Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Assessing the Social Validity of Canvas LMS-Based Cybersecurity Online Modules in High School STEM Classes

Gahangir Hossain

gahangir.hossain@unt.edu

University of North Texas

Mikyung Shin

Illinois State University

Brigette Whaley

West Texas A&M University

Mehnaz Afrose

West Texas A&M University

Enamul Hassan

University of North Texas

Research Article

Keywords: Bayesian cumulative link mixed effects model, Canvas, Cybersecurity Education, High school, Word networks

Posted Date: July 27th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10107954/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Assessing the Social Validity of Canvas LMS-Based Cybersecurity Online Modules in High School STEM Classes

Gahangir Hossain[1], Mikyung Shin[2], Brigette Whaley[3], Mehnaz Afrose[3], Enamul Hassan[1]

[1] University of North Texas

[2] Illinois State University

[3] West Texas A&M University

Abstract

The purpose of this study was to evaluate the overall social validity of Canvas learning management system-based cybersecurity online modules among 30 students in STEM high school classes and investigate whether students' technology self-efficacy influences this social validity. We employed a cross-classified Bayesian cumulative link mixed effects model to account for the Likert scale rating on social validity. The cumulative log odds rating 4 or lower showed significantly more frequent responses compared to rating 5 (logit coefficient = 6.09). The odds ratio for this type of technology self-efficacy was 3.70, indicating that the odds of rating higher social validity after using Canvas LMS-based online modules were statistically significant by 3.70 times per one scale increase on the self-efficacy response scale (logit coefficient = 1.31). Using the Leiden algorithm, the word network graphs showed small to moderate modularity and assortativity. In the open-ended responses, words such as "cybersecurity, " "metaverse," and "online" showed a relatively high degree of centrality connected to positive sentiment words. Words such as "information," "long," "video game," and "metaverse" were connected with negative sentiment words. centralities related to the least preferred cybersecurity topics. These

word correlation network results validate the commonly observed students' responses and their patterns in the unstructured responses.

Keywords: Bayesian cumulative link mixed effects model, Canvas, Cybersecurity Education, High school, Word networks

Assessing the Social Validity of Canvas LMS-Based Cybersecurity Online Modules in High School STEM Classes

Introduction

Cybersecurity is one of the significant issues in the US that can threaten people's daily lives and requires exponential attention across all societal domains (Finnemore & Hollis, 2016). Nowadays, human beings are facing increasing cybersecurity challenges due to the widespread use of online devices, such as smartphones, computers, and interconnected apps (Al-Turjman & Salama, 2021). At every school, most teachers and students are inevitably using online tools for teaching and learning content, which is also an essential component for meeting the needs of diverse populations (Ribble, 2015). Thus, cybersecurity issues have become an integral part of everyone's lives, and all individuals should be aware of these issues and discuss how to prevent and address related cybersecurity concerns.

Based on the urgent need to raise the public's cybersecurity awareness, the research team developed cybersecurity online modules using the Canvas learning management system (LMS) for high school students in science, technology, engineering, and mathematics (STEM) classes. These online modules offer a flexible and accessible avenue for individuals seeking to acquire

comprehensive knowledge and practical skills in safeguarding digital assets. In selecting a wide range of cybersecurity topics, the authors reviewed and considered national, state, and local education standards related to cybersecurity curriculum (Authors, 2025a). Thus, from basic security principles to advanced threat detection and mitigation strategies, we aimed to incorporate instructional design components, including videos, games, hands-on activities, online discussions, and quizzes, within the modules.

Literature Review

Cybersecurity Programs for Students

High school cybersecurity programs are strategically integrated into the STEM curriculum, a deliberate approach that ensures alignment with core educational principles (Aydeniz, 2018). The curriculum of these programs includes ethical hacking, network security, data protection, and the intricacies of cyber threats (Deylami et al., 2015). The purpose of this curriculum is to equip students with strong knowledge in both technology and fundamental principles of cybersecurity (Mouheb et al., 2019). These programs integrate cybersecurity into the entire educational journey of students, while also helping them build a strong ethical foundation and a deep understanding of security principles (Sussman, 2023).

Researchers incorporated various instructional designs to support students' active engagement in learning cybersecurity issues online. For example, one notable cybersecurity program is game-based learning, a mechanism for cybersecurity education for high school students (Jin et al., 2018). Game-based learning is a teaching method that utilizes interactive and engaging games to enhance students' knowledge (Lampropoulos et al., 2019). This approach can be applied in teaching cybersecurity concepts in a way that a game may stimulate, including a

scenario where students need to identify and defend various cyberattacks, and in doing so, they must apply their knowledge to protect virtual systems. Structured as immersive programs, students explored the camps' evolving cyber threats and how to protect against the current challenges. Participating students could engage in activities such as ethical hacking, incident response simulations, and cryptography challenges, fostering a dynamic learning environment. Beyond technical skills, students could improve their understanding of ethical considerations and expand their sense of responsibility in handling cybersecurity issues.

Use of Canvas as an LMS

Researchers demonstrated the potential efficacy of using Canvas as an LMS for online teaching and training. For example, Magalhães et al. (2023) used Canvas for healthy eating interventions for children. They conducted a two-iteration mixed-method study that evaluated the perception of usability and feasibility of this LMS and found it particularly useful for elementary school children. They have utilized it in an online healthy eating intervention that promotes self-regulation among nine sixth-grade children and their mothers. Users explored the platform and performed various tasks, including commenting on forums, attending conferences, and uploading files. Participants positively assessed the platform's usability and enjoyability. They identified several factors that influenced their engagement and motivation, such as the topic's relevance, the possibility of combining it with other tasks, peer interaction, and the help provided.

More recently, other researchers investigated the effectiveness of Canvas in promoting interactive online learning. For example, Santiana et al. (2021) investigated the perception towards the use of Canvas among 77 college students enrolled in the Technology Enhanced Language Learning course. The results showed that students accessed Canvas mostly to join online learning activities such as reading the learning modules, joining online discussions, and

completing assignments. The participants shared that Canvas was an easy-to-use platform with supporting features that encouraged their motivation to learn and provided them with opportunities for interactive learning experiences. However, Oudat and Othman (2024) pointed out that Canvas had technical and accessibility issues for dyslexic and non-native English speakers. In maximizing the learning opportunities through LMSs such as Canvas, software developers and companies should consider issues related to accessible interfaces and data security and include multiple options to support technical barriers for diverse users (Creed et al., 2024).

Purpose of Study and Research Questions

The purpose of this study is twofold: (1) to evaluate the overall social validity of Canvas LMS-based cybersecurity online modules, assessing 30 high school students' social validity of the intervention, and (2) to investigate whether students' technology self-efficacy influences this social validity. Social validity is the degree of social acceptance and appropriateness regarding the intervention's goals, interventions, and dependent variables to participants such as students (Wolf, 1978). Assessing social validity in behavioral research is highly recommended and one of the quality indicators (Huntington et al., 2023). Pan (2020) highlighted that students' technology self-efficacy was related to their attitude toward technology-based self-directed learning. Thus, we assumed that technology self-efficacy could influence students' social validity. Specifically, we addressed the following research questions:

1. How do high school students rate the social validity of learning cybersecurity through Canvas LMS-based online modules?

