. National Security Crisis) and millions of cyber-security jobs going unfilled annually (Defensenews, 2018), there is a need to improve on the lack of cyber-security awareness materials dedicated to educate and protect citizens. In efforts to protect citizens, cyber-security awareness materials should be free and readily available to guide users understanding of the vulnerabilities existing in their technological devices. We examined cyber-security content that is relevant and applicable to technology users today using CompTIA Security+ and Network+ certification exam objectives topics. After examining the content, we derived at the topics we wanted to include in our courses which included the following: threats, attacks, vulnerabilities, risk management, cryptography, software security, and computer networks. We also strive throughout this work to create a learner centered environment that makes the users comfortable when learning. To create this environment, we implemented instructional design models and principles such as Universal Design Learning (UDL), Paivio's Dual Coding, Mayer and Anderson's Contiguity Principle, and Howard Gardner's Multiple Intelligences to the development of the course.

LITERATURE REVIEW

Cyber Security Concepts & Strategies

The need for degree programs that focus on educating and training individuals for occupations in the cyber security field is important, however the need for improved cyber security awareness materials for the average everyday person is just as important**.** Dupuis (2017) developed an introductory cyber security course for non-technical majors with intentions to increase cyber security practices. First, the work discussed the need for the masses to be educated on the fundamentals of cyber security. Next, the approach taken in the development of the undergraduate course in cyber security was detailed. Then, authors discussed the results of two iterations of the introductory cyber security course

which included feedback from students and lessons learned. Following results, the curriculum within the course was analyzed within the context of Bloom's taxonomy. Finally, authors explained the benefits the course has to offer to various stakeholders, such as students, STEM programs, colleges, and society. Qualitative responses from stakeholders about the cyber security course such as "Helped me get more information about installing anti-virus software", "I did not know much about computers so I learned a lot about them", and "It opened my eyes to the dangers of the Internet" exemplifies the accomplishment of the previous goal to expose students to information about cyber security that they did not previously know or understand. Also, the benefits to having the course available to stakeholders include increased interest in technology from female demographic; students learn how to better protect their information and improve their behavior from a cyber security and privacy standpoint; Colleges ability to provide an important class that serves as a public good while helping fulfill a general education requirement; and society at large benefits by having more people educated in cyber security and privacy. The course was successful in the two iterations and stakeholders benefitted from the content about cyber security. However, a suitable textbook for the intended audience is needed to accommodate those who prefer accessing the content physically instead via eBook (Dupuis, 2017).

There is a prominent need for more training and education materials to be available to cyber-security professionals. Unfortunately, despite this need, there is little rigorous evidence to inform educators on effective ways to engage, educate, or retain cyber-security students. Scheponik et al. (2016) conducted a series of think-aloud interviews with cyber-security students to examine how they reason about core cyber-security concepts. The qualitative data via interviews will be used to develop engaging cyber-security assessment tools. Cyber-security students from three universities, University of Maryland, Baltimore County, Prince George's Community College, and Bowie State University were interviewed about their understanding of cyber-security especially adversarial thinking. Student statements were analyzed using a structured qualitative method, novice-led paired thematic analysis, to document student misconceptions and problematic reasoning. Preliminary findings reveal that students misinterpret fundamental cyber-security concepts. The concepts of confidentiality with integrity and authentication with authorization were used interchangeably by subjects during interviews. The misinterpretation of cyber-security concepts suggests that individuals are becoming too easily satisfied that a system is secure after identifying only one possible source of security for a system rather than seeking to explore the adversarial space more thoroughly. Upon completion of the 26 interviews conducted, more insight into how cyber-security education can be measured and improved will be used to develop assessment tools to measure student learning in cyber-security (Scheponik et al., 2016).

