Validation of an Instrument to Measure Self-Efficacy in Information Security

Joseph C. Tise
Institute for Advancing Computing Education
Winchester, VA, USA
joe@csedresearch.org

Monica M. McGill
Institute for Advancing Computing Education
Peoria, IL, USA
monica@csedresearch.org

Abstract

Problem. Extant measures of students' cybersecurity self-efficacy lack sufficient evidence of validity based on internal structure. Such evidence of validity is needed to enhance confidence in conclusions drawn from use of self-efficacy measures in the cybersecurity domain.

Research Question. To address this identified problem, we sought to answer our research question: *What is the underlying factor structure of a new self-efficacy for Information Security measure?*

Method. We leveraged exploratory factor analysis (EFA) to determine the number of factors underlying a new measure of student self-efficacy to conduct information security. This measure was created to align with the five elements of the information security section of the K-12 Cybersecurity Education framework. Participants were 190 undergraduate students recruited from computer science courses across the U.S.

Findings. Results from the EFA indicated that a four-factor solution best fit the data while maximizing interpretability of the factors. The internal reliability of the measure was quite strong ($\alpha = .99$).

Implications. The psychometric quality of this measure was demonstrated, and thus evidence of validity based on internal structure has been established. Future work will conduct a confirmatory factor analysis (CFA) and assess measurement invariance across subgroups of interest (e.g., over- vs. under-represented race/ethnicity groups, gender).

CCS Concepts

• **Social and professional topics** → **Computing education**; **Computing education programs**; **Computer science education**.

Keywords

cybersecurity education, self-efficacy, instrument, validation, information security

ACM Reference Format:
Joseph C. Tise and Monica M. McGill. 2024. Validation of an Instrument to Measure Self-Efficacy in Information Security. In *Proceedings of the 2024 ACM Virtual Global Computing Education Conference V. 1 (SIGCSE Virtual 2024), December 5–8, 2024, Virtual Event, NC, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3649165.3690095

SIGCSE Virtual 2024, December 5–8, 2024, Virtual Event, NC, USA

ACM ISBN 979-8-4007-0598-4/24/12
https://doi.org/10.1145/3649165.3690095

1 Introduction

In the United States, only 9% of the cybersecurity workforce is Black (compared to 13% of the population), 4% are Hispanic (compared to 19% of the population), and 24% are women (compared to 51% of the population) [4]. This gap is particularly acute given the fact that cybersecurity jobs are in high demand and industry is increasingly seeking qualified candidates to fill these roles. The most recent data from the U.S. Bureau of Labor Statistics supports this, indicating that the field will grow over 30% from 2023 through 2032 [27]. One way to broaden participation in cybersecurity is to bring more exposure of the field to high school students by leveraging both in school and out of school time programs (e.g., CyberPatriot, GenCyber, Cyber Academy) [22, 26]. To standardize K-12 cybersecurity education, the U.S. National Institute of Standards and Technology (NIST) and Cyber.org developed the *K-12 Cybersecurity Education Framework* [8]. The framework has been specifically designed to establish curriculum standards for those who want to incorporate cybersecurity into their classroom curriculum. These standards have been incorporated into Cyber.org's free curriculum materials that they provide to teachers who attend their professional development.

Given the need for more cybersecurity professionals, ways to measure how interested students might be in pursuing post-high school opportunities can be used to help identify practices and pedagogies that might impact students either positively or negatively. Self-efficacy is a key factor related to interest, persistence, and academic achievement across a wide variety of subjects [7, 13, 24]. Students with low self-efficacy for cybersecurity will not pursue education or careers in cybersecurity. However, there are relatively few instruments that measure high school self-efficacy in cybersecurity, and none to date have been specifically designed to map to the *K-12 Cybersecurity Education Framework*. This is a problem because we must be able to measure students' self-efficacy for cybersecurity if we wish to enhance it through intervention.