2. How do high school students' social validity ratings vary by their technology self-efficacy awareness?

3. What do high school students share opinions on the open-ended social validity questionnaire?

Methods

Participants and Setting

Thirty high school students in STEM classes at a public high school in the southern United States participated in this cybersecurity training. Table 1 summarizes the demographic information of participants. Of the 30 high school students, their grades ranged from 9 to 12, with 20 male students (67%) and 9 female students (30%). More than half the participants were White or Caucasian (n = 18; 60%), followed by Black or African American (n = 5; 17%), Multiracial (n = 2; 6.7%), American Indian/Native American or Alaska Native (n = 1, 3.3%), and Native Hawaiian or Other Pacific Islander (n = 1; 3.3%). Regarding the daily time used for mobile devices, the largest number of students (n = 11; 37%) spent more than 6 hours, followed by 3 to 6 hours (n = 8; 27%), less than 1 hour (n = 7; 23%), and 1 to 3 hours (n = 4; 13%). They used computers (n = 14; 47%) and smartphones and computers together (n = 13; 43%) most frequently at school or home, respectively.

Two female teachers with over 10 years of experience in STEM classes served as instructors for the project. Both were White or Caucasian, and one teacher had Hispanic/Mexican origin. In continuous collaboration and partnership with schools in the Texas Panhandle, we invited high school STEM teachers to the current workshop upon receiving a letter of support from the school or local Independent School Districts, following the guidelines of Institutional Review Boards (IRBs) form the West Texas A&M University, Canyon, TX, and The University of North Texas, Denton, TX.

Cybersecurity Online Modules

The researchers have reviewed all the latest cybersecurity curricula, standards, and guidelines for students in K-12 grades to select content and topics aligned with the currently recommended practices. For example, the team has reviewed cybersecurity standards by the National Institute of Standards and Technology (Pascoe et al., 2024) and the Computer Science Teachers Association (2017). Then, based on reviews of the latest academic journal articles (e.g., Chen et al., 2021; Ibrahim et al., 2024), the team selected eight topics on cyber ethics, privacy, forensics, and investigation (Unit 1), cyber threats analysis: Concept of cyber data (Unit 2), basic ethical hacking: What do hackers do through wireless/ mobile networks (Unit 3), cybersecurity through games-based learning (Unit 4), securing networks, internet, the web/cloud, and email accounts, detection, and protection with tools (Unit 5), social media security, and educational tools for kids learning cybersecurity (Unit 6), blockchain, encryption-decryption, authentication passwords, multi-factor, and single-sign-on (Unit 7), metaverse and cybersecurity (Unit 8), cybersecurity frameworks/ career, standards (Unit 9), and review and assessment (Unit 10). In each unit, we provided a self-regulatory to-do checklist, which served as explicit prompts for students' expected learning behaviors to complete and master to move to the next lesson (e.g., read the unit objectives, watch the sequenced videos, complete the unit quiz at an 80% mastery level with multiple trials, engage in built-in online hands-on activities and simulations, share reflections in the group discussion, check completed for each step-by-step to-do list).

Before the development of the online modules, the research team contacted the education specialists, school administrators, and teachers in STEM fields, including the career and technical education department, and invited them to a two-day online workshop. Panels evaluated the content validity of cybersecurity basic topics. The content included phishing and spam emails, malware, ethics, privacy, policy, and assessment.

Survey Questionnaires

Researchers developed survey questionnaires to measure students' social validity. After reviewing previous studies assessing students' social validity in technology-incorporated intervention studies (e.g., Ives et al., 2024; Nohelty et al., 2023), we constructed five 5-point Likert scale questions related to participants' beliefs regarding improved understanding of cybersecurity, likeness of the project, improved interest in cybersecurity, generalization of the knowledge, and confidence in the cybersecurity topic. Based on previous literature on the role of users' technology self-efficacy (e.g., Saville & Foster, 2021), we constructed three additional 5-point Likert scale questions related to confidence in navigating and using different online tools and technology features, setting and following a learning sequence, and self-regulating and monitoring their behavior during online learning. Lastly, the other five open-ended questions included social validity questions such as the most and least preferred topics of the online modules, cybersecurity topics they want to learn in the future, how online programs allowed them to share thoughts on cybersecurity, and overall experience with the project.

Data Collection

After receiving approval for the current research from the Institutional Review Board, we recruited schoolteachers interested in training their students in STEM high school classes. We sent invitation emails to the local independent school districts (ISDs), and a partnership agreement letter from the school or local ISDs was completed. Later, we arranged a time to introduce the current project to the teachers at the school. School teachers were invited to attend an initial meeting on delivering parental consent to students. The teachers learned the purpose of the current project and agreed to maintain the confidentiality of those asked to participate in the study. Training for the high school teachers was provided individually for a week (maximum of

five working days). Classroom teachers distributed and collected the parents' consent and child assent forms. The 9 through 12 students who submitted parental consent were only invited to participate in this study. In the STEM class, students completed the cybersecurity online modules for about 30 minutes (sequenced chunks of 5 to 10-minute videos per module), 10 sessions, and about two to three sessions per week throughout the fall semester of 2023. Each teacher guided students while they used Canvas LMS. After completing all modules, each student completed an online survey distributed via the Qualtrics platform within the last online module.

Data Analysis

R code used to analyze students' responses to survey questionnaires is available at https://cybersecurity-basic.netlify.app (Authors, 2025b). We initially asked questions through an ordinal 5-point scale, yet no students rated "strongly disagree," leading to a 4-point scale in the analysis. Assuming each rating response (Level 1) belongs to items (Level 2) and students (Level 2), we employed a cross-classified Bayesian cumulative link mixed effects model (CLMM) to account for the Likert scale rating on social validity and considered the proportional odds model, assuming the logit coefficients for each predictor variable are same across the categories of the ordinal rating response (Liu, 2022). Bayesian approaches are recommended when sample sizes are small, improving model estimation in case of greater complexity in the random effect structures and reducing the probability of Type I errors (Cavanaugh et al., 2023). We used "weakly informative priors" in the model. Winter and Bürkner (2021) stated that the use of 'weakly informative priors' was generally recommended in a study of small samples to prevent overfitting and allow the model to be more conservative than the frequentist models with noninformative priors. Additionally, following Bürkner and Charpentier's recommendation

(2020), we modeled the monotonic effects of ordinal predictors (monotonically increasing or decreasing relationship with the response rating) using the following equations:

Level 1: $\text{logit}\left[\pi_{kij}\left(Y_{ij} \leq k\right)\right] = \ln\left(\frac{\pi(Y_{ij} \leq k)}{\pi(Y_{ij} > k)}\right) = \alpha_k - \beta_{0ij}$

Level 2: $\beta_{0ij} = \gamma_{00} + \gamma_{01}\text{mo}\left(navigating_using_j\right) + \gamma_{02}\text{mo}\left(learning_sequence_j\right) + \gamma_{03}\text{mo}\left(self_regulation_j\right) + u_{0i} + u_{0j}$, with $u_{0i} \sim \mathcal{N}(0, \tau_{0i}^2)$, $u_{0j} \sim \mathcal{N}\left(0, \tau_{0j}^2\right)$.