Currently, the United States faces the threat of malicious cyber-attacks daily which affect businesses, government, and our society. To protect the country from the growing number of cyber threats in the modern tech age, universities are striving to increase cyber security awareness amongst its students who will soon be future combaters in cyber warfare. For this study, the objective is to apply innovative student learning methodologies to teach cyber-security to a group of motivated CS/IT students who are interested in the topic. The Challenge Based Learning (CBL) methodology was applied in efforts to encourage students to collaborate with their peers, ask questions, develop a deeper understanding of the content, and take the initiative to solve real-world problems. Wilson and Kiy (2014) engaged students to develop stimulating questions which reflected their interests in information security, devised challenges about safeguarding confidential information from cyber-attacks, and formulated solutions to secure data and computer network. For guiding activities, students participated in two cyber-security competitions against their peers from other local universities. In these simulated real-life competitions, students teamed up, quickly brainstormed ideas, and applied their knowledge to defend against hypothetical cyber-attacks. After performing assessments, students reported to have an increase in their willingness to teach others cyber security topics. There was also an increase in knowledge and skill set amongst students in computers and information security. 80% of the students stated that they benefitted from the CBL experience such as networking with industry professionals, improving computer and security skills, and applying these skills in a practical, real world environment. The application of the Challenge Based Learning methodology to cyber-security education was proven to be successful as it challenged students to work together as a team to provide solutions to the problems, increase computer skills, security knowledge, ability to teach others, and interest on the topic of cyber-security (Wilson & Kiy, 2014).

Technology security tools are used to secure users; however, users are persuaded to execute sound technological practices while using their devices. Research by Zhang-Kennedy, Chiasson and Biddle (2016) utilized an online interactive comic series called Secure Comics based on instructional design principles was developed to improve user's understanding of security threats. Interview analysis consisting of survey questionnaires were used to assess

users' conceptualization of security password guessing attacks, antivirus protection, and mobile online privacy shows that poor understanding of security threats influences users' motivation and ability to practice safe behaviors. They found that Secure Comics improved user understanding of cyber-security principles and motivated positive changes in security management behavior. The comics successfully influenced users' improved behavior changes including updating security software settings, cautious web surfing or downloading, and sharing of information with family and friends without prompting. Participants showed good retention of the content in the comic and showed improvements in awareness of the threats and why they should abide by recommended security guidelines. Their feedback indicated that the comics were engaging and useful learning tools which persuaded them to adopt improved security practices (Zhang-Kennedy, Chiasson, & Biddle, 2016).

The U.S. government has made cyber-security a national priority, however, there are still deficiencies in the number of cyber-security materials available to the general public. Endicott-Popovsky, and Popovsky (2014) addressed the lack of cyber-security materials via the development of an innovative curricular model that holistically develops future cyber-security professionals. The curriculum model, SSCD-IAC (Secure Software Code Development - Information Assurance Curriculum) was developed based on system activity-based learning, which combines learning and productive activities directed toward developing professional abilities and motivation. The innovative curricular model led to the development of 23 cyber-security courses taught within the collegiate curriculum and Information Security and Risk Management (ISRM) Certificate program. The growth of the program was attributed to the curricular model's ability to not only increase cyber-security expertise amongst the participants but also encourage those participants after the completion of the program to come back to lecture and recruit employees for their respective firms (Endicott-Popovsky & Popovsky, 2014).

Cyber-security and information security are often used interchangeably however they are not analogous. Research by Von Solms and Van Niekerk (2013) o compared the terms cyber-security and information security to identify how they differ from one another. The concept of Information and Communication Technology Security (ICT) was used as a central component in comparing and analyzing the definitions of cyber-security and information security. They found that the aim of information security is to ensure business continuity and minimize business damage by limiting the impact of security incidents. Contrarily, cyber-security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets (Von Solms & Van Niekerk, 2013).

