

THE EFFECTS OF CYBERSECURITY AWARENESS, ATTITUDE, AND BEHAVIOR ON INFORMATION PROTECTION EFFECTIVENESS AMONG SECONDARY VOCATIONAL SCHOOL STUDENTS IN CHINA

Weng Zhen^{1*} and Songpon Nakharacruangsak²

Master of Science Program in Information Technology, Faculty of Digital Technology and Innovation,
Southeast Bangkok University^{1,2}

Author email: wengzhen34@gmail.com^{1*}, Songpon@southeast.ac.th²

Received: April	2, 2026
Revised: May	27, 2026
Accepted: June	12, 2026

Abstract

The purposes of the research were: 1) to assess the current levels of cybersecurity awareness, cybersecurity attitude, cybersecurity behavior, and information protection effectiveness among students at a secondary vocational school in eastern China; 2) To analyze the direct effects of cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior on information protection effectiveness; and 3) To investigate the joint influence of cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior on information protection effectiveness when included in the same model, and to identify the key predictors. This study adopted a quantitative cross-sectional design, and 352 valid samples were collected through simple random sampling using a 5-point Likert scale questionnaire. Data were analyzed using reliability and validity tests, Pearson correlation analysis, simple linear regression, and hierarchical multiple regression via SPSS 26.0. The findings showed that cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior all had significant positive effects on information protection effectiveness, with cybersecurity behavior having the strongest explanatory power. The three variables jointly explained 36.7% of the variance in information protection effectiveness, and an awareness–attitude–behavior gap was identified among the students. The study concludes that strengthening behavioral training, integrating cybersecurity education into curricula and institutional support, and promoting school-family-enterprise collaboration can effectively improve students' information protection effectiveness.

Keywords: Cybersecurity Awareness, Cybersecurity Attitude, Cybersecurity Behavior, Information Protection Effectiveness, Secondary Vocational School Students

Introduction

In recent years, internet use among minors in China has become almost universal. According to the latest report released by CNNIC, there were approximately 193 million underage internet users in China in 2022, and the internet penetration rate in this group reached 97.2% [1]. A considerable proportion of these minors experienced cybersecurity incidents such as account hijacking and malware infection in the preceding six months. This coexistence of digital dividends and security risks means that cybersecurity literacy and protection capabilities in cyberspace have become emerging priorities for both schooling and social governance.

At the same time, earlier exposure to the internet and "platformized" patterns of use have one hand, basic security skills and privacy-protective habits have not improved in tandem with usage frequency. For example, only about half of underage internet users are able to perform basic tasks such as registering/deleting accounts or changing passwords [1]. On the other hand, the social acceptance and practical effectiveness of single technical tools—such as parental controls or "youth modes"—remain limited; systematic coordination among platform governance, school-based education and family support is still needed [2]. International studies likewise indicate that the "human factor" has long been the weakest link in information security, and that enhancing awareness and training can significantly reduce high-risk behaviors such as using weak passwords or casually clicking suspicious links [3], [4]. Taken together, the structural tension of "high penetration–high exposure–lags in literacy and behavior" forms the practical backdrop for this study.

Against this background, students in secondary vocational schools exhibit several distinctive stage-specific characteristics. First, they are in a key transition from "learner" to "quasi-professional": while completing their studies, they also need to interact with enterprise-level information systems and campus business systems. Second, they frequently engage in practical training and skills competitions, which gives rise to diverse internet-use scenarios and complex account and data management. Building on these features, the present study focuses on students at a secondary vocational school in eastern China and examines the effects of cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior on information protection effectiveness.