In the equations, $\text{logit}\left(\pi_{kij}\right)$ is logit link for the cumulative probability, $\pi_{kij}(x) = P\left(Y \leq k \mid x_1, x_2, \ldots, x_p\right)$, of being at or below a particular cut point with *k* (*k* = 1, 2, and 3) for the *i*th survey item (*i* = 1, 2, …, *I*) for *j*th student (*j* = 1, ⋯ *J*). α_k indexes thresholds (i.e., cut points), and β_{0ij} is the logit coefficient, indicating a random intercept that depends on both items and students. γ_{00} to γ_{03} are level 2 logit coefficients. γ_{00} is the intercept, the overall logit or log odds of being at or below a particular rating across items and schools. γ_{01}, γ_{02}, and γ_{03} are student-level covariates predictors related to technology self-efficacy. $u_{0\text{i}}$ and $u_{0\text{j}}$ account for random deviations across items and students, assumed to be normally distributed with a mean of zero and variance of $\tau_{0\text{i}}^2$ and $\tau_{0\text{j}}^2$, respectively. This cross-classified Bayesian CLMM was fitted with the brm() function in the *brms* R package (Bürkner, 2017).

We employed word network analysis to analyze open-ended responses regarding students' experiences with cybersecurity online modules. A word network refers to how a list of words (nodes) are connected (edges) as a graph where influential nodes get more networks and neighbors (Newman, 2018). We measured important nodes through centrality. The following four centrality metrics were calculated via *igraph* (Csárdi & Nepusz, 2006): (a): degree centrality $C_D(v) = \frac{\deg(v)}{|V|-1}$, where $\deg(v)$ indexes the number of edges connected to node v, and $|V|$

presents the total number of nodes; (b) betweenness centrality $C_B(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}$, where σ_{st} represents the number of shortest paths between nodes s and t, and $\sigma_{st}(v)$ indicates the number of shortest paths passing node v, (c) closeness centrality $C_C(v) = \frac{N-1}{\sum_{v \neq u} d(v,u)}$, in which $d(v,u)$ denotes the shortest path distance between nodes v and u, and *N* is the number of nodes; and (d) eigenvector centrality $C_E(v) = \frac{1}{\lambda} \sum_{u \in V} A_{(v,u)} C_E(u)$, where $A_{(v,u)}$ is the adjacency matrix, λ is the largest eigenvalue of the adjacency matrix, and $C_E(u)$ is eigenvector centrality of node u (Bamakan et al., 2019; Yu et al., 2024). We also assigned each node to a community membership (node color) using the Leiden algorithm (Traag et al., 2019) and displayed the word co-occurrence through the width of edges.

Following the procedures suggested by Authors (2023), we implemented the text preprocessing of the selected columns in the imported Excel file. We have categorized students' written response columns into three different corpora (i.e., opinions indicating the most preferred topics, the last preferred topics, and overall reflections). For the preprocessing, we tokenized text, converted tokens to lowercase, removed stop words, and set the minimum length of the token as two characters via the *quanteda* R package (Benoit et al., 2018). Then, we constructed a document-feature matrix and analyzed co-occurring words within each student's open-ended response via *widyr* (Robinson & Silge, 2022). A workflow was used through *TextAnalysisR* (Shin, 2025) to complete these text-mining procedures.

Results

High School Students' Social Validity and Technology Self-Efficacy

Table 2 summarizes the results of the Bayesian CLMM on high school students' social validity and monotonic effects of technology self-efficacy after learning cybersecurity through Canvas LMS-based online modules. The online outputs (see https://cybersecurity-

basic.netlify.app) show that Rhat values for all logit coefficients were 1, and effective sample size measures (i.e., Bulk_ESS and Tail_ESS) showed Markov chain Monte Carlo convergence. Fig. 1 depicts the visualization of posterior predictive checks and indicates a good fit between the model predictions and the observed data for the ratings of 2 and 4 and a slight overestimation for the ratings of 3 and 5.

The random intercept variance for items (τ^2_{0i} = 3.38) was slightly higher than that for students (τ^2_{0j} = 2.31). Based on the proportional odds model, the average cumulative logit or log odds of being in the rating 2 or below was −0.62 (95% CI = −3.42 to 2.53), in the rating 3 or below with 2.53 (95% CI = −0.20 to 5.86), and the rating 4 or below with 6.09 (95% CI = 3.39 to 9.46) across items and students. Odds ratio (OR) results validated limited responses for the rating 2 (OR = 0.54, 95% CI = 0.03 to 12.57) and more frequent responses for the rating 3 or lower (OR = 12.56, 95% CI = 0.81 to 349.85) compared to rating 4 or 5. In particular, the cumulative log odds rating 4 or lower showed significantly frequent responses compared to rating 5 (OR = 441.18, 29.55 to 12777.27).

Monotonic effects related to ordinal technology self-efficacy predictors were also estimated. When high school students felt more confident in navigating and using different online tools and technology features, their rating on the social validity measure was slightly positive with a logit coefficient of 0.16 (95% CI = 0.56 to −0.95), indicating students' higher technology self-efficacy minimally increased the odds of rating higher social validity by 17% (OR = 1.17, 95% CI = 0.39 to 3.53). When students were likely to set and follow a learning sequence effectively when using online tools and technology, their rating on social validity was also slightly increased with a logit coefficient of 0.87 (95% CI = 0.72 to −0.44). There were odds of evaluating with a higher social validity rating by 2.40 times for every one-scale increase

in this technology self-efficacy (OR = 2.40, 95% CI = 0.64 to 11.58). The logit coefficient for students' technology self-efficacy related to self-regulation and monitoring their behavior during technology instruction was 1.31 (95% CI = 0.06 to 2.78). The odds ratio for this type of technology self-efficacy was 3.70, indicating that the odds of rating higher social validity after using Canvas LMS-based online modules were statistically significant by 3.70 times per one scale increase (95% CI = 1.06 to 16.09).

Opinions on the Open-Ended Social Validity Questionnaire

Undirected word networks were constructed. As shown in Fig. 2, regarding questions about preferred cybersecurity topics and content, a graph of word correlations revealed 36 nodes and 188 edges with a density of 0.30. This graph included words that appeared at least twice in each student's response and had a correlation coefficient of at least 0.32 between those word pairs. The average geodesic distance (i.e., shortest paths between two nodes) was 2.66, and the length of the longest geodesic was 6. The global transitivity (i.e., the probability that adjacent nodes were connected) was 0.51, with an average local transitivity of 0.57, indicating moderate clustering in the network. The graph also showed a mild community structure of a graph (modularity = 0.39), resulting in 13 community clusters using the Leiden algorithm and a slight similarity with connected nodes (assortativity = 0.34). Unit topics related to "cybersecurity, " "metaverse," and "online" in community 2 demonstrated relatively higher degree centralities of 16 and 20, connected to positive sentiment words such as "interesting," "enjoy," and "good." Words such as "game," "types of hackers," and "cyber ethic" also represented online activities that were favorable to participants, connected to words such as "favorite," easy," "key" and "component." One quote by a 12th male student, "I liked learning about all of the different key components that went into protecting your personal information online, and learning about the

three different types of hackers and their motives," corroborates the importance of these keywords in positioning their preferred cybersecurity topics. Moreover, "online" (124.88) and "personally" (83.03) were shown to be the words with the highest two betweenness centralities. The word "online" also had relatively higher associations with "people" (0.80) and "information" (0.45) than with other words, indicating the active bridging roles within the network.