In light of the critical need for more cybersecurity professionals (particularly those from historically underrepresented groups in the field), the relationship between self-efficacy and persistence within domains, and the preliminary work already completed in the cybersecurity education space, we embarked on this project with one overarching purpose: to develop a psychometrically sound measure of students' self-efficacy for information security. Accordingly, we posed the following research question:

> *What is the underlying factor structure of a new self-efficacy for Information Security measure?*

Given the *K-12 Cybersecurity Education Framework* is comprehensive, we scoped this instrument to focus specifically on Information Security. As a first step in our measure-development process, we tested the instrument with undergraduate students to gather preliminary evidence of validity, and a future study will further test the instrument with high school students. We detail the results of this analysis in the remainder of this paper.

2 Background

2.1 Self-Efficacy in Education

Self-efficacy is defined as one's belief in their ability to complete a certain action [5]. People typically do not pursue activities for which they have little confidence in their abilities to succeed. For this reason, enhancing students' self-efficacy for a particular domain is critical to ensure their persistence in that domain. However, researchers and practitioners cannot enhance self-efficacy without first being able to measure it effectively. Fortunately, numerous self-efficacy measures exist, contextualized to a number of domains, topics, and activities [1, 6, 25]. Over the past 40 years, prior research has used these measures to link students' self-efficacy to numerous academic outcomes of interest, including persistence [14], interest [24], learning strategy use [15], and academic achievement [7]. Given the abundance of evidence in education research, self-efficacy has been shown to be a critical predictor of future performance and behavior within any discipline.

2.2 Self-Efficacy for Cybersecurity

Several studies have investigated self-efficacy within a cybersecurity context, and some reported positive outcomes for students' self-efficacy after participating in cybersecurity courses or extracurricular activities [9–11, 17, 19, 21]. For example, Konak examined different types of self-efficacy and found that after participating in a one-week information security program aimed at K12 students, not only did students show significant improvements in overall self-efficacy, but students also showed improvements in problem-solving self-efficacy, online safe behavior self-efficacy, and networking self-efficacy. Notably, female student' networking self-efficacy improved more than male students by almost 30 percentage points [20].

Despite the fruitful contributions of these prior studies, most of the extant K-12 cybersecurity education literature uses researcher-created measures of self-efficacy with little or no evidence of validity or reliability shown with the exception of Amo et al. [3] and its adapted measure by McGill [22]. The cybersecurity field still lacks a validated instrument to measure self-efficacy in a way that aligns with the Framework.

2.3 Exploratory Factor Analysis

One of the most common methods used to produce evidence of validity for a new measure [2] is exploratory factor analysis (EFA). EFA is a type of analysis rooted in structural equation modeling (SEM) that enables the researcher to determine how items in a measure relate to each other to form the underlying structure (i.e., factors) of the measure. For example, a measure designed to assess three distinct (but related) facets of a construct ought to result in a three-factor structure–one factor for each facet. Such alignment between the underlying structure of the measure and the theory or framework upon which the measure was built is considered key evidence of validity [2], and enhances the confidence researchers can have in conclusions drawn from use of the measure.

Table 1: Cyber.org K-12 Cybersecurity Education Framework. (Note: CIA refers to Confidentiality, Integrity, and Availability of information within a system or organization.)

Information Security	CIA Triad Access Control Data Security Threats & Vulnerabilities Cryptography
Network Security	Authentication Securing Network Components Threats & Vulnerabilities
Physical Security	Threats & Vulnerabilities Security Controls

3 Method

3.1 Instrument Development

Thirty seven items were developed based on the five *Information Security* components of the Cyber.org K-12 Cybersecurity Education framework [8] (see Table 1). We referenced Bandura's 2006 guide for creating self-efficacy scales to help us finalize the question stem, item wording, and use of a 7-point Likert scale. We settled on a 37 item scale to start, with the understanding that we would retain only 3 or 4 of the best items for each component of the *Information Security* framework (to ensure the final measure is not too long).

