Cybersecurity

Ryan Cryderman, Morgan Lindsey, Alyssa Mulvihill, Kimberly Parson, Samantha Potter,

Brenda Sanchez, and Dylan Waddle

American College of Education

DL5723: Applying Learning Theories in ID

Dr. Tiffany Oakes

February 5, 2023

Cybersecurity

As technology continues to grow and develop, so does the need for cybersecurity. Cybersecurity is crucial, as it safeguards personal data from theft and loss. With education including more technology, it is essential that educators are trained in cybersecurity. These trainings help to keep both student and staff information safe. A virtual training was created to educate high school teachers on what cybersecurity is and how to protect themselves and their students. The following paper will overview the audience and theoretical basis for this training, illustrate the course plan via a concept map, and describe the assessment component.

Audience

The recipients of this training are 20 American high school teachers. All the teachers have at least a master's degree and speak English fluently. Personnel records reveal that the teachers completed a basic cybersecurity training two years ago, but the school's technology department determined that retraining is essential for compliance. Furthermore, when the teachers were surveyed, all of them reported that they place a high importance on cybersecurity.

As the learners regularly have professional development sessions via Zoom, they are familiar with virtual training. However, differences exist in work styles. In one of the previous professional development sessions, 15 teachers stated that they enjoy working in groups, while the remaining five teachers reported that they prefer to work alone. The intention for the training is that it will employ group learning, so a plan will be in place to ensure that the voices of all learners are heard. Learners will be encouraged to communicate with their groups in the Discord discussion boards, and the course facilitator will check in with the groups to make sure they are functioning well. As Brookes et al. (2021) suggested, effective groups allow all members to feel heard, safe, and respected.

Theories

There are many different learning theories in education. When designing training and coursework, designers will implement different learning theories into their design. The following section will discuss social exchange theory and group learning theory, two learning theories which were integrated into this training.

Social Exchange Theory

One prominent learning theory is the social exchange learning theory. Homans's social exchange theory was developed in 1961 and argued that exchanges between individuals are a social process. These exchanges and relationships are built on a cost-versus-benefit scale. Individuals will continue a relationship or exchange if the benefits outweigh the cost (Almuqrin, 2022). This theory also proposes that the value of the cost is dependent on the individual and their prior experiences. Accordingly, this theory is often utilized in educational settings and with group work. Within this training course, the social exchange theory influences the learning activities and assessments. For example, *Game of Threats*, an activity in the course, will present learners with choices that may or may not prevent a cyberattack. Each choice will have a corresponding cost and benefit, which will then contribute to the outcome of the scenario. Thus, learners will develop their critical thinking skills in preparation for real cyberattacks.

Group Learning Theory

Another learning theory in education is the group learning theory. This theory asserts that individuals work best when in groups. Within these groups, individuals can collaborate and communicate toward a common goal. When working in groups, individuals can ask questions, receive feedback, challenge ideas, and reflect on results (Vora & Markóczy, 2012). Indeed, working in groups has many benefits. Within this training course, the group learning theory will

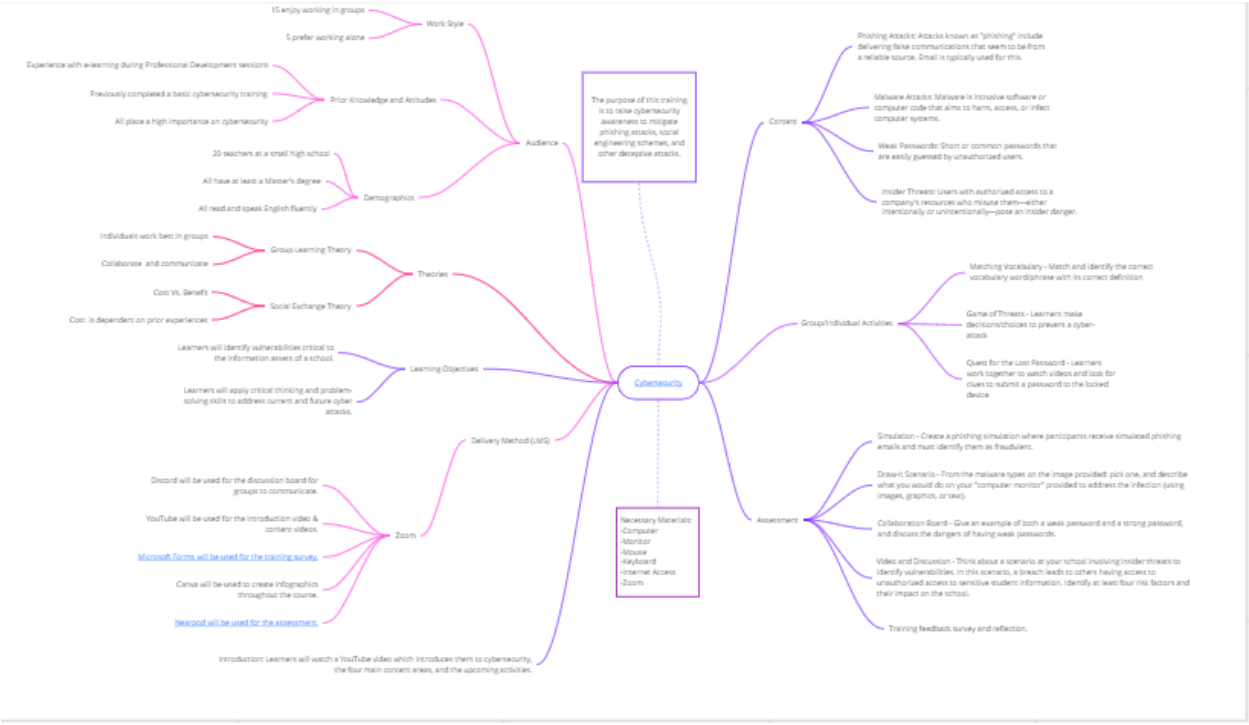
support the learning activities and assessments. For example, in *Quest for the Lost Password,* learners will work collaboratively to find clues in a series of videos. However, when learners play *Matching Vocabulary*, a word identification activity, they will have the option to work independently. This option will appeal to the preferences of the teachers who prefer to work alone. Nevertheless, the activities in the training will mainly promote group learning.