Fig. 3 shows word networks on students' perspectives toward the least preferred regarding cybersecurity topic and content. The graph represented 30 nodes and 164 edges with 0.38 density among words with at least a co-occurrence of 2 and a correlation of 0.32. Both global (0.50) and average local (0.50) transitivity showed similar patterns with questions on preferred cybersecurity topics. With a mild modularity of 0.33 and a somewhat small assortativity of 0.18, the network led 11 community clusters. Words such as "information," "long," "video game," and "metaverse" showed relatively higher degree (14 and 20) centralities and were connected to negative sentiment words of "least" and "dislike." Aligning with these results, students expressed their dislike for the long content in the video or digital materials and the discussion section on Canvas LMS cybersecurity online modules. Students find the unfamiliar cybersecurity topic to be the least interesting. For example, one 12th-grade female student shared, "I did not really enjoy the video game unit, but I think that's because I know nothing about video games, but it did teach me very much needed information."

As shown in Fig. 4, the students' open-ended responses on overall experiences showed 27 nodes and 100 edges with 0.29 density among words with at least a co-occurrence of 3 and a correlation of 0.38. The global transitivity (0.45) and average local transitivity (0.49) demonstrated moderate clustering in the network. The modularity (0.26) and assortativity (0.16)

of connected nodes led to 14 community clusters. The average geodesic distance was 2.79, and the length of the longest geodesic was 8. A positive sentiment word of "enjoy" in the community 1 group showed a high degree (20) and eigenvector (1) centralities connected with "learn" (correlation = 0.55) and "program" (correlation = 0.63). Additionally, words such as "keep," "information," and "safe" in the community 2 group demonstrated distinctive clusters among commonly mentioned responses, where "information" showed relatively higher centralities (degree = 16, eigenvector = 0.61). One 12th-grade female student underscored this positive perspective, saying, "It was fun for the most part and really opened my eyes on how to avoid being hacked. I would most likely recommend this to others so they can also understand how to avoid being hacked."

Discussion

The purpose of this study was to evaluate the overall social validity of Canvas learning management system-based cybersecurity online modules among high school students in their STEM classes and investigate whether students' technology self-efficacy influences this social validity.

High School Students' Social Validity and Technology Self-Efficacy

With our first research question, we employed cross-classified Bayesian CLMM to explore the Likert scale ratings. The social validity 5-point survey showed that students rated more frequently for the rating 3 or lower (OR = 12.56) than for rating 4 or 5. The cumulative log odds rating 4 or lower showed significantly frequent responses compared to rating 5 (OR = 441.18). No students rated "strongly disagree" for all aspects, and relatively sparse responses for "disagree" or "strongly agree." This generally positive social validity toward the Canvas LMS-based cybersecurity online modules suggests a potential instructional method to supplement the

existing high school STEM curriculum and content. Quayyum et al. (2021) found growing and rapid attention to the cybersecurity topic and concerns among school-aged children and adolescents, yet there is still a lack of research on measuring the learners' awareness of cybersecurity risk regarding their social validity. Additionally, Magalhães et al. (2023) found positive usability and feasibility of Canvas as a platform to deliver interventions for school-aged children. Our findings are consistent with this previous literature and even generated its usefulness and social validity among high school students.

With respect to the second research question, in general, the results indicate that students' technology self-efficacy positively impacted students' social validity when using Canvas LMS-based online modules. In particular, when they had a higher degree of technology self-efficacy related to self-regulation and monitoring their behavior during technology instruction, the odds of rating higher social validity significantly increased by 3.70 times (logit coefficient = 1.31, OR = 3.70). Previous studies highlighted the role of technology self-efficacy in the online learning environment (Al-Hattami, 2025; Yang et al., 2024). Our findings are consistent with students' favorable online learning experiences among those with higher technology self-efficacy than those with lower levels, particularly self-regulation and monitoring (Chou et al., 2024). When high school students were able to check their learning behavior and follow the expected sequence embedded in the Canvas LMS online modules, students showed more positive social validity. The interactive nature of many platforms allowed participating high school students to engage with real-world scenarios, simulating cyber threats and attacks. Furthermore, the self-paced nature of online courses provided learners with varying schedules, enabling them to balance education with other commitments.

Opinions on the Open-Ended Social Validity Questionnaire

The results regarding the third research question showed high school students' sentiments toward their experiences of using the Canvas LMS-based cybersecurity online modules. When we explored the open-ended opinions on the social validity questionnaire, many of the frequently observed responses were related to their sentiment about whether they liked and disliked cybersecurity units, topics, and activities. The word correlation network analysis validated the relationships among frequently observed words for each question related to students' preferred, least preferred, and overall experiences in the project. For example, online learning about the "metaverse" and exploring various "types of hackers" and "cyber ethic" were considered favorable topics and activities. Given that there are ongoing cybersecurity threats and concerns in the virtual space, it is necessary to proactively learn about cybersecurity ethics and behaviors (Al-Emran & Deveci, 2024). On the other hand, when the content was delivered through asynchronous instruction, video-based instruction, online discussion, and quizzes that were "long" in length content, students expressed the "least" likes and "dislikes." Although previous researchers pointed out students' improved engagement and usage of content review through game-based and video-based learning environments, the actual growth of knowledge could depend on students' learner characteristics (Chen et al., 2021). Additionally, although videos were displayed as a sequenced introduction with 5 to 10-minute breakdowns per module, a total of 30 minutes per module in 10 sessions, the level of sustained attention in the e-learning environment could vary by each individual student with varying needs and cognitive differences (Kokoç et al., 2020).

Limitations and Future Research

A few limitations were found in the current study. First, the number of high school students participating was 30 in the current study across two studies. To supplement this limited

number of samples for the CLMM analysis, we employed the Bayesian approach with weakly informative priors in the model (Winter & Bürkner, 2021). There is a continuous need to explore how practitioners can reflect on issues regarding small samples in the authentic education and school setting. Second, as the social validity results indicated, some high school students shared feedback that video, discussion, and quiz-based cybersecurity online modules on Canvas were insufficient to promote their understanding of the related issues. Students with diverse learning needs may need explicit teacher-guided instruction and demonstration with sequenced hands-on activities. In future research, researchers need to incorporate how various instructional models and designs could impact students' social validity. Lastly, because the study aimed to explore the social validity of students' Canvas LMS-based cybersecurity online Modules, we did not collect student data comparing their improvement in cybersecurity knowledge and skills over the semester. Although one of the surveys included a self-reported survey question on how they evaluated their learning experiences, other researchers can collect time-related log data or pre- and post-tests to quantify students' growth of cybersecurity knowledge.

Conclusion

Industry experts continuously develop and update courses to ensure alignment with the latest cybersecurity trends and technologies. Certification programs tied to these courses further enhance participants' credibility in the job market as employers increasingly value formalized cybersecurity education. Online courses offered through platforms like Canvas democratize access to cybersecurity education, empowering individuals globally to contribute to the cyber defense ecosystem.