We conducted four rounds of item development and in each round, refined the items based on feedback from experts in the information security field to enhance evidence of validity based on test content [2]. In the first round, we leveraged ChatGPT 3.5 to create sets of items as a starting point, using the exact phrasing from the framework within prompts. We then reviewed, rephrased, and reduced the items to a core set. We then shared the items with four experts who teach and evaluate K-12 cybersecurity education in the U.S. and are familiar with the Framework. Each round provided additional refinement of the items until the changes were all addressed. Each reviewer received a $75 gift card for sharing their expertise.

We first piloted the measure with university students in cybersecurity courses and programs to ensure that the items would produce sufficient variance to conduct an exploratory factor analysis (i.e., we wanted to avoid a potential floor effect). Ethical review board approval was obtained prior to initiating the study. Once the underlying structure of the measure has been established, we plan to gather further evidence of validity with high school students (see *Adjustments and Future Work* section). Ultimately, we envision this measure could be used in both high school and college populations.

Table 2: Participants' Year of Enrollment and Age.

Year	N	%
First-year	63	33.16
Second-year	35	18.42
Third-year	43	22.63
Fourth-year	37	19.47
Fifth-year +	12	6.32

Age	N	%
18 - 19	77	40.53
20 - 21	62	32.63
22 - 23	22	11.58
24+	29	15.26

Table 3: Participants' Race/Ethnicity.

Race/Ethnicity	N	%
African-American or Black	26	13.68
Asian	47	24.74
Hawaiian or Pacific Islander	1	0.53
Hispanic/Latine	15	7.89
Middle Eastern	4	2.11
Native American or Native Alaskan	1	0.53
White	66	34.74
Multiracial	14	7.37
Declined to Answer	16	8.42

3.2 Participants

Participants were recruited via email from computer science (CS) courses across multiple universities in the United States. The research team sent course instructors an invitation email with the survey link included, and the instructors distributed the email and survey link to their students on behalf of the research team. This included targeted recruitment from students in cybersecurity courses and programs.

The sample ($n = 190$) was diverse regarding year of enrollment and age of participants (see Table 2). Further, most of the sample (72.11%) indicated they had never taken a cybersecurity course, while 16.84%, 5.26%, and 5.79% had taken one, two, and three or more cybersecurity courses, respectively. Most of the sample (71.58%) indicated English was their native language. Regarding gender, the sample was mostly Men (56.84%), but Women (27.37%) and those who identified as agender (0.53%), non-binary (0.53%), multiple genders (2.63%), and those who declined to answer (12.10%) were also represented. Finally, the sample was relatively diverse regarding race and ethnicity (see Table 3).

After consenting, participants completed the survey online which included demographic items and the 37-item self-efficacy measure. Participants could enter their emails at the end to enter a raffle to win one of fifty $25 gift cards. The self-efficacy items took approximately five minutes to complete, on average ($mean = 4.77, SD = 5.88$).

3.3 Data Analysis

Participants were asked to rate their confidence in their abilities to do each stated action from 1 (Cannot do at all) to 7 (Highly certain can do). The internal reliability of the measure was strong ($\alpha = .99$).

Preliminary analyses were conducted in Stata version 18 to ascertain if the data were adequate to conduct exploratory factor analysis (EFA). First, missing data mechanisms were examined, and we found that data were largely not missing (i.e., only 6.73% were missing), and data that were missing were MCAR (missing completely at random). We then conducted Bartlett's test of sphericity to determine if items were sufficiently intercorrelated to warrant factor analysis. This test indicated that they were ($\chi^2_{(666)} = 32320.654$, $p < .001$). We then conducted the Kaiser-Meyer-Olkin Measure of Sampling Adequacy test to determine if we had enough data coverage given the number of items in our measure—this test indicated that we did ($KMO = .976$).

Given the adequate results from our preliminary analyses, the data were then submitted to an exploratory factor analysis (EFA) to uncover the underlying structure of the measure. Since the items were presented on a Likert scale (and are thus ordinal), we used the weighted least square mean and variance adjusted (WLSMV) estimator with a geomin rotation to extract the factors.

Table 4: Model Fit Statistics for Factor Solutions Compared.