The core research question of this study is: What are the effects of cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior on information protection effectiveness among secondary vocational school students? This question matters because, although the age and social experience of secondary vocational students are similar to those of upper-secondary school students, they are required to access school and enterprise information systems with relatively high privileges and at high frequency for skills training and internships. Improper cybersecurity practices may directly threaten individuals, schools, and partner enterprises [1]. At present, school-based cybersecurity education still relies mainly on lectures and campaign-style activities, and there is a lack of data-driven, locally grounded

research specifically targeting secondary vocational students. As a result, there is insufficient empirical evidence to inform curriculum design and management decisions by schools and education authorities. This study is expected to make contributions at three levels. At the school level, it will provide empirical evidence for designing targeted cybersecurity training at the secondary vocational school, thereby enhancing the security of the campus network and training platforms. At the vocational education system level, it will help fill the local empirical research gap on cybersecurity literacy among secondary vocational students and offer a reference point for education authorities when formulating cybersecurity education policies. At the academic level, drawing on TPB, PMT, and TAM, the study constructs and tests a direct-effect framework examining how awareness, attitude, and behavior independently and jointly affect information protection effectiveness [5], [6], [7]. This study contributes to the literature by offering empirical evidence from secondary vocational students, validating a direct-effects model within a high-risk educational context, and identifying a significant gap between awareness, attitude, and behavior in cybersecurity practice.

Research Objectives

1. To assess the current levels of cybersecurity awareness, cybersecurity attitude, cybersecurity behavior, and information protection effectiveness among students at the secondary vocational school.
2. To analyze the direct effects of cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior on information protection effectiveness.
3. To investigate the joint influence of cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior on information protection effectiveness when included in the same model, and to identify the key predictors.

This study empirically tests the following four hypotheses:

- H1: Higher levels of cybersecurity awareness are positively associated with better information protection effectiveness.
- H2: More positive cybersecurity attitude is positively associated with better information protection effectiveness.
- H3: More regulated (norm-compliant) cybersecurity behavior is positively associated with better information protection effectiveness.
- H4: When cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior are simultaneously included in the same model, they exert a significant joint positive predictive effect on information protection effectiveness.

Research Methodology

1. Research Design and Theoretical Framework

This study adopts a quantitative, cross-sectional, non-experimental design, with current students at the focal secondary vocational school as the research population. The conceptual model includes three independent variables—cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior—and one dependent variable—information protection effectiveness. The core objective is to test the effects of these variables on information protection effectiveness.

Figure 1 presents the conceptual framework of this study, illustrating the direct effects of cybersecurity awareness, attitude, and behavior on information protection effectiveness. Arrows denote the positive direct effects hypothesized in H1–H3, while the three variables collectively exert a significant joint positive predictive effect on information protection effectiveness (H4).

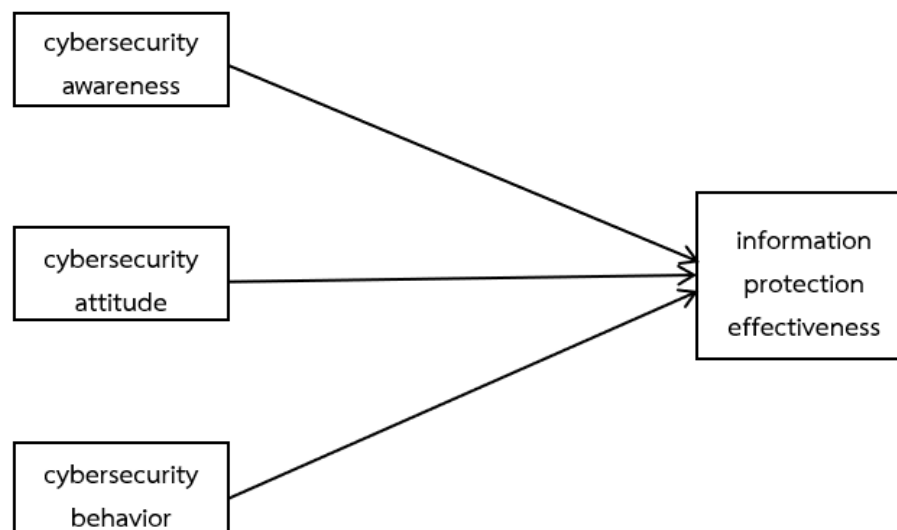


Figure 1 Conceptual framework of the direct effects of cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior on information protection effectiveness

The theoretical framework draws on three established theories. Protection Motivation Theory (PMT) explains individuals' protective decision-making mechanisms through threat appraisal and coping appraisal, providing support for the relationship between cybersecurity awareness and information protection effectiveness [8]. The Technology Acceptance Model (TAM) posits that perceived usefulness and perceived ease of use determine technology adoption intentions, supporting the hypothesized positive effect of cybersecurity attitude on outcomes [6]. The Theory of Planned Behavior (TPB) states that behavior is jointly driven by attitude, subjective norms, and perceived behavioral control, reinforcing the impact of attitude and behavior on outcomes [5].