In this study, we evaluated the social validity of a basic cybersecurity course designed for high school students (grades 9–12) and delivered via Canvas. A cross-classified Bayesian

cumulative link mixed effects model was utilized to analyze survey data, including Likert scale ratings on social validity. Future studies may include additional survey methods such as interviews, NASA-TLX, usability testing, and observations to gain deeper insights. As part of future work, the same approach will be applied to intermediate and advanced modules, with further student data being collected and analyzed using a range of tools and algorithms.

While this study shows mild modularity in course design, the findings indicate overall positive sentiments and social validity, demonstrating the potential effectiveness of this approach in high school cybersecurity education. Given that these sentiment-related words showed higher levels of centrality compared to other words, the patterns of word connections and the strengths of associated words corroborate their relative importance within students' open-ended responses. These results encourage students to explore more advanced cybersecurity modules, supporting deeper engagement in the subject.

Declarations

Funding

Office of Naval Research, Science, Technology, Engineering and Mathematics Program

Availability of data and materials

The data and materials used and analyzed for the manuscript are publicly available at https://cybersecurity-basic.netlify.app

Competing interests

The authors declare that they have no competing interests.

Human Ethics

The protocol was approved by West Texas A&M University, Canyon, TX, and University of North Texas, Denton, TX, Institutional Review Boards (IRBs). All experiments were

performed in accordance with relevant guidelines and regulations. This study adhered to the Declaration of Helsinki.

Consent to Participate

Participants informed consent to participate in the study has been obtained from each participant.

Consent to publish

Not Applicable

References

Al-Emran, M., & Deveci, M. (2024). Unlocking the potential of cybersecurity behavior in the metaverse: Overview, opportunities, challenges, and future research agendas. *Technology in Society, 77*, Article 102498. https://doi.org/10.1016/j.techsoc.2024.102498

Al-Hattami, H. M. (2025). Understanding how digital accounting education fosters innovation: The moderating roles of technological self-efficacy and digital literacy. *The International Journal of Management Education, 23*(2), Article 101131. https://doi.org/10.1016/j.ijme.2025.101131

Al-Turjman, F., & Salama, R. (2021). Cyber security in mobile social networks. In *Security in IoT Social Networks* (pp. 55–81). Academic press. https://doi.org/10.1016/B978-0-12-821599-9.00003-0

Aydeniz, M. (2018). Integrating Computational Thinking in School Curriculum. In M. S. Khine (Eds.) *Computational Thinking in the STEM Disciplines* (pp. 253–277). Springer. https://doi.org/10.1007/978-3-319-93566-9_13

Authors. (2023). Blinded for peer review.

Authors. (2025a). Blinded for peer review.

Authors. (2025b). https://osf.io/byrw7/?view_only=ec0b6ba61fef4134b371ff54fead3314

Bamakan, S. M. H., Nurgaliev, I., & Qu, Q. (2019). Opinion leader detection: A methodological review. *Expert Systems with Applications*, *115*, 200–222. https://doi.org/10.1016/j.eswa.2018.07.069

Benoit, K., Watanabe, K., Wang, H., Nulty, P., Obeng, A., Müller, S., & Matsuo, A. (2018). quanteda: An R package for the quantitative analysis of textual data. *Journal of Open Source Software, 3*(30), Article 774. https://doi.org/10.21105/joss.00774

Bürkner, P.-C. (2017). brms: An R package for Bayesian multilevel models using Stan. *Journal of Statistical Software, 80*(1), 1–28. https://doi.org/10.18637/jss.v080.i01

Bürkner, P. C., & Charpentier, E. (2020). Modelling monotonic effects of ordinal predictors in Bayesian regression models. *British Journal of Mathematical and Statistical Psychology*, *73*(3), 420–451. https://doi.org/10.1111/bmsp.12195

Cavanaugh, R., Quique, Y. M., Swiderski, A. M., Kallhoff, L., Terhorst, L., Wambaugh, J., Hula, W. D., & Evans, W. S. (2023). Reproducibility in small-N treatment research: A tutorial

using examples from aphasiology. *Journal of Speech, Language, and Hearing Research*, *66*(6), 1908–1927. https://doi.org/10.1044/2022_JSLHR-22-00333

Chen, W., He, Y., Tian, X., & He, W. (2021). Exploring cybersecurity education at the K-12 level. In E. Langran & D. Rutledge (Eds.), *Proceedings of SITE Interactive Conference* (pp. 108–114). Association for the Advancement of Computing in Education. https://www.learntechlib.org/primary/p/220175/

Chen, Y. C., Lu, Y. L., & Lien, C. J. (2021). Learning environments with different levels of technological engagement: a comparison of game-based, video-based, and traditional instruction on students' learning. *Interactive Learning Environments*, *29*(8), 1363–1379. https://doi.org/10.1080/10494820.2019.1628781

Chou, S. W., Hsieh, M. C., & Pan, H. C. (2024). Understanding the impact of self-regulation on perceived learning outcomes based on social cognitive theory. *Behaviour & Information Technology*, *43*(6), 1129–1148. https://doi.org/10.1080/0144929X.2023.2198048

Computer Science Teachers Association (2017). *CSTA K–12 Computer Science Standards, Revised 2017.* https://csteachers.org/k12standards

Creed, C., Al-Kalbani, M., Theil, A., Sarcar, S., & Williams, I. (2024). Inclusive augmented and virtual reality: A research agenda. *International Journal of Human–Computer Interaction*, *40*(20), 6200–6219. https://doi.org/10.1080/10447318.2023.2247614

Csardi, G., & Nepusz, T. (2006). The igraph software package for complex network research. *InterJournal, Complex Systems, 1695*, 1–9. https://igraph.org

Deylami, H. M., Mohaghegh, M., Sarrafzadeh, A., McCauley, M., Ardekani, I., & Kingston, T. (2015). Capture the talent: Secondary school education with cyber security competitions.

International Journal of Foundations of Computer Science and Technology, 5(6), 555–66. https://doi.org/10.5121/ijfcst.2015.5606

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law, 110*(3), 425–479. https://doi.org/10.1017/S0002930000016894

Huntington, R. N., Badgett, N. M., Rosenberg, N. E., Greeny, K., Bravo, A., Bristol, R. M., Byun, Y. H., & Park, M. S. (2023). Social validity in behavioral research: A selective review. *Perspectives on Behavior Science*, *46*(1), 201–215. https://doi.org/10.1007/s40614-022-00364-9

Ibrahim, A., McKee, M., Sikos, L. F., & Johnson, N. F. (2024). A systematic review of K-12 cybersecurity education around the world. *IEEE Access, 12*, 59726–59738. https://doi.org/10.1109/ACCESS.2024.3393425

Ives, L. A., Serel, M., Diaz, A. J., LeBlanc, L., & Dallery, J. (2024). Social validity of digital social incentives in the treatment of substance use disorders. *Journal of Applied Behavior Analysis.* Advance online publication. https://doi.org/10.1002/jaba.2916

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning, 12*(1), 150–158. https://doi.org/10.11591/edulearn.v12i1.7736

Lampropoulos, G., Anastasiadis, T., Siakas, K., & In, L. E. (2019, April). Digital game-based learning in education: Significance of motivating, engaging and interactive learning environments. In *24th International Conference on Software Process Improvement-Research into Education and Training (INSPIRE 2019)* (pp. 117–127).

Liu, X. (2022). *Categorical data analysis and multilevel modeling using R*. Sage.

Kokoç, M., IIgaz, H., & Altun, A. (2020). Effects of sustained attention and video lecture types on learning performances. *Educational Technology Research and Development, 68*(6), 3015–3039. https://doi.org/10.1007/s11423-020-09829-7

Magalhães, P., Pereira, B., Figueiredo, G., Aguiar, C., Silva, C., Oliveira, H., & Rosário, P. (2023). An Iterative Mixed-Method Study to Assess the Usability and Feasibility Perception of CANVAS® as a Platform to Deliver Interventions for Children. *International Journal of Human–Computer Interaction*, *40*(23), 8057–8075. https://doi.org/10.1080/10447318.2023.2277491

Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity curriculum design: A survey. In Z. Pan, A. Cheok, W. Müller, M. Zhang, A. El Rhalibi, & K. Kifayat (Eds.), *Transactions on edutainment XV* (Lecture Notes in Computer Science, Vol. 11345). Springer. https://doi.org/10.1007/978-3-662-59351-6_9

Newman, M. (2018). *Networks*. Oxford University Press.

Nohelty, K., Hahs, A. D., Rodriguez, K. A., Rue, H., Cameron, M. J., & Dixon, D. R. (2023). Assessing the social validity of telehealth-based applied behavior analysis services for autism spectrum disorder. *Behavioral Interventions, 38*(3), 590–610. https://doi.org/10.1002/bin.1938

Oudat, Q., & Othman, M. (2024). Embracing digital learning: Benefits and challenges of using Canvas in education. *Journal of Nursing Education and Practice*, *14*(10), 39–43. https://doi.org/10.5430/jnep.v14n10p39

Pan, X. (2020). Technology acceptance, technological self-efficacy, and attitude toward technology-based self-directed learning: learning motivation as a mediator. *Frontiers in Psychology*, *11*, Article 564294. https://doi.org/10.3389/fpsyg.2020.564294

Pascoe, C. , Quinn, S., & Scarfone, K. (2024). *The NIST cybersecurity framework 2.0, NIST cybersecurity white papers*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*, Article 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know*. International Society for Technology in Education.

Robinson, D., & Silge, J. (2022). *widyr: Widen, process, then re-tidy data* (R package version 0.1.5). https://CRAN.R-project.org/package=widyr

Santiana, S., Silvani, D., & Ruslan, R. (2021). Optimizing LMS CANVAS for interactive online learning perceived by the students. *Journal of English Education and Teaching*, *5*(4), 529–543.

Saville, J. D., & Foster, L. L. (2021). Does technology self-efficacy influence the effect of training presentation mode on training self-efficacy? *Computers in Human Behavior Reports, 4*, Article 100124. https://doi.org/10.1016/j.chbr.2021.100124

Shin, M. (2025). *TextAnalysisR: A text mining workflow tool* (R package version 0.0.2). https://mshin77.github.io/TextAnalysisR

Sussman, L. L. (2023). Reinventing cybersecurity internships during the COVID-19 pandemic. *Journal of Cybersecurity Education, Research and Practice, 2022*(2), Article 7. https://doi.org/10.32727/8.2023.6

Traag, V. A., Waltman, L., & van Eck, N. J. (2019). From Louvain to Leiden: Guaranteeing well-connected communities. *Scientific Reports, 9*(1), Article 5233. https://doi.org/10.1038/s41598-019-41695-z

Winter, B., & Bürkner, P. C. (2021). Poisson regression for linguists: A tutorial introduction to modelling count data with brms. *Language and Linguistics Compass*, *15*(11), Article e12439. https://doi.org/10.1111/lnc3.12439

Wolf, M. M. (1978). Social validity: the case for subjective measurement or how applied behavior analysis is finding its heart. *Journal of Applied Behavior Analysis*, *11*(2), 203–214. https://doi.org/10.1901/jaba.1978.11-203

Yang, H., Kim, J., Kelly, S., & Goke, R. (2024). The virtual classroom divide: how does the self-efficacy gap reshape online learning? *Communication Education, 73*(3), 267–281. https://doi.org/10.1080/03634523.2024.2347206

Yu, G. J., Lee, H. S., & Lee, C. K. (2024). Analysis of transaction networks among Korean IT corporations in nine metropolitan regions: Assessing connection strengths and developing a node centrality composite indicator. *Smart Media Journal*, *13*(2), 108–121. https://doi.org/10.30693/SMJ.2024.13.02.108

Table 1 Demographic profiles of participants

Characteristic	*N* = 30
Grade	
9	3 (10%)
10	9 (30%)
11	2 (6.7%)
12	15 (50%)
NR	1 (3.3%)
Gender	

Characteristic	$N = 30$
Female	9 (30%)
Male	20 (67%)
NR	1 (3.3%)
Race or ethnicity	
White or Caucasian	18 (60%)
Black or African American	5 (17%)
American Indian/Native American or Alaska Native	1 (3.3%)
Native Hawaiian or Other Pacific Islander	1 (3.3%)
Multiracial	2 (6.7%)
Other	3 (10%)
Daily time used for mobile devices	
Less than 1 hour	7 (23%)
1 to less than 3 hours	4 (13%)
3 to less than 6 hours	8 (27%)
More than 6 hours	11 (37%)
Type of mobile devices used at school for learning	
Computer	14 (47%)
Smartphone	3 (10%)
Smartphone, Computer	13 (43%)
Type of mobile devices used at home for learning	
Computer	7 (23%)
Smartphone	7 (23%)

Characteristic	$N = 30$
Smartphone, Computer	13 (43%)
Smartphone, Tablet, Computer	3 (10%)

Table 2 Cross-classified Bayesian CLMM results of social validity

Variable	Logit coefficient			Odds ratio	
	Estimate	Est.Error	95%CI	Exp(Estimate)	Exp(95%CI)
Intercept					
1|2	—	—	—	—	—
2|3	−0.62	1.49	[−3.42, 2.53]	0.54	[0.03, 12.57]
3|4	2.53	1.49	[−0.20, 5.86]	12.56	[0.81, 349.85]

4|5	6.09	1.53	[3.39, 9.46]	441.18	[29.55, 12777.27]
Technology self-efficacy					
Navigating and using	0.16	0.56	[−0.95, 1.26]	1.17	[0.39, 3.53]
Learning sequence	0.87	0.72	[−0.44, 2.45]	2.40	[0.64, 11.58]
Self-regulation	1.31	0.66	[0.06, 2.78]	3.70	[1.06, 16.09]
Random effects					
Items (τ^2_{0i})	3.38				
Students (τ^2_{0j})	2.31				

Note. CI = credible interval.

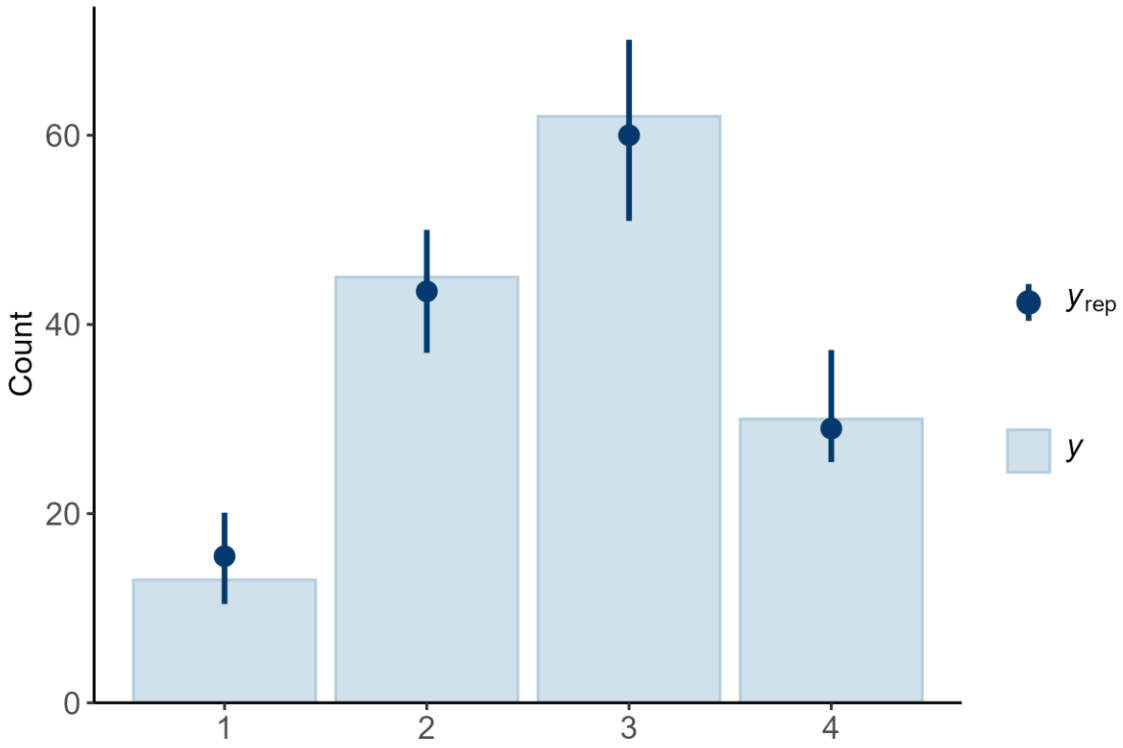


Fig. 1 Visualization of posterior predictive check

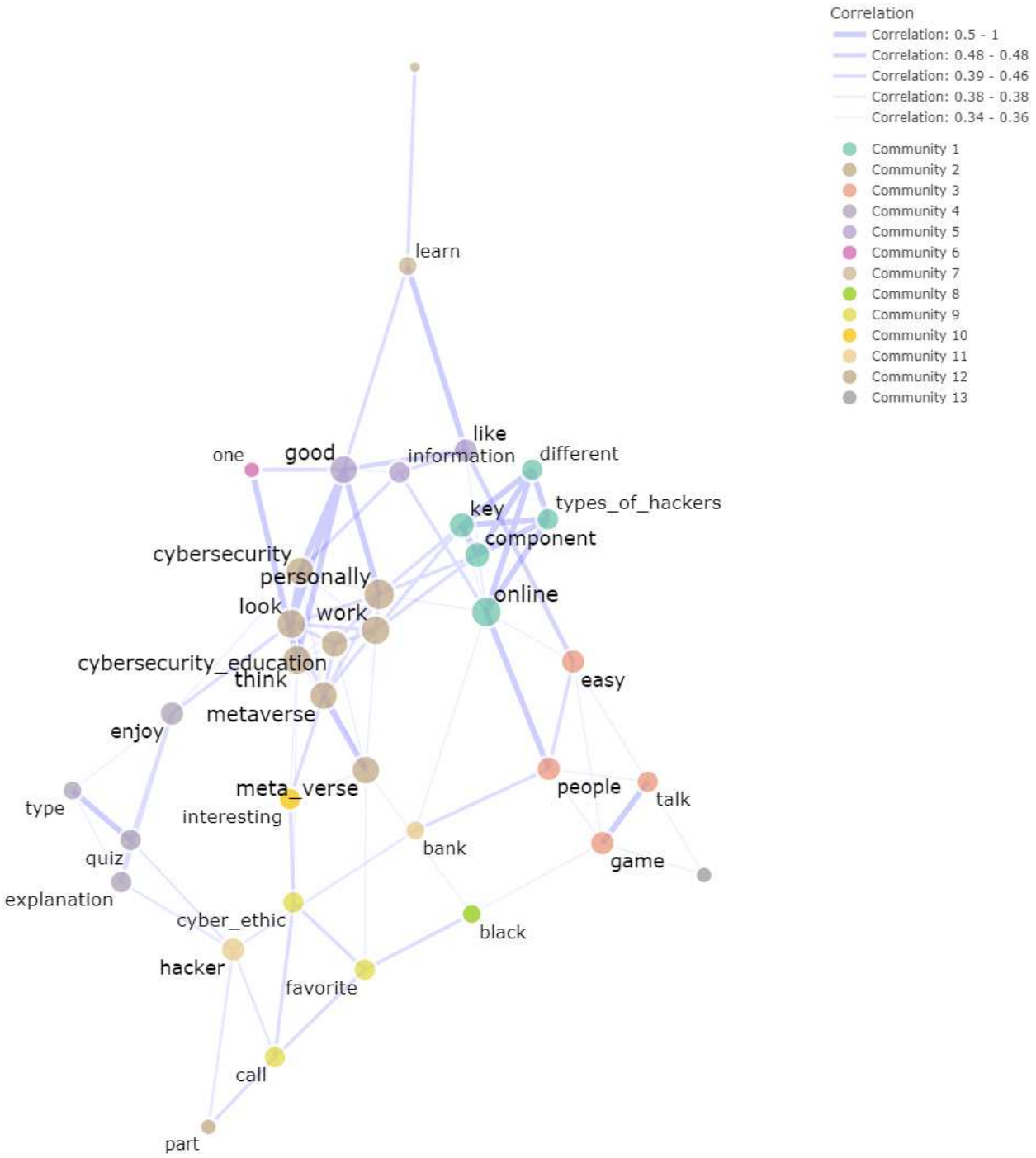


Fig. 2 Word correlation networks of the most preferred topics (co-occurrence ≥ 2, correlation ≥ 0.32)

Note. Centrality indexes for each node are available at https://cybersecurity-basic.netlify.app/most.

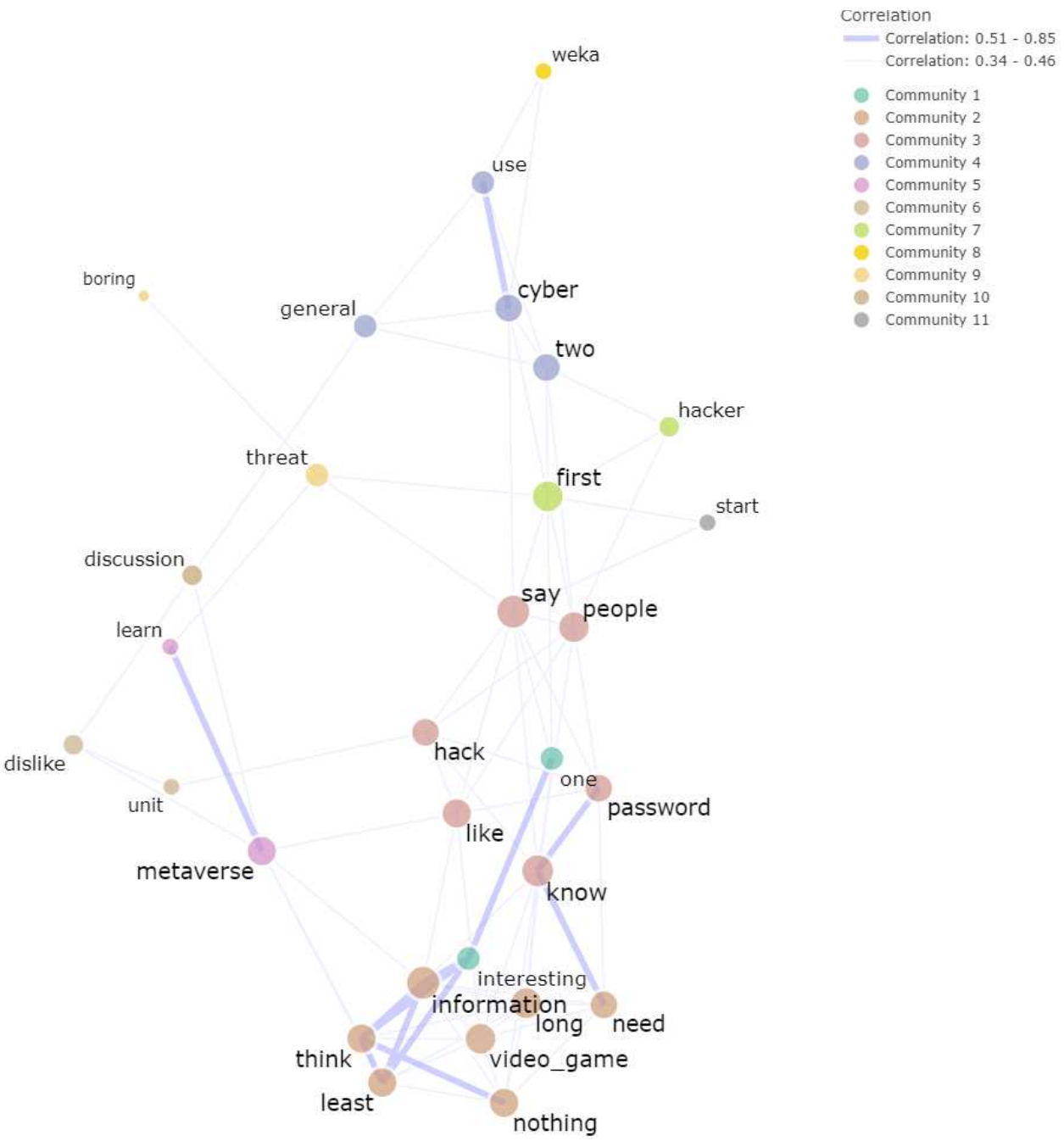


Fig. 3 Word correlation networks of the least preferred topics (co-occurrence ≥ 2, correlation ≥ 0.32)

Note. Centrality indexes for each node are available at https://cybersecurity-basic.netlify.app/least.

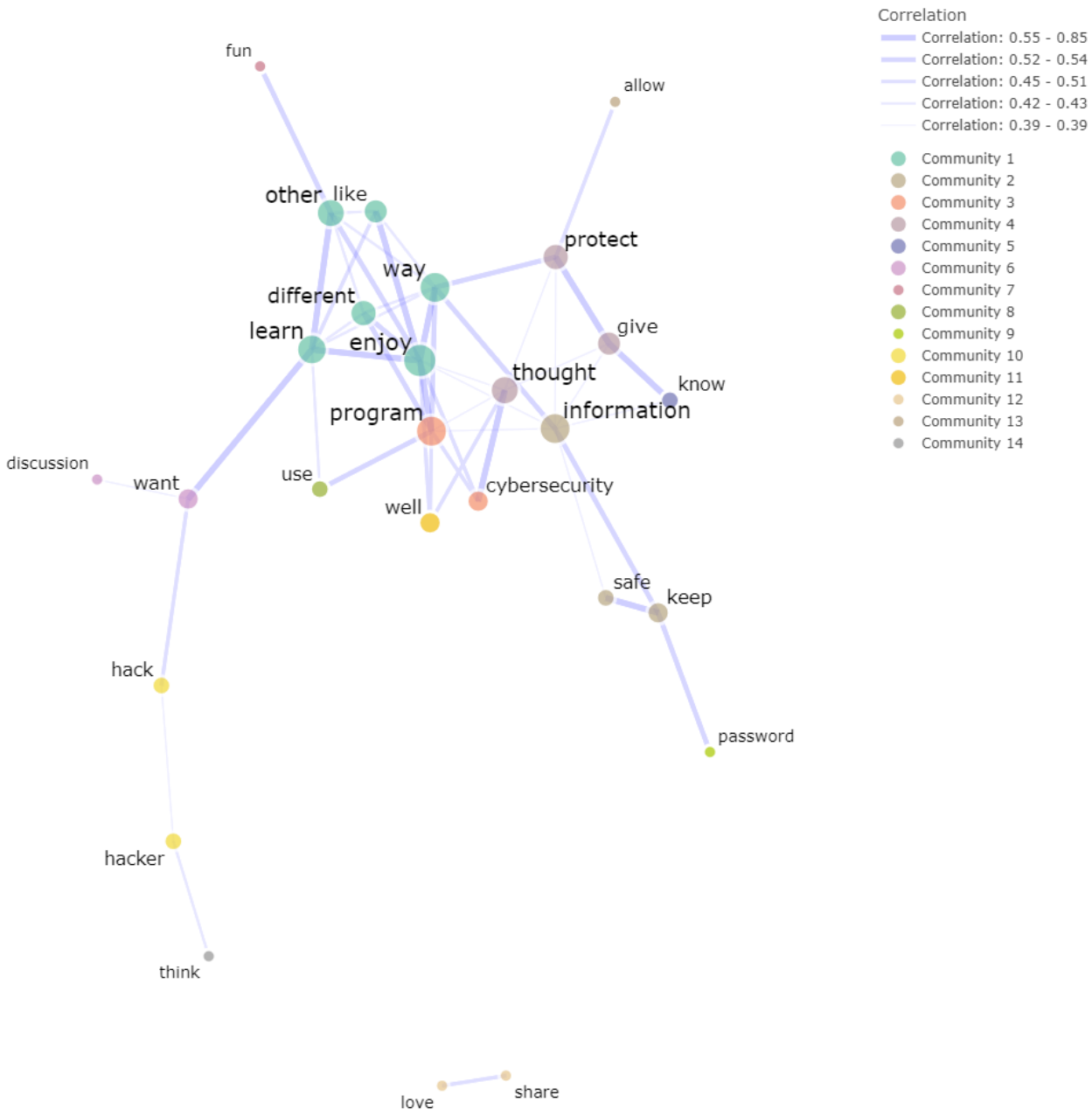


Fig. 4 Word correlation networks for overall experiences (co-occurrence ≥ 3, correlation ≥ 0.38)

Note. Centrality indexes for each node are available at https://cybersecurity-basic.netlify.app/overall.