	RMSEA	CFI	SRMR	χ^2	% Variance Explained
3 Factors	0.088	0.981	0.054	1373.607*	74.05
4 Factors	0.074	0.987	0.036	1067.503*	78.44
5 Factors	0.058	0.993	0.029	806.719*	81.24

*p < .05

3.4 Researcher Positionality Statements

The first author is trained as an educational psychologist with expertise in quantitative and mixed methodology, theories of student learning and motivation, and self-regulated learning. He approaches CS education research from a learning sciences perspective and a post-positivist epistemological stance [23]. The second author began her career in cybersecurity, has extensive experience teaching CS at the post-secondary levels, and has extensive experience conducting CS education research. She approaches education research with an eye on CS education for all students, centering on equitable outcomes across various subgroups. She brings this perspective into this project by ensuring that decisions throughout the research process reflect the needs of various students, particularly those from underrepresented groups in the field of CS.

4 Results

Upon model convergence in the EFA analysis, we examined fit statistics for each of five alternative models (1-factor model to a 5-factor model). Global fit statistics were largely acceptable on all models (i.e., $RMSEA \leq .06, CFI \geq .95, SRMR \leq .08$)[18], but were best on the 3-, 4-, and 5-factor models (see Table 4). Since the measure was constructed based on the K-12 Cybersecurity Standards established by Cyber.org, we anticipated a 5-factor structure and thus did not consider the 1- or 2-factor solutions any further.

4.1 Identifying the Best Factor Solution

The χ^2 values for all models were statistically significant (which is not desirable in evaluating model fit), but obtaining significant χ^2 values is common in SEM because χ^2 is known to be quite sensitive

to factors like sample size, correlations and shared variance among variables, and multivariate non-normality[**?**]. Further, the the χ^2 test of model fit tests whether the model fits the data *perfectly*. Thus, even slight departures from exact model fit can yield a significant χ^2 value when tested against this very high standard. As described in Chapter 12 of Kline's (2015) textbook, "The binary decision of whether to reject or not reject the exact-fit null hypothesis does not by itself determine whether to reject the model or to retain it" (p. 265). Indeed, the other global fit indices (RMSEA, CFI, and SRMR) indicated overall good fit on the three solutions.

To further examine the three solutions in light of the significant χ^2 values, we compared the loadings and residual variances of each item and the eigenvalues of and total variance explained by each factor among the three solutions, in line with recommendations from the psychometric literature [12, 16]. Solutions that included cross-loaded items (i.e., items that loaded onto more than one factor) were deemed less ideal than solutions with no or fewer cross loadings. Similarly, solutions that produced items with higher communalities (i.e., lower residual variances) were more favorable than solutions with items with lower communalities. Finally, once a factor solution was determined, we trimmed one item (Item #18) from the measure that was cross loaded (i.e., items that loaded significantly onto two or more factors) to enhance interpretation.

After considering several criteria in a comprehensive fashion (see *Data Analysis* section), we settled on a four factor solution (see Tables 5 and 6). We found the four factor solution provided the best balance among total variance explained, distinct factors, overall model fit, and interpretability. It is important to note that settling on a factor structure via EFA is not a clear-cut process. Although researchers partly rely on statistics to help choose a factor structure, raw statistics are not the only criteria referenced–less objective criteria (e.g., interpretability, balancing variance explained against factor structure complexity) are equally important to consider [12]. Therefore, even though the five-factor solution exhibited better global fit indices and explained slightly more variance in the items, we retained only the four-factor solution because it had fewer cross-loaded items and made the factors more interpretable (i.e., items included in each factor were more clearly thematic).

Finally, no items actually loaded significantly onto the fifth factor of the five-factor solution, so the meaning of a fifth factor was further reduced. It is also important to note that in EFA, a solution with *n* number of factors will always explain more variance than a solution with *n-1* factors [12]. Further, a measure could technically has as many factors as it does items, and if all possible factors were retained, the model would explain 100% of the variance in the items. Of course retaining all possible factors would negate the purpose of factor analysis (a data reduction technique), thus we decided the slightly higher variance explained by including a fifth factor was not worth the reduction in interpretability.