Instructional Design Models & Principles

Instructional design model modifications can be accredited to the sociological changes in society such as moving from an industrial age to an information age. Today, instructional models are structured to cater to different types of learners as opposed to the less authentic mass education philosophy that presented information in a uniformly. Baturay (2008) analyzed the Morrison, Ross, and Kemp's model of instructional design, Dick and Carey's model, and Smith and Ragan's instructional model to examine the main and unique qualities of instructional design models. The three instructional design models Morrison, Ross, and Kemp; Dick and Carey, and Smith and Ragan were compared to one another based on the fundamental ADDIE model by exploring their respective principles and design approaches. After analyzing the three instructional design models, we find that the Morrison, Ross, and Kemp's model provides more flexibility than the other three because the designer can start with whatever element they want to without the completion of previous steps in the model. Also, regarding the test items in the model, the Smith & Ragan's model has a 'writing test item' stage and in the Dick & Carey model there is a developing criterion test items' stage at the very beginning of the designs. Instructional design models provide structure to learning by presenting a creating a customized and learner-centered environment. However, due to the nature of catering to multiple learner types, instructional design models should not be uniform but therefore be subject to adjust with the respect to the educational setting, learners, and objectives of the instruction (Baturay, 2008).

Aesthetic principles in instructional design learning are seen as immersive, infused with meaning, and felt as coherent and complete. Instructional design learning materials in today's society benefit greatly from the aesthetics' ability to engage learners. Research by Parrish (2009) aimed to examine the aesthetic first principles for creating artful instruction while abiding to current instructional design learning theories to create an engaging learning experience. The common concerns of literary criticism - plot, character, theme, and context are used to create a useful framework for the first principles of aesthetics which include learning experiences have beginnings, middles, and endings; learners are the protagonists of their own learning experiences; learning activity, not subject matter, establishes the theme of

instruction; context contributes to immersion in the instructional situation; and instructors and instructional designers are authors, supporting characters, and model protagonists. To apply these principles into instructional design, guidelines were presented to apply these principles into instructional design. Each first principle of aesthetics was connected to a related learning and instructional design theory. For example, the first aesthetic principle, learning experiences have beginnings, middles, and endings was found to have the related learning and instructional design theories: inquiry learning, problem-based learning, problem-centered learning, project-based learning, goal-based scenarios, and elaboration theory. These connections create a heightened the form of engagement with learners that isn't limited to scientific or technological constraints but instead takes a holistic account of ourselves and the world. Aesthetic considerations in teaching and instructional design include much more than providing an attractive frame or surface to instructional events. Aesthetic approaches in combination with instructional design principles and theories do not make instruction easier to but they indeed create meaning to content and expand approaches to future experience with learning (Parrish, 2009).

Media technology-enhanced and student-centered learning environments are used to facilitate the learning and understanding of abstract concepts. Sangawang (2015) developed an instructional design framework from instructional design theories such as cognitive processes, creating thinking approach, and organization learning. An achievement test and a questionnaire were used to assess students' opinions toward the developed framework. Results revealed that the framework provides excellent potential for development and evaluation. The framework creates conditions for internal mental learning process, creating processing memory, perception knowledge & information, and situated cognition. With this framework, learners will be capable of developing knowledge in society by social interaction, shared thought, and decision making (Sangsawang, 2015).

Differentiating learner types based on their individual abilities and preferences are important to understand best practices needed to instruct in a contemporary education environment. A recent study by Al-Azawei, Parslow, and Lundqvist (2017) used the Universal Design for Learning (UDL) and the Technology Acceptance Model (TAM) to examine the effectiveness of blended e-learning and learner satisfaction. Universal Design Learning principles such as multiple means of representation, action and expression, and engagement were implemented to engage and satisfy a wide variety of learners and their learning types. Results suggested that using educational technologies to address curricula limitations is a bridge to enhancing learner willingness to accept e-learning. Their findings should prompt e-learner instructor practitioners to prioritize the design and structure of e-courses to successfully implement e-learning. (Al-Azawei, Parslow, & Lundqvist, 2017).