Concept Map

The cybersecurity training has many key components which will contribute to the success of the learners. Figure 1 is a concept map of the one-hour virtual training. This concept map displays all components of the training, including the learning objectives, content covered, learning activities, and assessments.

Figure 1

Concept Map for Cybersecurity Training



Note: An enlarged version of the concept map may be found here.

Assessment

To ensure that the teachers have a firm grasp on the content of the training, an assessment was created. Taking place near the end of the training, this assessment incorporates content from throughout the session. The following section will outline the purpose and objectives of the assessment, as well as the tasks to be assessed and the performance criteria.

Purpose and Objectives

The purpose of this training is to raise cybersecurity awareness to mitigate phishing attacks, social engineering schemes, and other deceptive attacks. Therefore, learners should be able to identify the four most common cybersecurity threats. In addition, learners should be able to use critical thinking and problem solving to analyze, assess, and make recommendations for future occurrences. Within each of the four threat categories, learners will be able to identify and address the threat using critical thinking and problem solving. By the end of the training, learners should report a high level of confidence in their ability to recognize a potential threat and prevent it from happening in the future. Learners will have the opportunity to report their confidence in an end-of-course survey.

Tasks to be Assessed

In the last 15 minutes of the training, learners will be assessed on the four types of cyberattacks that were discussed in the training. Throughout the course, learners will gain knowledge on phishing, malware, weak passwords, and insider threats. Therefore, the purpose of the assessment is to check their understanding of these cyberattacks.

Overall Steps of Assessment

First, learners will complete four key tasks, with each one devoted to one of the cyberattack types. Learners will complete these tasks in Nearpod. Then, learners will return to

the Zoom meeting to reflect on their learning with the group. In accordance with group learning theory, individuals can ask questions, receive feedback, and reflect on results on the assessment while expanding their knowledge in a collaborative way (Vora & Markóczy, 2012). The last part of the assessment is the end of course survey, which will take place in Microsoft Forms. The survey will give learners the opportunity to share their final thoughts on the training and share how confident they are in recognizing the cyberattacks. The following paragraphs will describe the tasks in greater detail.

Phishing

In the Phishing activity, the learners will take a quiz which tests their ability to identify phishing emails. Learners will review emails similar to what they might receive to their district email accounts. There will be a total of five emails for learners to review. Learners will analyze each email to determine if the email is credible or if it is a phishing email. To determine this, learners will examine key components commonly found in phishing emails, including unusual greetings, grammar and spelling errors, inconsistencies in the email address, unusual attachments, threats, and feelings of urgency. Learners must successfully identify four of the five e-mails to meet the requirements of this section. As ElSaryary (2021) explained, an authentic assessment should relate to a real-life task that centers on the learner. Thus, the Phishing activity will represent an authentic component of the assessment.

Malware

In the Malware activity, the learner will use critical thinking to address a malware issue. Given an image depicting several types of malware, the learner will be instructed to select a type of malware and describe their course of action to address the threat. The learner will draw on a virtual computer monitor using images, graphics, or text to convey the plan of action. Thus, the

learner will have multiple means of expression for demonstrating their competency within the activity. Furthermore, as suggested by Villaroel et al. (2021), this task adds an element of challenge to the assessment by asking learners to create a way to address the selected malware.

Weak Passwords

During this activity, learners will have the opportunity to generate their own ideas for passwords. They will use their new knowledge gained in the training to identify specific characteristics that classify passwords as strong or weak. In the discussion box, learners will submit their ideas for passwords and discuss the potential dangers of having a weak password. This portion of the assessment allows learners freedom of choice, although they will still need to think critically to apply and illustrate their knowledge of strong password characteristics.