4.2 The Final Four-factor Solution

After examining the items associated with each factor, we labeled the four factors as *CIA Triad, Access Control, Malware and Hacking,* and *Cryptography*, respectively. *CIA Triad* items tap students' self-efficacy as it relates to Confidentiality, Integrity, and Availability of information within a system or organization. *Access Control* items assess students' self-efficacy related to explaining and distinguishing three aspects of access control: identification, authentication, and authorization. *Malware and Hacking* items assess students' self-efficacy related to identifying, explaining, and remediating acts and tools for gaining unauthorized access to a system. Finally, *Cryptography* items assess students' self-efficacy related to developing, using, and explaining coded algorithms used to protect sensitive information.

5 Discussion

These results indicate that the items included in this measure of students' cybersecurity self-efficacy are not completely aligned with the K-12 Cybersecurity Education framework structure. It appears that items designed to assess self-efficacy for Data Security and self-efficacy for Threats & Vulnerabilities (two parts of the framework) were not distinguishable to the participants. Instead, these items loaded onto a single factor, which we ultimately named *Malware and Hacking*.

The discrepancy between the factor solution identified and the K-12 Cybersecurity Education framework does not necessarily imply that the elements of the framework are not distinct; these results simply show that students largely did not answer the questions in a way that illuminated any potential distinctions. Thus, researchers and policymakers can consider two paths forward in light of these results: 1) Reconsider the elements of the K-12 Cybersecurity Education framework with an eye toward conceptual distinction between Data Security and Threats & Vulnerabilities, or 2) Attempt to develop new self-efficacy items for these two elements of the framework that are more clearly aligned with it and are simultaneously distinct from the other existing items.

Despite the slight misalignment between the final factor structure and the framework upon which the items were written, this measure of information security self-efficacy shows promise for use in research and practice. To our knowledge, this is the first self-efficacy instrument created specifically for an information security context. Others who wish to promote cybersecurity education through intervention can use this measure to assess the impact their intervention has on students' motivation.

5.1 Limitations

As with any research, this study had some limitations that need to be mentioned. First, the data for this study was collected from college students studying computer science. Therefore, this sample may not represent other populations of interest. That is, this measure was created based on the K-12 Cybersecurity Education framework and is intended eventually to be used with high school students. Our next phase of development for this measure is to confirm the factor structure with high school students, but until that follow-up study is completed, this measure may only be appropriate for college students. Second, the measure at present is quite long. At 36 items, this measure is likely too long to be used with many other measures in a single survey administration. Thus, our future research will also confirm the factor structure of a shortened version of the measure.

Third, due to our sample size, we were unable to conduct any measurement invariance analyses across subgroups (e.g.,

Table 5: Item Loadings for the 4 Factor Solution (Items 1-29)