In the 20th Century, traditional learning was the fundamental practice in education. Generic in its purest form, traditional learning aimed to educate every student the same way (i.e. lectures). Howard Gardner and John Dewey opposed this traditional style of learning and presented the idea that a learner-centric educational environment was the most effective form of education. Achkovska-Leshkovska and Spaseva (2016) analyzed and identified the key concepts within Dewey's and Gardner's educational ideas. To compare the educational ideas, historical-comparative method and content analysis were applied to investigate important concepts such as curriculum, methods of teaching and learning, and teachers' role. As a result, they found that Dewey and Gardner both preferred integrated curriculum and student-centered teaching concepts in teaching which was used to link the material being taught to the student's personal skills. In summary, though the theories are quite similar, it is implied that Gardner's theory was an extension of Dewey's theory and educational ideas (Achkovska-Leshkovska & Spaseva, 2016).

METHODS

Two cyber-security courses were developed in Google Classroom to increase cyber-security expertise while complying with different user learning styles. The introductory level course, Intro to Cyber Security 101, was designed to teach students the fundamental concepts of cyber-security. This course presented students of young age groups and expertise with the key components of cyber-security such as threats, attacks, vulnerabilities, risk management, cryptography, software security, and computer networks. The advanced level course, Intro to Threats, Attacks, and Vulnerabilities 101, was designed to extend on my own prior understanding of cyber-security principles. This course composed extensive components of threats, attacks, and vulnerabilities in cyber-security such as malware, application/ service attacks, and threat actors. The structure of the courses and learning modules was inspired by the examination of CompTIA Security+ and Network+ certification exam objectives along with articles including the Journal of Cyber-security Education Research and Practice (JCERP) and Center for Information Security and Assurance Research Lab.

Our introductory course is developed for introductory learners and appropriate for an outreach type activity for a Center of Academic Excellence in Cyber Defense (CASE-CD).

Course & Learning Module Structure

Before the students access the components of the course, they are prompted to perform an assessment in the 'Intro to Cyber Security' section that evaluates the student's experience of cyber-security prior to beginning the course. After completing the assessment, students can proceed through the course's learning modules. Each module is structured to include YouTube videos focusing on the module's topic from Professor Messer; a PDF file presenting the cyber-security concepts with a combination of text and graphics; an assessment to evaluate the student's understanding of course content; and a lab that student's perform to apply their knowledge acquired from the course.

Academic based cyber-security courses and applied instructional design principles inspired the design and a model of our cyber-security courses. We implemented a sub-set of student learning goals (Dupuis, 2017) to create course content. We also attribute the creation of our assessments and lab activities to Dupuis' study because it was proven that quizzes/ assessments allowed students to learn and understand technical, social, and behavioral components of cyber security in addition to lab assignments that made the course more relevant and increased cyber security posture. To engage the learner and help them retain information, we satisfied Paivio's Dual Coding and Mayer and Anderson's Contiguity Principle theories by inserting graphics, text, and audio media types to the cyber-security courses. In Paivio's Dual Coding Theory, it is implied that the combination of related text and images helps to enhance comprehension, and increases long-term memory. Meyer and Anderson focused more on the integration of media types into the content by stating that "When text is integrated on the screen close to related visuals, learning is more effective than when they are placed in isolation" (Zhang-Kennedy et al., 2016). Universal Design Learning (UDL) applications inspired how we presented course in different ways and actions in efforts to reach multiple learner types. According to (Al-Azawei et al., 2017), it has been shown that UDL application in higher education can promote learner experience in terms of performance, engagement, satisfaction, social presence, learning stress, and learning flexibility. The three guiding UDL application frameworks we used in our work included the following:

- Multiple means of representation (MMR): Presenting learning content in multiple ways to assist learners in mastering learning content with less effort.
- Multiple means of action and expression (MMAE): An essential step in the learning process is the way students express their understanding.
- Multiple means of engagement (MME): In order to engage students, materials should be stimulated and motivated in different ways and actions.

Learner Styles

To accommodate the different user leaner styles, we analyzed and implemented a sub-set of Howard Gardner's Multiple Intelligences learning styles. Howard Gardner proposed that each person has all intelligent learning styles but some styles are unique to each person (Achkovska-Leshkovska & Spaseva, 2016). The learning styles include linguistic, logical-mathematical, spatial, musical, bodily-kinesthetic, intrapersonal and interpersonal. The spatial and linguistic styles guided us to implement videos, and text with pictures. Also, the interpersonal style aided our decision to use the Google Classroom application because it offers users the ability to interact with others by commenting any questions/ concerns pertaining to the learning modules within the cyber-security courses.