This study adopts a regression-based approach as a baseline model. Future research may extend this model using SEM to examine mediation effects.

2. Participants and Sampling

The target population consists of current students enrolled at a secondary vocational school in eastern China. Inclusion criteria are: currently enrolled, providing consent to participate, and being able to complete the online questionnaire independently. Exclusion criteria are: duplicate submissions and clearly invalid responses.

This study adopts simple random sampling (SRS). SRS is appropriate for this study as it ensures equal probability of selection and reduces sampling bias across student groups. The sampling frame is a roster of currently enrolled students provided by the Academic Affairs Office. The sampling frame is randomly shuffled using a computer, and the online questionnaire link is distributed according to the randomized order. For students who do not respond by the deadline, invitations are extended to subsequent entries on the randomized list until the target number of valid responses is reached. The sampling list is used only to contact students; the questionnaire itself does not record identifiable information. A Cochran finite-population correction is used, and the target number of valid questionnaires is set at 352 to ensure the statistical power of subsequent factor analysis and regression analysis.

3. Questionnaire and Measures

The questionnaire includes four construct scales, all using 5-point Likert-type items (1 = "strongly disagree" to 5 = "strongly agree").

3.1 Cybersecurity Awareness

Dimensions measured include cognitive knowledge and risk perception, drawing on the cybersecurity awareness scale developed in [9]. The scale contains 8 items (including 1 reverse-coded item) focusing on confidentiality/privacy, phishing recognition, and strong passwords. Each item is scored from 1 to 5; the reverse-coded item is recoded as 6 minus original score; the mean of all items serves as the construct score.

3.2 Cybersecurity Attitude

The dimension measured is value evaluation of security norms and willingness to comply, based on the "perceived usefulness" dimension in TAM and the "attitude" dimension in TPB [5], [6]. The scale contains 8 items (including 1 reverse-coded item) adapted from [10]. Scoring follows the same procedure as awareness.

3.3 Cybersecurity Behavior

The dimension measured is everyday protective practices such as password management, two-factor authentication, caution with links and attachments, timely updates, privacy settings, and device hardening [11]. The scale contains 8 items (including 1 reverse-coded item) developed using Hadlington's Risky Cybersecurity Behaviours scale as reference [10].

3.4 Information Protection Effectiveness

The dimension measured is self-reported information protection outcomes over the past three months, including whether losses have been avoided, ability to identify and recover from incidents, and effectiveness of privacy protection [4]. The scale contains 8 items (including 1 reverse-coded item).

4. Pilot Study, Reliability, and Validity

A small-scale pilot test was conducted to examine the comprehensibility of questionnaire items. Based on feedback, item wording was adjusted to ensure appropriateness for the cognitive level of secondary vocational students. Content validity was assessed using the Index of Item-Objective Congruence (IOC) by three experts, with all items exceeding 0.67.

For the formal dataset, Cronbach's α is calculated for each subscale. Values between 0.70 and 0.95 are considered acceptable, with values ≥ 0.80 indicating good internal consistency. The Kaiser-Meyer-Olkin (KMO) measure and Bartlett's test of sphericity are reported for each construct. KMO ≥ 0.60 and Bartlett's $p < 0.05$ indicate that the correlation matrix is suitable for multivariate analyses.

5. Data Collection Procedures and Ethics

This study was submitted to the school management committee for review, and data collection began only after formal approval was granted. Before data collection, students received a written informed consent form explaining the research purpose, participation rights, data confidentiality, and use of results. Only students who signed the consent form proceeded to the questionnaire.