#	Question	CIA Triad	Access Control	Malware & Hacking	Crypto-graphy
1	I can define the confidentiality component of the CIA triad.	**0.888***	0.116*	0	-0.046
2	I can define the integrity component of the CIA triad.	**0.927***	0.114	-0.018	-0.05
3	I can define the availability component of the CIA triad.	**0.886***	0.051	0.005	0.043
4	I can explain how the confidentiality component of the CIA triad can be used to protect data at rest.	**0.802***	-0.111	0.253*	0.038
5	I can explain how the availability component of the CIA triad can be used to protect data in use.	**0.873***	0.021	0.06	0.048
6	I can explain how the integrity component of the CIA triad can be used to protect data in motion.	**0.881***	-0.003	0.089	0.023
7	I can explain identification in access control.	0.117	**0.719***	0.111	-0.01
8	I can explain authentication in access control.	0.191*	**0.683***	-0.021	0.094
9	I can explain authorization in access control.	0.253*	**0.673***	-0.025	0.043
10	I can provide examples of authentication methods.	0.043	**0.522***	0.072	-0.002
11	I can explain the difference between single factor and multi-factor authentication.	-0.048	**0.429***	0.138	-0.007
12	I can distinguish between **authentication** and **authorization** in information security.	0.07	**0.775***	0.06	-0.025
13	I can distinguish between **identification** and **authorization** in information security.	0.008	**0.968***	0.021	-0.046
14	I can distinguish between **authentication** and **identification** in information security.	0.021	**0.927***	0.022	-0.026
15	I can apply at least one security measure to protect data at rest.	0.025	**0.440***	0.311*	0.129
16	I can develop a plan to apply two or more security measures to protect data at rest.	-0.038	**0.429***	0.357*	0.189
17	I can identify weaknesses in a security measure designed to protect data in transit.	0.03	0.287*	**0.498***	0.119
19	I can name at least one security measure used for data in all three states.	0.112	0.025	**0.706***	0.088
20	I can explain to a friend about how security measures protect data in all three states.	0.208*	0.172*	**0.555***	0.048
21	I can evaluate the success of existing security measures.	0.064	0.021	**0.719***	0.038
22	I can identify different types of malware that can affect information security.	0.106	-0.069	**0.803***	0.024
23	I can explain how malware can infiltrate a system.	-0.017	0.097	**0.764***	-0.008
24	I can identify different types of malicious users.	0.018	-0.017	**0.902***	-0.082
25	I can describe how hacking attacks can compromise information security.	0.029	0.039	**0.861***	-0.117
26	In an example scenario, I could point out at least two different techniques used by hackers to access a system.	0.011	0.009	**0.907***	-0.055
27	I can identify at least two different types of vulnerabilities in a system.	-0.006	-0.083	**0.954***	0.041
28	I can apply my knowledge of attacks to make informed decisions about information security.	0.004	0.172*	**0.738***	0.03
29	I could teach a friend the difference between vulnerabilities and threats.	0.04	0.058	**0.859***	-0.143

Note: Item #18 was cross loaded and removed from the final results.

race/ethnicity, gender, disability status). Such analyses are critical to ensure equitable and valid assessment for all students. Finally, elucidating the internal structure of the measure via factor analysis is just one of several ways to demonstrate evidence of validity for a measure [2]. This study was not able to demonstrate other forms of validity evidence (e.g., relations to other variables), due to logistical restrictions. Future research ought to explore other forms of validity evidence to further vet the quality of this self-efficacy measure.

5.2 Adjustments and Future Work

In a forthcoming study, we plan to pare the measure down from 36 items to 15-20 items so as to not overburden participants. Table 7 shows the preliminary set of items we plan to include in the shorter version. In the coming months, we plan to collect data from a representative sample of U.S. high school students. This new data will enable us to confirm the factor structure and conduct measurement invariance analyses to ensure the measure performs equitably across subgroups of high school students.

Table 6: Item Loadings for the 4 Factor Solution (Items 30-37)

#	Question	CIA Triad	Access Control	Malware & Hacking	Crypto-graphy
30	I can list **at least one way** artificial intelligence can make encryption stronger.	-0.127	0.1	**0.632***	0.068
31	I can explain what a cipher is.	0.092	-0.001	-0.038	**0.760***
32	I could pass a quiz about how key generation in cryptography works.	0.051	-0.084	0.359*	**0.657***
33	I can explain how key distribution in cryptography works.	0.027	0.053	0.233	**0.720***
34	I can distinguish between public keys and private keys.	0.043	0.013	0.178	**0.674***
35	I can fully understand a textbook chapter (in my native language) about how data encoded using hexadecimal (base-16) can benefit encryption.	0.029	0.152	-0.022	**0.555***
36	I can explain the steps needed in an algorithm for encrypting data.	-0.043	0.018	0.217	**0.742***
37	I can summarize how encryption algorithms protect data.	-0.025	0.250*	-0.01	**0.763***

Table 7: Shortened version to be tested with high school students.