Student Learning Objectives (SLO)

The Georgia Department of Education outlines the primary purpose of SLOs which is to improve student performance at the classroom level (Woods, 2015). A way to evaluate this improvement is to assess student's pre and post assessment scores. In Georgia, when implementing SLOs into course content, instructors are required to measure student's growth using pre-assessments and post-assessments. SLOs in addition to pre and post-assessments were inserted into the introduction of every learning module in the cyber-security courses we created as a way to evaluate the student's understanding of the course material. While our work follows the Georgia standards, similar standards exist at most intuitions and from various accrediting bodies.

RESULTS

After the implementation of cyber-security concepts, instructional design principles, SLOs, and other key concepts, we were able to construct the two cyber-security courses (Intro to Cyber Security 101 & Intro to Threats, Attacks, and Vulnerabilities 101) in Google Classroom. Although there remains room for improvement, the courses created are great initial steps to accomplishing our objective, which was to create cyber-security awareness materials to increase cyber-security expertise in addition to accommodating user learning styles. Depicted below, are images taken from the Cryptography module in Intro to Cyber-security 101.Figure 1 details the primary page for the class.

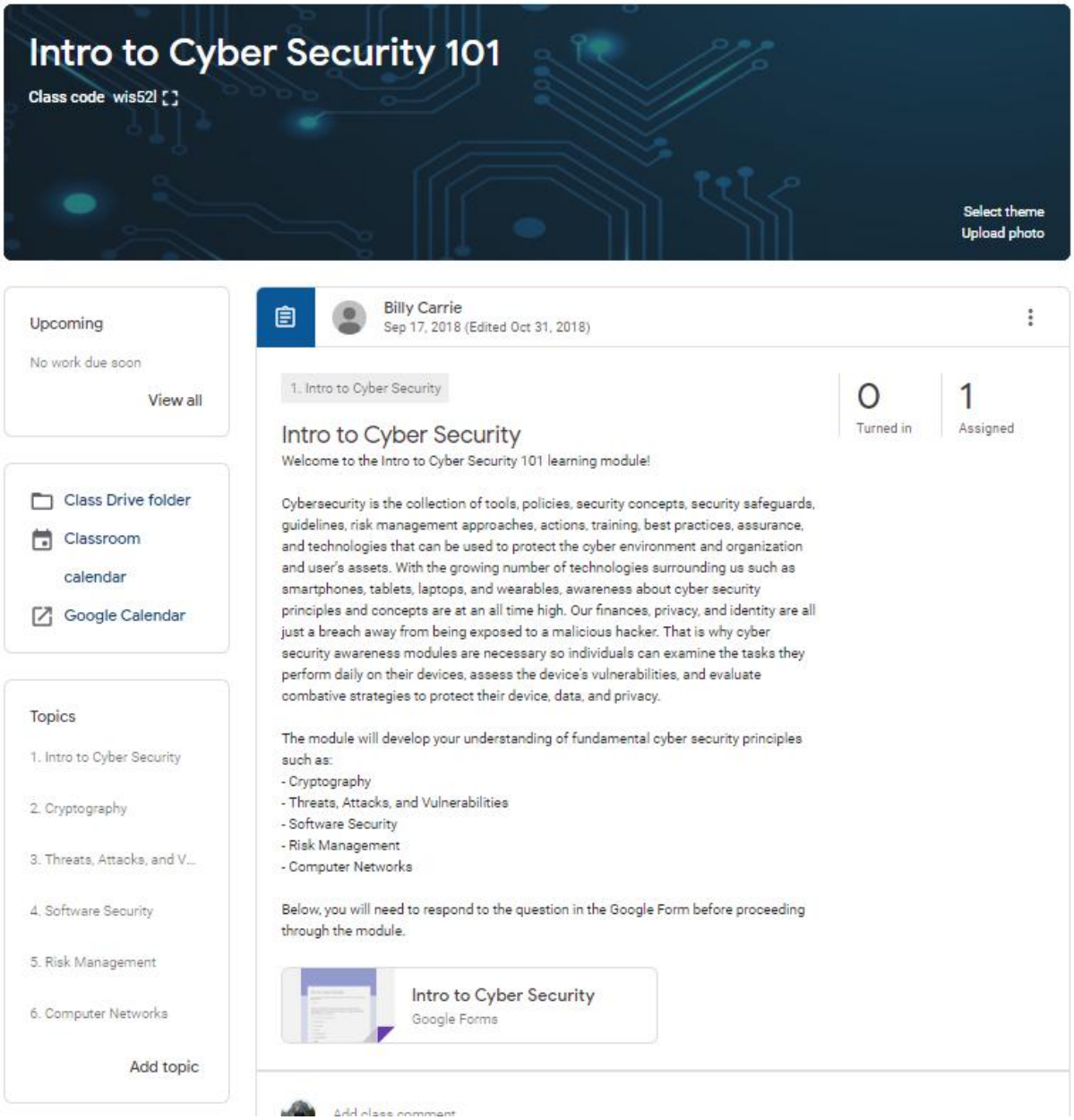

Figure 1. Intro to Cyber Security in Google Classroom.

Figure 2 displays the Cryptography module contents in Google Classroom such as the videos, PDF file with module concepts in text, assessments, and lab activity. Image 2 depicts the Cryptography assessment in Google Forms used to measure student's expertise before and after they complete the module. Image 3 shows the Cryptography lab that

students will perform to receive hands on experience with applying the concepts they have learned throughout the module.