From October to November 2025, the questionnaire was distributed and collected online via a survey platform (link/QR code). Participation was anonymous and voluntary. The expected completion time was 8–10 minutes. After data export, all records were de-identified before analysis.

6. Data Analysis

Data were analyzed using SPSS 26.0, with a significance level set at $p < 0.05$. The analytical procedures included: descriptive statistics (mean, standard deviation, minimum, maximum) and reliability analysis (Cronbach's α) to assess current levels and internal consistency; Pearson correlation analysis to examine linear relationships among variables; simple linear regression models to test H1–H3, with information protection effectiveness as the dependent variable and each predictor entered separately; hierarchical multiple regression to test H4, with behavior entered in Step 1, and awareness and attitude added in Step 2. Multicollinearity diagnostics (Tolerance, VIF) were conducted for the final model.

Overall, the research procedure consisted of questionnaire development, pilot testing, data collection, reliability and validity assessment, and statistical analysis.

Research Results

The findings are presented below in the same sequence as the research objectives: first, the current levels of the four constructs; second, the direct effects of cybersecurity awareness, attitude, and behavior on information protection effectiveness; and third, their joint influence in the same model.

1. Data Preprocessing and Sample Characteristics

A total of 352 valid questionnaires were obtained ($N = 352$). All items were scored on a five-point Likert scale. For data cleaning, the survey was administered by course instructors in a standardized manner. Anonymous responses and unified instructions were used. Routine quality checks were carried out after data collection; no questionnaires met the exclusion criteria.

Among the respondents, 213 were male (60.5%) and 139 were female (39.5%). There were 127 first-year students (36.1%), 116 second-year students (33.0%), and 109 third-year students (31.0%). The largest group were from electronics and information (123 students, 34.9%), followed by equipment manufacturing (92 students, 26.1%) and transportation (85 students, 24.1%). Finance and commerce (52 students, 14.8%) was relatively smaller. Overall, the sample distribution indicates that students from different grades and majors were adequately represented, supporting the reliability of subsequent statistical analyses.

Table 1 Distribution of Sample Background Characteristics ($N = 352$)

Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	213	60.5
	Female	139	39.5
Grade	First year	127	36.1
	Second year	116	33.0
	Third year	109	31.0
Major	Electronics & IT	123	34.9
	Equipment Manufacturing	92	26.1
	Transportation	85	24.1
	Finance & Commerce	52	14.8

From Table 1, it can be seen that the respondents were drawn from different genders, grades, and majors, with a slightly higher proportion of male students and a relatively balanced representation across grade levels.

2. Reliability and Validity Testing

Internal consistency was assessed using Cronbach's α . The coefficients were 0.899 for awareness, 0.905 for attitude, 0.928 for behavior, and 0.908 for information protection effectiveness, all ≥ 0.80 , indicating good internal consistency. KMO values ranged from 0.918 to 0.928, and Bartlett's tests of sphericity were all significant ($\chi^2 = 1334.64\text{--}1925.07$, $df = 28$, $p < 0.001$), suggesting that the data were suitable for factor analysis.

Table 2 Reliability and KMO Test Results for the Main Variables

Construct	Cronbach's α	KMO Measure	Bartlett's χ^2 (df = 28)	p-value
cybersecurity awareness	0.899	0.927	1334.641	< 0.001
cybersecurity attitude	0.905	0.928	1452.208	< 0.001
cybersecurity behavior	0.928	0.922	1925.073	< 0.001
information protection effectiveness	0.908	0.918	1588.077	< 0.001

From Table 2, it can be seen that all variables achieved satisfactory reliability and validity levels, indicating that the data were appropriate for further statistical analysis.

3. Descriptive Statistics

Overall, all four means are above the midpoint of 3 on the five-point scale. cybersecurity attitude has the highest mean ($M = 3.79$, $SD = 0.63$), followed by cybersecurity awareness ($M = 3.62$, $SD = 0.69$) and information protection effectiveness ($M = 3.55$, $SD = 0.64$), whereas cybersecurity behavior has the lowest mean ($M = 3.33$, $SD = 0.68$).

Table 3 Descriptive Statistics for the Four Main Variables (N = 352)

Variable	Minimum	Maximum	Mean (M)	SD
cybersecurity awareness	1	5	3.62	0.69
cybersecurity attitude	1.25	5	3.79	0.63
cybersecurity behavior	1	5	3.33	0.68
information protection effectiveness	1.63	5	3.55	0.64

From Table 3, it can be seen that cybersecurity attitude recorded the highest mean score, while cybersecurity behavior showed the lowest mean score, indicating the existence of an awareness–attitude–behavior gap among the students.

4. Correlation Analysis

Pearson's correlation coefficients were computed with two-tailed tests. The results showed: cybersecurity awareness–cybersecurity attitude = 0.490, cybersecurity awareness–cybersecurity behavior = 0.395, cybersecurity awareness–information protection effectiveness = 0.395, cybersecurity attitude–cybersecurity behavior = 0.436, cybersecurity attitude–information protection effectiveness = 0.434, cybersecurity behavior–information protection effectiveness = 0.554. All correlations are statistically significant at $p < 0.001$. The correlation between behavior and information protection effectiveness is the strongest ($r = 0.554$).

These findings preliminarily support the proposed hypotheses and indicate that cybersecurity behavior may play the most influential role in predicting information protection effectiveness.

Table 4 Correlation Matrix for cybersecurity awareness, cybersecurity attitude, cybersecurity behavior, and Information protection effectiveness (N = 352)

	cybersecurity awareness	cybersecurity attitude	cybersecurity behavior	information protection effectiveness
cybersecurity awareness	—	0.490	0.395	0.395
cybersecurity attitude	0.490	—	0.436	0.434
cybersecurity behavior	0.395	0.436	—	0.554
information protection effectiveness	0.395	0.434	0.554	—

From Table 4, it can be seen that all four variables were positively and significantly correlated with one another, while cybersecurity behavior exhibited the strongest relationship with information protection effectiveness.

5. Hypothesis Testing

5.1 Tests of H1–H3 (Simple Regression Models)

Hypothesis H1: Higher levels of cybersecurity awareness are positively associated with better information protection effectiveness. The regression results show that cybersecurity awareness has a significant positive effect on information protection effectiveness, with $\beta = 0.395$, $t = 8.045$, $p < 0.001$, supporting H1. The model has $R^2 = 0.156$.

Hypothesis H2: More positive cybersecurity attitude is positively associated with better information protection effectiveness. The regression results indicate that attitude has a significant positive predictive effect, with $\beta = 0.434$, $t = 9.014$, $p < 0.001$, supporting H2. The model has $R^2 = 0.188$.

Hypothesis H3: More regulated cybersecurity behavior is positively associated with better information protection effectiveness. The regression results reveal that behavior has the strongest positive effect, with $\beta = 0.554$, $t = 12.452$, $p < 0.001$, supporting H3. The model has $R^2 = 0.307$.

Overall, the simple regression results consistently demonstrate that cybersecurity awareness, attitude, and behavior each have significant positive effects on information protection effectiveness, with cybersecurity behavior showing the strongest explanatory power.

Table 5 Simple Regression Models Testing H1–H3

Predictor	β	t	p-value	F	R^2
cybersecurity awareness	0.395	8.045	< 0.001	64.723	0.156
cybersecurity attitude	0.434	9.014	< 0.001	81.260	0.188
cybersecurity behavior	0.554	12.452	< 0.001	155.063	0.307

From Table 5, it can be seen that cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior each had a significant positive effect on information protection effectiveness when examined separately, with cybersecurity behavior exhibiting the strongest explanatory power.

5.2 Test of H4 (Hierarchical Multiple Regression)

Hypothesis H4: When cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior are entered into the same model, they jointly have a significant positive predictive effect on information protection effectiveness.

In Step 1, cybersecurity behavior was entered as the baseline. In Step 2, cybersecurity awareness and cybersecurity attitude were added. When all three predictors are included in Model 2, cybersecurity awareness ($\beta = 0.140$, $p = 0.006$), cybersecurity attitude ($\beta = 0.183$, $p < 0.001$), and cybersecurity behavior ($\beta = 0.419$, $p < 0.001$) all remain positive and statistically significant. Within Model 2, behavior still has the largest effect size.