Category	Item
CIA Triad	I can explain how the confidentiality component of the CIA triad can be used to protect data at rest. I can explain how the availability component of the CIA triad can be used to protect data in use. I can explain how the integrity component of the CIA triad can be used to protect data in motion.
Access Control	I can distinguish between authentication and authorization in information security. I can distinguish between identification and authorization in information security. I can distinguish between authentication and identification in information security.
Malware & Hacking	I can identify different types of malware that can affect information security. I can identify different types of malicious users. I can describe how hacking attacks can compromise information security. I could teach a friend the difference between vulnerabilities and threats.
Cryptography	I can explain what a cipher is. I can explain how key distribution in cryptography works. I can explain the steps needed in an algorithm for encrypting data. I can summarize how encryption algorithms protect data.

6 Conclusion

This measure shows promising psychometric properties regarding the underlying factor structure and high reliability of the data produced. Researchers and practitioners could use this measure in its current state and feel reasonably confident that it effectively assesses students' self-efficacy for information security.

Future research could further test this measure to understand how it relates to other outcomes of interest that are theoretically related (e.g., academic performance, intentions to pursue cybersecurity). Policy makers ought to consider potential conceptual similarities among the elements of the K-12 Cybersecurity Education framework, while researchers can consider how new items could potentially better distinguish the Data Security and Threats & Vulnerabilities elements of the standards.

Finally, the framework addresses K-12 cybersecurity education, while our research only examined one area (information security) for one student population (undergraduate students). This leaves ample opportunity for additional instrumentation to be created for usage across various grade levels and various cybersecurity topics.

Acknowledgments

This material is based upon work supported by the U.S. National Science Foundation under Grant No. 2028426.

References

[1] Hyun Seon Ahn and Mimi Bong. 2019. Self-efficacy in learning: Past, present, and future. In *The Cambridge Handbook of Motivation and Learning*, K. A. Renninger and S. E. Hidi (Eds.). Cambridge University Press, Cambridge, England, 63–86.

[2] American Educational Research Association, American Psychological Association, and National Council on Measurement in Education. 2014. *Standards for Educational and Psychological Testing.* American Educational Research Association, Washington, D.C.

[3] L.C. Amo, M. Zhuo, S. Wilde, D. Murray, K. Cleary, C. Amo, S. Upadhyaya, and H.R. Roa. 2015. Cybersecurity Engagement and Self-Efficacy Scale. https://sites.google.com/site/amoceses/home

[4] Aspen Digital. 2021. Diversity, Equity, and Inclusion in Cybersecurity. https://www.aspeninstitute.org/wp-content/uploads/2021/09/Diversity-Equity-and-Inclusion-in-Cybersecurity_9.921.pdf

[5] Albert Bandura. 1977. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review* 84, 2 (1977), 191–215. https://doi.org/10.1111/1467-9280.00090 arXiv: 0003-066X/82/3702-0122 ISBN: 0033-295X (Print)\r0033-295X (Linking).

[6] Albert Bandura. 2006. Guide for constructing self-efficacy scales. In *Self-efficacy Beliefs of Adolescents*, Frank Pajares and Tim Urdan (Eds.). Information Age, Greenwich, 307–337. Issue: 1 ISSN: 1886-8576.

[7] Tiffany Cambridge-Williams, Adam Winsler, Anastasia Kitsantas, and Elizabeth Bernard. 2013. University 100 orientation courses and living-learning communities boost academic retention and graduation via enhanced self-efficacy and self-regulated learning. *Journal of College Student Retention: Research, Theory and Practice* 15, 2 (Jan. 2013), 243–268. https://doi.org/10.2190/CS.15.2.f

[8] Cyber Innovation Center & CYBER.ORG. 2021. K-12 Cybersecurity Learning Standards. (2021). https://cyber.org/sites/default/files/2021-10/K-12%20Cybersecurity%20Learning%20Standards_1.0.pdf

[9] Melissa Danforth and Charles Lam. 2017. Effects of a four-week cyber security summer program on the attitudes and college interests of high school students. In *Journal of The Colloquium for Information Systems Security Education*, Vol. 4. 19–19.