Insider Threats

In this task, the learner will interact with a short informational video on insider threats. Questions are asked throughout the video to check for understanding. For example, the video defines why insider threats are hazardous (Security Innovation, 2018). Learners are asked to answer a corresponding question about this subject. After the video, learners will analyze and assess a real-world scenario involving insider threats to identify vulnerabilities. An image and information will be provided to the learner. The scenario will involve the actual school and a breach that leads to others having unauthorized access to sensitive student information. Learners will identify the risk factors and their impact on the school. In line with social exchange theory as described by Almuqrin (2022), this activity will encourage learners to reflect on the potential costs of leaving data exposed. The possible vulnerabilities will be data sharing, unauthorized use of devices, leaving a device unattended when logged in, sharing of credentials, and an unattended USB left with sensitive student information. After the learner identifies the

vulnerabilities in the case, they will provide recommendations for preventing future occurrences of each vulnerability. They will reflect, share, and discuss their findings and recommendations with their groups.

Performance Criteria

To determine if the learner is successful, an authentic formative assessment will be used. As described previously, there are four main activities within the assessment. These activities will use both quantitative and qualitative measures. In the Phishing activity, a quantitative assessment, the learner must receive an 80% or higher to move on to the next segment. If the learner scores below 80%, the learner will go back to the start of the activity to complete it again. In regard to the three qualitative assessments, learners should be able to demonstrate a concise yet thorough understanding of the content in the applied activity. Each individual activity provides learners with instructions and criteria. As recommended by Zaim et al. (2020), the activities will allow learners to demonstrate their competency and learning progress. After all activities are complete, learners will reflect collectively on their learning in a Zoom discussion.

At the end of training, learners will be asked to take a poll and an end of course survey. The poll asks learners to rate themselves on how confident they are in identifying threats in the workplace. A scale of 1 to 10 will be used, with 10 representing the highest level of confidence. This poll will allow the instructor to identify learners with a low level of confidence. Then, the instructor will be able to provide support and additional resources to improve the confidence of these learners. The end of course survey will help learners reflect on what they learned in the training and provide valuable feedback to improve the course.

Thus, the assessments and survey will not only provide feedback to the learner, but they will also help the instructor of the course support struggling learners. Furthermore, the Zoom

discussion component will allow learners to learn as a group. For further illustration of the assessment, the links in the Appendix will provide access to a brief screencast overview of the assessment, a preview link for the assessment, and the link that students would use to access the assessment.

Conclusion

With technology developing and becoming a key component of instruction, the need for cybersecurity is essential. Cybersecurity helps to ensure data stays protected. With the proper training, educators can ensure that their information and their students' data is secure and protected. Utilizing social exchange theory and group learning theory, this training will help these teachers become more informed about vulnerabilities and more able to address threats when they arise. The assessment at the end will measure the success of the training. Resultantly, the high school will provide a safer environment for its employees and its students.

References

Almuqrin, A. H. (2022). Social exchange theory and theory of reasoned action affecting knowledge sharing: A case from Saudi Arabia. *Journal of Information Studies & Technology (JIS&T)*, *2022*(1), 1–16. https://doi.org/10.5339/jist.2022.5

Brookes, D. T., Yang, Y., & Nainabasti, B. (2021). Social positioning in small group interactions in an investigative science learning environment physics class. *Physical Review Physics Education Research, 17*(1), 1–13. https://doi.org/10.1103/PhysRevPhysEducRes.17.010103

ElSayary, A. (2021). Transdisciplinary steam curriculum design and authentic assessment in online learning: A model of cognitive, psychomotor, and affective domains. *Journal of Turkish Science Education (TUSED), 18*(3), 493–511. https://doi.org/10.36681/tused.2021.86

Security Innovation. (2018, July 11). *Insider threats in 2 minutes* [Video]. YouTube. https://www.youtube.com/watch?v=QXnNkSeT6dM

Villarroel, V., Bruna, D., Brown, G. T. L., & Bustos, C. (2021). Changing the quality of teachers' written tests by implementing an authentic assessment teachers' training program. *International Journal of Instruction, 14*(2), 987–1000.

Vora, D., & Markóczy, L. (2012). Group learning and performance: The role of communication and faultlines. *International Journal of Human Resource Management, 23*(11), 2374–2392. https://doi.org/10.1080/09585192.2011.616523

Zaim, M., Refnaldi, Arsyad, S. (2020). Authentic assessment for speaking skills: Problem and solution for English secondary school teachers in Indonesia. *International Journal of Instruction, 13*(3), 587-604. https://doi.org/10.29333/iji.2020.13340a

Appendix

1. Nearpod Assessment Screencast
2. Nearpod Assessment Preview
3. Nearpod Assessment Student-Paced Link (Select “Join as a Guest”)