The model fit improves from $R^2 = 0.307$ (Model 1) to $R^2 = 0.367$ (Model 2), with an increase of $\Delta R^2 = 0.060$. The change in F is $\Delta F(2, 348) = 16.458$, $p < 0.001$, indicating that adding cybersecurity awareness and cybersecurity attitude significantly enhances the model's explanatory power. Collinearity diagnostics show no issues: minimum tolerance = 0.690, maximum VIF = 1.448, both well below the threshold of 5.

Table 6 Hierarchical Multiple Regression Models Testing H4

Model	Predictor	β	t	p	R ²	ΔR^2	F	Sig.
Model 1	cybersecurity behavior	0.554	12.452	< 0.001	0.307	—	155.063	< 0.001
Model 2	cybersecurity awareness	0.140	2.786	0.006	0.367	0.060	67.225	< 0.001
	cybersecurity attitude	0.183	3.560	< 0.001				
	cybersecurity behavior	0.419	8.604	< 0.001				

From Table 6, it can be seen that all three predictors remained statistically significant when entered into the same model and jointly explained 36.7% of the variance in information protection effectiveness, with cybersecurity behavior remaining the strongest predictor.

6. Summary of Hypothesis Testing Results

A summary of the hypothesis testing results is presented in Table 7. All four hypotheses were statistically supported, indicating that the proposed positive associations and joint predictive effect were confirmed by the data.

Table 7 Summary of Hypothesis Testing Results

Hypothesis	Content	Statistical Method	Key Statistics	Result
H1	Higher levels of cybersecurity awareness are positively associated with better information protection effectiveness	Simple Linear Regression	$\beta = 0.395$, $p < 0.001$, $R^2 = 0.156$	Supported
H2	More positive cybersecurity attitude is positively associated with better information protection effectiveness	Simple Linear Regression	$\beta = 0.434$, $p < 0.001$, $R^2 = 0.188$	Supported
H3	More regulated cybersecurity behavior is positively associated with better information protection effectiveness	Simple Linear Regression	$\beta = 0.554$, $p < 0.001$, $R^2 = 0.307$	Supported
H4	Joint positive predictive effect of the three constructs	Hierarchical Multiple Regression	$R^2 = 0.367$, $\Delta R^2 = 0.060$, $p < 0.001$	Supported

From Table 7, it can be seen that all four hypotheses were supported, indicating that cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior each had significant positive effects on information protection effectiveness, both individually and jointly.

Conclusion and Discussion

Conclusion

This study investigated the effects of cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior on information protection effectiveness among students at a secondary vocational school in China.

The findings indicate that students generally demonstrated moderate-to-high levels of cybersecurity awareness, attitude, behavior, and information protection effectiveness. Among the three predictors, cybersecurity behavior showed the strongest relationship with information protection effectiveness.

The hypothesis testing results confirmed that cybersecurity awareness, cybersecurity attitude, and cybersecurity behavior each had significant positive effects on information protection effectiveness. When entered simultaneously into the hierarchical regression model, all three variables remained significant predictors, jointly explaining 36.7% of the variance in information protection effectiveness.

The study therefore concludes that improving students' cybersecurity behavior, together with strengthening awareness and positive attitudes, can effectively enhance information protection effectiveness in secondary vocational education settings.

Discussion

The descriptive results provide a deeper look into the students' cybersecurity profiles. While students show a certain level of cybersecurity knowledge and risk perception, hold relatively positive attitudes toward complying with security requirements, and report reasonably good information protection outcomes, their cybersecurity behavior scores are clearly lower than those of awareness and attitude. This reflects a typical "awareness–attitude–behavior gap" [1], [2], indicating a noticeable gap between "knowing and valuing" and "actually doing" in everyday practice. For secondary vocational students, the challenge is no longer merely to tell them what is right or wrong, but to help them form stable secure behavior patterns.

The correlation results underscore the practical importance of students' proactive cybersecurity behaviors. Students who have a better understanding of cyber threats, who recognize the importance of security rules, and who adopt more standardized protective practices tend to experience fewer security incidents. These support the basic logic of the conceptual framework grounded in PMT, TAM, and TPB [5], [6], [8]. In particular, the finding that behavior is the strongest predictor suggests that the extent to which personal information can be well protected largely depends on students' concrete practices in areas such as password management, link verification, system updating, and privacy settings. The findings are consistent with previous research showing that human factors are often the weakest link in information security [3], [10].

They are also consistent with TPB, which posits that behavior directly determines outcomes. Compared with studies focusing on university students and general internet users [12], [19], the present findings further suggest that cybersecurity behavior may play an even more critical role among secondary vocational students. This may be related to their frequent exposure to practical training environments, enterprise systems, and semi-professional digital tasks, where improper security practices can directly affect information protection outcomes.

Even though awareness, attitude, and behavior jointly explain a meaningful proportion of the variance, a large part remains unexplained. This suggests that other factors may also play important roles, including school management policies, technical safeguards, platform designs, family supervision, peer norms, and individual characteristics such as self-control and risk preference [2], [4]. From a practical point of view, cybersecurity education should not rely solely on changing students' awareness and behavior; it also needs the support of institutional arrangements and technological measures. Additionally, this study is limited to a single institution, which may affect generalizability.

Finally, this study highlights the unique context of secondary vocational education. Compared with previous studies mainly focusing on general high schools or universities, it addresses the specific situation of secondary vocational students. These students often interact with school information systems, training equipment, and enterprise platforms in real or semi-real work environments. Weak cybersecurity habits in this context may affect not only personal accounts but also school networks and enterprise data. By empirically testing how awareness, attitude, and behavior jointly influence information protection effectiveness, this study provides localized evidence for integrating cybersecurity education into vocational programmes and underscores the importance of behavior-focused interventions.

Recommendations

1. Strengthening Cybersecurity Awareness

First, cybersecurity awareness should be integrated into existing courses through short, scenario-based learning materials focusing on password management, phishing recognition, privacy settings, and data backup.

2. Enhancing Cybersecurity Attitude

Second, schools should strengthen cybersecurity attitude by embedding it into professional competence education, student handbooks, and internship requirements, while encouraging positive reinforcement for good security practices.

3. Promoting Cybersecurity Behavior

Third, cybersecurity behavior should be the primary focus of training. Schools should create secure default environments, design task-based assessments that require protective actions, and organize practical drills to help students form stable security habits.

4. Strengthening Institutional Support and Collaboration

Finally, institutional support and multi-party cooperation should be enhanced through school–family–enterprise collaboration, school-level planning, and regular evaluation of students’ cybersecurity literacy and information protection effectiveness.

References

- [1] China Communist Youth League Central Committee Department of Youth Rights Protection, China Internet Network Information Center, “The 5th National Report on Minors’ Internet Use in China,” China Internet Network Information Center, Dec. 2023. [Online]. Available: <https://qnzz.youth.cn/qckc/202312/P020231223672191910610.pdf>
- [2] W. M. Ji and H. R. Wang, “Characteristics, problems, and governance strategies of minors’ internet use,” *Social Governance*, vol. 4, pp. 12–21, 2023.
- [3] R. Rohan et al., “A systematic literature review of cybersecurity scales assessing information security awareness,” *Heliyon*, vol. 9, no. 3, 2023. [Online]. Available: <https://doi.org/10.1016/j.heliyon.2023.e14234>
- [4] M. Zwilling et al., “Cyber security awareness, knowledge and behavior: A comparative study,” *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022. [Online]. Available: <https://doi.org/10.1080/08874417.2020.1712269>
- [5] I. Ajzen, “The theory of planned behavior,” *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, 1991. [Online]. Available: [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- [6] F. D. Davis, “Perceived usefulness, perceived ease of use, and user acceptance of information technology,” *MIS Quarterly*, vol. 13, no. 3, pp. 319–340, 1989.
- [7] D. Craigen, N. Diakun-Thibault, and R. Purse, “Defining cybersecurity,” *Technology Innovation Management Review*, vol. 4, no. 10, 2014. [Online]. Available: <https://timreview.ca/article/835>
- [8] J. E. Maddux and R. W. Rogers, “Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change,” *Journal of Experimental Social Psychology*, vol. 19, no. 5, pp. 469–479, 1983. [Online]. Available: [https://doi.org/10.1016/0022-1031\(83\)90023-9](https://doi.org/10.1016/0022-1031(83)90023-9)
- [9] I. Arpaci, O. Aslan, and I. E. Oner, “Cybersecurity awareness scale (CSAS) for social media users: Development, validity and reliability study,” *Information Development*, p. 02666669251336562, 2025. [Online]. Available: <https://doi.org/10.1177/02666669251336562>
- [10] L. Hadlington, “Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom,” *International Journal of Cyber Criminology*, vol. 12, no. 1, pp. 269–281, 2018. [Online]. Available: <https://doi.org/10.5281/zenodo.1467909>
- [11] A. Ertan, G. Crossland, C. Heath, D. Denny, and R. Jensen, “Cyber security behaviour in organisations,” arXiv preprint arXiv:2004.11768, 2020. [Online]. Available: <https://doi.org/10.48550/arXiv.2004.11768>

-
- [12] L. Bognár and L. Bottyán, “Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students,” *Education Sciences*, vol. 14, no. 6, p. 588, 2024. [Online]. Available: <https://doi.org/10.3390/educsci14060588>
- [13] L. Huraj, T. Lengyelfalusy, A. Hurajová, and D. Lajčin, “Measuring cyber security awareness: A comparison between computer science and media science students,” *TEM Journal*, vol. 12, no. 2, 2023. [Online]. Available: <https://doi.org/10.18421/TEM122-05>
- [14] A. Lui, C. Womack, and P. Orton, “Collaborative online international learning as a third space to improve students’ awareness of cybersecurity,” *Education and Information Technologies*, vol. 30, no. 10, pp. 13835–13856, 2025. [Online]. Available: <https://doi.org/10.1007/s10639-025-13336-8>
- [15] X. Du and T. Chintakovid, “A survey of cybersecurity awareness among undergraduate students at Yunnan University of Finance and Economics in China,” in *Proceedings of the 2023 International Conference on Education, Knowledge and Information Management (ICEKIM 2023)*, X. Yuan et al., Eds., *Advances in Humanities and Communications*, vol. 13, pp. 740–753, Atlantis Press, 2023. [Online]. Available: https://doi.org/10.2991/978-94-6463-172-2_78
- [16] Y. Yang, J. Liu, and Y. Yang, “Research on China’s innovative cybersecurity education system oriented toward engineering education accreditation,” *Information*, vol. 16, no. 8, p. 645, 2025. [Online]. Available: <https://doi.org/10.3390/info16080645>
- [17] J. Prümmer, T. van Steen, and B. van den Berg, “A systematic review of current cybersecurity training methods,” *Computers & Security*, vol. 136, p. 103585, 2024. [Online]. Available: <https://doi.org/10.1016/j.cose.2023.103585>
- [18] F. Schiliro, “Towards a contemporary definition of cybersecurity,” arXiv preprint arXiv:2302.02274, 2023. [Online]. Available: <https://doi.org/10.48550/arXiv.2302.02274>
- [19] Q. An, W. C. H. Hong, X. Xu, Y. Zhang, and K. Kolletar-Zhu, “How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates,” *International Journal of Information Security*, vol. 22, no. 2, pp. 305–317, 2023. [Online]. Available: <https://doi.org/10.1007/s10207-022-00637-z>
- [20] G. A. Thomopoulos, D. P. Lyras, and C. A. Fidas, “A systematic review and research challenges on phishing cyberattacks from an electroencephalography and gaze-based perspective,” *Personal and Ubiquitous Computing*, vol. 28, no. 3, pp. 449–470, 2024. [Online]. Available: <https://doi.org/10.1007/s00779-024-01794-9>