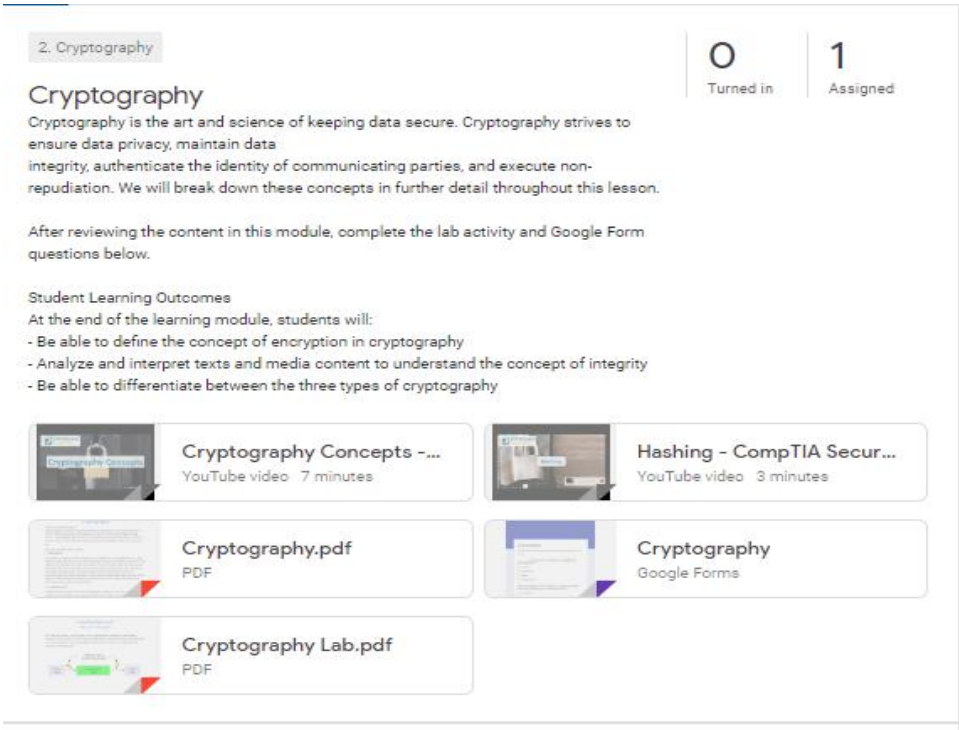

Figure 2. Cryptography Module

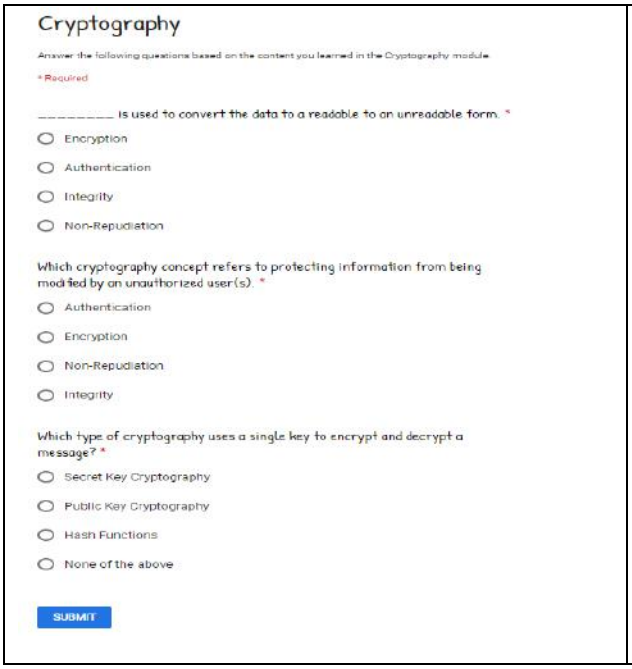

Figure 3. Assessment

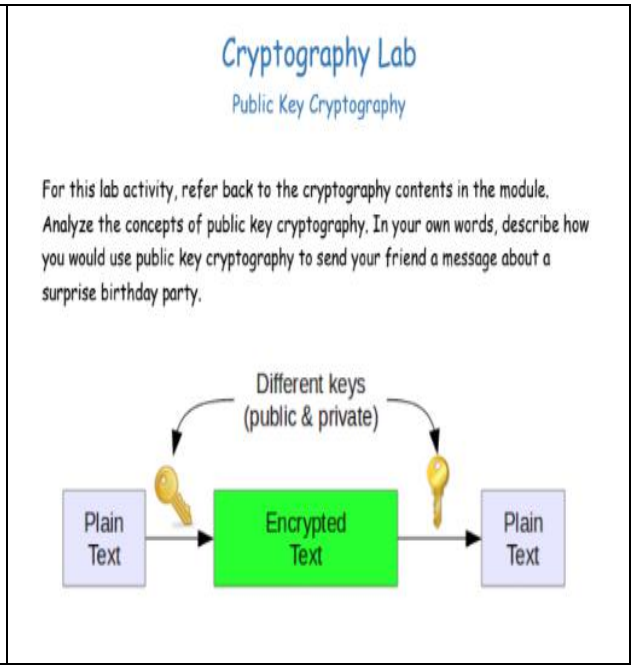

Figure 4. Sample Lab

We were able to implement a sub-set of Dupuis' student learning goals to create some of the course content such as components of computer networking and concepts involving encryption. The assessments and labs created in Google Forms (Figure 3) within the learning modules can be attributed to Dupuis' study and the multiple means of action and expression (MMAE), an UDL application framework. The images in the PDF file (Figure 4) and the YouTube videos (Figure 2) within the modules were implemented into the course based on Paivio's Dual Coding, Mayer and Anderson's Contiguity Principle, Howard Gardner's Multiple Intelligences, multiple means of representation (MMR), and multiple means of engagement (MME) to incorporate different media types and cater to different learner types.

The topics mentioned in the two cyber-security courses which include threats, attacks, vulnerabilities, risk management, cryptography, software security, and computer networks were selected based on the CompTIA Security+ and Network+ certification exam objectives. Each topic above is seen to be an important component to cyber-security efforts today in keeping personal identifiable information and intellectual property safe from hackers. Each topic featured its own learning module which included definitions, concepts, and applications to help the users learn more about cyber-security.

Each topic's structure is similar to the Cryptography depicted in Figured 1-4 above. For example, the Computer Networks module contains three Professor Messer YouTube videos, assessments, lab activity, and PDF file with definitions and concepts of computer networks. The users are provided a pre-assessment to gauge their understanding of content before accessing the learning module's contents. The three videos focused on different areas within computer networks such as routers, firewalls, wireless authentication security, and penetration testing. There is a PDF file containing definitions of computer network concepts such as firewalls, wired/ wireless connections, and spoofing in text format. A post-assessment is available to gauge the user's expertise of computer networks after reviewing the course contents. To apply what the user has learned, a lab activity is available for users to perform actions such as accessing their Wi-Fi connectivity settings and analyzing the details of the security encryption that their phone is currently using such as network speed, IP address, etc.

CONCLUSION

Through implementation of credible cyber-security concepts and instructional design principles, we constructed two cyber-security courses in Google Classroom in efforts to overcome the shortage of cyber-security awareness materials publicly available. With refinements made to the course content such as updating the content & tasks in the assessments and labs, we believe the courses will be sustainable and effective for instructing individuals about cyber-security concepts throughout the nation. Looking ahead, we plan to refine course assessments by including questions in short-answer format to analyze in-depth understanding of course content. We intend to expand upon current course content and incorporate additional cyber-security concepts to instruct users and keep the information up-to-date as technology changes at a rapid pace. Also, we were unable to evaluate the effectiveness of the courses in increasing cyber-security expertise due to time constraints. Therefore, to measure the effectiveness of the two courses, we plan to use human subjects and examine their pre/ post assessments in the course modules. While our course is targeted toward younger students, we aim to design a module more appropriate for adult learners and incorporate standard content such as offered by the SANS institute.

REFERENCES

Achkovska-Leshkovska, E., & Spaseva, M. S. (2016). John Dewey's educational theory and educational implications of Howard Gardner's multiple intelligences theory. *International Journal of Cognitive Research in Science, Engineering and Education/IJCRSEE, 4*(2), 57-66.

Al-Azawei, A., Parslow, P., & Lundqvist, K. (2017). The Effect of Universal Design for Learning (UDL) Application on E-learning Acceptance: A Structural Equation Model. *The International Review of Research in Open and Distributed Learning, 18*(6).

Baturay, M. H. (2008). Characteristics of basic instructional design models. *Ekev Academic Review, 12*(34), 471-482.

Defensenews (2018). https://www.defensenews.com/pentagon/2018/11/14/a-crisis-of-national-security-new-report-to-congress-sounds-alarm/

Dupuis, M. J. (2017). Cyber Security for Everyone: An Introductory Course for Non-Technical Majors. *Journal of Cyber-security Education, Research and Practice, 1*(3).

Endicott-Popovsky, B. E., & Popovsky, V. M. (2014). Application of pedagogical fundamentals for the holistic development of cyber-security professionals. *ACM Inroads, 5*(1), 57-68.

Parrish, P. E. (2009). Aesthetic principles for instructional design. *Educational Technology Research and Development, 57*(4), 511-528.

Sangsawang, T. (2015). Instructional design framework for educational media. *Procedia-Social and Behavioral Sciences, 176,* 65-80.

Scheponik, T., Sherman, A. T., DeLatte, D., Phatak, D., Oliva, L., Thompson, J., & Herman, G. L. (2016). How students reason about Cyber-security concepts. Paper presented at the Frontiers in Education Conference (FIE), 2016 IEEE.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Wilson, K. S., & Kiy, M. A. (2014). Some fundamental cyber-security concepts. IEEE access, 2, 116-124.

Woods, R. (2015). Georgia Department of Education SLO Operations Manual.

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2016). The role of instructional design in persuasion: A comics approach for improving cyber-security. *International Journal of Human-Computer Interaction, 32*(3), 215-257.