[10] Michael H Dunn. 2018. Assessing and Expanding Extracurricular Cybersecurity Youth Activities' Impact on Career Interest. (2018).

[11] Wu-chang Feng, Robert Liebman, Lois Delcambre, Michael Lupro, Tim Sheard, Scott Britell, and Gerald Recktenwald. 2017. {CyberPDX}: A Camp for Broadening Participation in Cybersecurity. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*.

[12] W. Holmes Finch. 2019. *Exploratory factor analysis.* Vol. 182. Sage Publications.

[13] Steve Graham, Karen R. Harris, and Linda Mason. 2005. Improving the writing performance, knowledge, and self-efficacy of struggling young writers: The effects of self-regulated strategy development. *Contemporary Educational Psychology* 30, 2 (April 2005), 207–241. https://doi.org/10.1016/J.CEDPSYCH.2004.08.001

[14] Sandra Graham and Bernard Weiner. 2012. Motivation: Past, present, and future. (2012).

[15] John T. Guthrie, Allan Wigfield, Pedro Barbosa, Kathleen C. Perencevich, Ana Taboada, Marcia H. Davis, Nicole T. Scafiddi, and Stephen Tonks. 2004. Increasing reading comprehension and engagement through concept-oriented reading instruction. *Journal of Educational Psychology* 96, 3 (2004), 403–423. https://doi.org/10.1037/0022-0663.96.3.403

[16] Joseph F Hair. 2009. Multivariate data analysis. (2009).

[17] William Earl Hilliker Jr. 2020. *Investigation of emotional intelligence and computer self-efficacy on the cybersecurity interest.* Ph. D. Dissertation. Eastern Michigan University.

[18] Li-tze Hu and Peter M. Bentler. 1999. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal* 6, 1 (Jan. 1999), 1–55. https://doi.org/10.1080/10705519909540118 Publisher: Routledge.

[19] Monique M Jethwani, Nasir Memon, Won Seo, and Ariel Richer. 2017. "I Can Actually Be a Super Sleuth" Promising Practices for Engaging Adolescent Girls in Cybersecurity Education. *Journal of Educational Computing Research* 55, 1 (2017), 3–25.

[20] Abdullah Konak. 2018. Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice* 2018, 1 (2018), 6.

[21] Ákos Lédeczi, MiklÓs MarÔti, Hamid Zare, Bernard Yett, Nicole Hutchins, Brian Broll, Péter Völgyesi, Michael B Smith, Timothy Darrah, Mary Metelko, et al. 2019. Teaching cybersecurity with networked robots. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. 885–891.

[22] Monica M. McGill. 2021. Cybersecurity Engagement and Self-Efficacy Scale, Version 2.0. Adapted from the Cybersecurity Engagement and Self-Efficacy Scale (2015) by Amo, L.C. and Zhuo, M. and Wilde, S. and Murray, D. and Cleary, K. and Amo, C. and Upadhyaya, S. and Roa, H.R..

[23] D. C. Phillips and N. Burbules. 2000. *Postpositivism and educational research.* Rowman and Littlefield, Lanham, MD.

[24] K. Ann Renninger and Suzanne E. Hidi. 2019. Interest development and learning. In *The Cambridge Handbook of Motivation and Learning*, K. Ann Renninger and Suzanne E. Hidi (Eds.). Cambridge University Press, Cambridge, 265–290. https://doi.org/10.1017/9781316823279

[25] Duane F. Shell, Carolyn C. Murphy, and Roger H. Bruning. 1989. Self-efficacy and outcome expectancy mechanisms in reading and writing achievement. *Journal of Educational Psychology* 81, 1 (March 1989), 91–100. https://doi.org/10.1037/0022-0663.81.1.91 Publisher: American Psychological Association, American Psychological Association Warwick & York.

[26] United States Air Force. 2020. Air Force Association's CyberPatriot: The National Youth Cyber Education Program. https://www.uscyberpatriot.org/

[27] U.S. Bureau of Labor Statistics. 2024. Occupational Outlook Handbook: Information Security Analysts. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm