ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 13 (2026) No. 6, pp. 151-164
DOI:10.33168/JLISS.2026.0609

The Impact of Self-Efficacy on Cybersecurity Awareness and Behaviour

Zhaopeng Hu[1,2,*], Md Gapar Md Johar[3,*], Jacquline Tham[2]

[1]School of Information Engineering, Nantong Institute of Technology, Nantong, China

[2]School of Graduate Studies, Postgraduate Centre, Management and Science University, Shah Alam, Selangor, Malaysia

[3]Software Engineering and Digital Innovation Center, Management and Science University, Shah Alam, Selangor, Malaysia

huzhaopeng88@sina.com; mdgapar@msu.edu.my; jacquline@msu.edu.my

Abstract. With the continuous development of internet technology, cybersecurity issues have become increasingly prominent, particularly among students in higher education institutions. Although higher education institutions have been committed to strengthening cybersecurity awareness campaigns, students' cybersecurity awareness and behaviour remain inadequate. Many cybersecurity issues stem precisely from students' insufficient understanding of the importance of protective measures. Self-efficacy is a key factor determining students' cybersecurity awareness and behaviour. To further elucidate the impact of self-efficacy on cybersecurity awareness and behaviour, this study focuses on students at higher education institutions in Nantong City, Jiangsu Province, China, to investigate the extent to which self-efficacy influences students' cybersecurity awareness and behaviour. Employing a quantitative research methodology, the study conducted a questionnaire survey of 467 students from higher education institutions in Nantong City, utilising SPSS and AMOS software for data analysis and hypothesis testing. The results indicate that self-efficacy has a significant positive impact on the cybersecurity awareness of students in higher education institutions. Furthermore, the study found that self-efficacy not only directly influences students' cybersecurity behaviour but also indirectly influences their behaviour by enhancing their cybersecurity awareness. This study fills a gap in cybersecurity research within the higher education sector in Nantong, Jiangsu Province, China.

Keywords: Self-efficacy, Cybersecurity Awareness, Cybersecurity Behaviour, Higher Education Institutions

1. Introduction

With the continuous improvement and development of technologies such as 5G network communication and artificial intelligence, various network threats are also increasing (Admass et al., 2024). For example, research shows that Generation Z's intention to adopt artificial intelligence in digital banking is significantly driven by their perceived usefulness, awareness, and trust in the technology (Lim et al., 2025). Students in higher education institutions are the main group of internet users, spending increasingly more time online daily, closely related to their daily lives and studies, and heavily reliant on cyberspace. In online shopping environments, this reliance translates into digital behaviors where high-quality electronic services generate customer value and foster e-loyalty among university students (Nun et al., 2025). Due to the openness, virtuality, and anonymity of cyberspace, students in higher education institutions face risks such as personal information leakage, online fraud, malware attacks, and harmful information when using the internet (CIIC, 2025). Across different organizational environments, sensitive information and digital infrastructure are consistently identified as the primary assets most vulnerable to cyber threats, requiring proactive resilience building (Bahmanova & Lace, 2024). However, when encountering network risks, although students in higher education institutions have relatively high digital literacy, they still have problems such as weak cybersecurity awareness and irregular cybersecurity behaviour. Even some students with a certain level of confidence (i.e., high self-efficacy) lack sufficient cybersecurity awareness, leading to them suffering from network risks and engaging in unsafe online behaviours (Wang & Chen, 2025). According to relevant survey data from the China Internet Network Information Centre (CNNIC), in 2023, the proportion of Chinese university students experiencing cybersecurity incidents reached 38.7%, of which personal information leakage accounted for 62.3% and online fraud accounted for 45.1% (CNNIC, 2024). Based on the Ministry of Education's estimate of the number of students enrolled in regular colleges and universities nationwide (approximately 40 million in 2024), it is estimated that approximately 15-16 million college students suffer from various online risks each year (including personal information leaks, online fraud, and account theft).

In Nantong City, Jiangsu Province, China, higher education institutions have not yet implemented extensive cybersecurity education programmes. Consequently, when students encounter cyber risks, they lack the confidence to deal with them effectively; coupled with a lack of cybersecurity awareness, they may be particularly vulnerable to harm. Consequently, this study focuses on the relationship between self-efficacy, cybersecurity awareness and cybersecurity behaviour among students at higher education institutions in Nantong, Jiangsu Province, China. It aims to clarify the mediating role of cybersecurity awareness, thereby providing theoretical and practical support for higher education institutions in Nantong to implement cybersecurity education and enhance students' cybersecurity awareness and behaviour.

2. Literature Review

With the continuous advancement of internet technology, higher education institutions have increasingly become a key area of risk in terms of cybersecurity. As students in these institutions rely heavily on the internet for learning, socialising and accessing information, their susceptibility to cyber threats continues to rise. Research indicates that, as frequent users of cyberspace, students in higher education institutions face a higher risk of falling victim to online fraud, privacy breaches and the dissemination of inappropriate content (Yue, 2024).

2.1 Self-efficacy (SE)

Self-efficacy plays a key role in cybersecurity behaviour. Self-efficacy (SE) is defined as an individual's belief in their ability to successfully perform a specific task (Xu & Xu, 2025). Cong et al. (2025) noted that self-efficacy significantly and positively predicts the level of cybersecurity behaviour among students in higher education institutions, with particularly notable effects in password management and

privacy protection. Concurrently, Warkentin et al. (2025) found through empirical research that self-efficacy not only directly influences behaviour but also enhances individuals' understanding of security strategies and their willingness to implement them. Furthermore, in phishing scenarios, the higher an individual's self-efficacy, the greater their ability to identify fraudulent information and take protective measures (Lee et al., 2023). From the perspective of educational interventions, research indicates that cybersecurity courses or training can significantly enhance students' levels of self-efficacy, thereby further improving their security behaviour (Abdul & Mat, 2024). Furthermore, studies in the financial sector confirm that managing human vulnerabilities through continuous training is essential for effective cybersecurity prevention (Danilavičius, 2025). Consequently, self-efficacy serves not only as a direct predictor of behaviour but also as a crucial psychological mechanism linking cognition and behaviour.

2.2 Cybersecurity Awareness (CSA)

In terms of cybersecurity awareness, it is widely regarded as a fundamental factor influencing the cybersecurity behaviour of students in higher education institutions. Cybersecurity awareness refers to an individual's ability to recognise cyber threats, assess risks, and take proactive measures to protect themselves. Fostering a robust security awareness culture through continuous education serves as a fundamental defense mechanism to improve secure digital behaviors and resist emerging cyber threats (Khan et al., 2025). Bognár & Bottyán (2024), through the construction of a structural equation model, demonstrated that cybersecurity awareness among students in higher education institutions possesses a multidimensional structure (such as password security, device protection and information identification), and that each dimension significantly influences their security behaviour. Similarly, Ahmead et al. (2024) found in a survey of undergraduates that students with lower levels of cybersecurity awareness were more likely to exhibit high-risk online behaviours, such as clicking on unknown links or neglecting privacy protection (Ahmead et al., 2024).

Further research indicates that although students in higher education generally possess basic cybersecurity knowledge, there remains a gap between their security awareness and actual behaviour. Moallem's (2018) study noted that whilst students are able to identify common cyber threats, they frequently engage in unsafe behaviour in practice, reflecting that security awareness has not yet been fully translated into behavioural habits. Meanwhile, Al Zaidy's (2025) empirical research indicates that the majority of students in higher education institutions possess a high level of security cognition at the conceptual level (such as recognising strong passwords), but their behavioural responses in complex situations remain inadequate.

2.3 Cybersecurity Behaviour (CSB)

Cybersecurity behaviour is influenced not only by cybersecurity awareness but also by beliefs (such as self-efficacy). A wealth of research indicates that the effect of cybersecurity awareness alone on cybersecurity behaviour is not particularly strong; this phenomenon is particularly evident among students in higher education institutions. Jangid (2025) points out that although most students in higher education institutions have a basic understanding of common threats (such as phishing or the risks of weak passwords), they frequently exhibit high-risk behaviour in their actual online activities, such as reusing simple passwords or clicking on unknown links. This suggests that relying solely on cybersecurity awareness is insufficient to regulate cybersecurity behaviour. Further empirical research has revealed that, in cross-sectional studies of undergraduates, students in higher education institutions already exhibit insufficient cybersecurity awareness; if they have previously experienced a cybersecurity threat, this significantly reduces their self-confidence, leading them to engage in risky online behaviour and expose themselves to cyber risks (Ahmead et al., 2024).

Consequently, enhancing cybersecurity behaviour can be achieved by strengthening students' self-efficacy and cybersecurity awareness within higher education institutions. Extensive research indicates

that self-efficacy not only directly influences cybersecurity behaviour but also acts indirectly through cybersecurity awareness (Zheng, 2025; Gustara et al., 2025; Han et al., 2025). For example, Zheng et al. (2025) found that cybersecurity awareness has a significant positive impact on anti-fraud behaviour, with self-efficacy playing a partial mediating role. Furthermore, research by Bognár & Bottyán (2024) also indicates that cybersecurity education or training can significantly improve students' cybersecurity behaviour by enhancing their cybersecurity awareness and self-efficacy.

In summary, the cybersecurity behaviour of students in higher education institutions is the result of multiple interacting factors, with cybersecurity awareness and self-efficacy being two key variables. This mirrors findings in other digital contexts, where the online purchasing behaviors and artificial intelligence adoption of Generation Z are similarly governed by psychological factors such as attitude and perceived behavioral control (Oanh & Cuong, 2025). Similar structural mechanisms exist in broader educational technology adoption, where psychological factors significantly mediate the relationship between external variables and students' actual behavioural intentions (Paudel & Acharya, 2024). However, a review of the existing literature reveals that current research still has many shortcomings. Firstly, most scholars tend to focus on the direct impact of individual variables on cybersecurity behaviour, with a lack of in-depth exploration of the interactive relationship and causal pathways between cybersecurity awareness and self-efficacy. Secondly, although some studies have addressed mediating effects, empirical research on the complete pathway of 'Self-Efficacy(SE)→Cybersecurity Awareness(CSA)→ Cybersecurity Behaviour (CSB)' remains relatively limited, particularly with regard to validation among students in higher education institutions in Nantong City, Jiangsu Province, China.

In light of these research gaps, this paper takes students in higher education institutions in Nantong City, Jiangsu Province, China, as its research subjects, focusing on the interrelationships between self-efficacy, cybersecurity awareness and cybersecurity behaviour. Through empirical analysis, the paper aims to validate the validity of the proposed model.

3. Hypotheses and Research Methods

3.1 Hypotheses

Any research must clarify the relationship between the research question and broader theoretical concepts. Clarifying the relationships between variables helps to better understand the research question, thereby highlighting the significance of the study. This study examines the influence of self-efficacy on the cybersecurity awareness and behaviour of students in higher education institutions in Nantong City, Jiangsu Province, China. Self-efficacy refers to an individual's level of confidence and ability in dealing with cybersecurity threats (Blythe & Coventry, 2018). Furthermore, cybersecurity awareness is employed as a mediating variable, whilst cybersecurity behaviour serves as the dependent variable. Based on these variables, this paper proposes a conceptual framework aimed at addressing the gap in the existing literature regarding the influence of self-efficacy on cybersecurity awareness and behaviour among students in higher education institutions in Nantong, Jiangsu Province, China. Similar to how integrated theoretical frameworks effectively predict university students' continuous digital behaviors, a well-structured conceptual model is vital for deconstructing their cybersecurity decision-making processes (Goh et al., 2025).

Self-efficacy is an individual's internal confidence in their ability to perform specific security behaviours (Parkinson et al., 2017; Amin et al., 2025). Students in higher education institutions with higher self-efficacy are more confident in understanding and executing cybersecurity behaviours, such as setting strong passwords, regularly updating systems, identifying phishing attacks, and protecting personal privacy. This belief can enhance students' ability to adopt more proactive security measures when faced with cyber threats (Bottyán, 2023; Gwenhure, 2025). According to existing research, self-efficacy plays a significant role in the process of cybersecurity behaviour and is a key factor influencing

the implementation of such behaviours (Amin et al., 2025; al Kalbani & al Kalbani, 2025). Consequently, there is a positive relationship between self-efficacy and cybersecurity behaviour; that is, the higher the self-efficacy of students in higher education institutions, the more likely they are to engage in cybersecurity behaviours. Based on the above research, the following hypothesis is formulated.

H1: There is a positive correlation between self-efficacy(SE) and cybersecurity behaviour(CSB).

Self-efficacy refers to an individual's belief in their ability to perform specific security behaviours (Parkinson et al., 2017; Amin et al., 2025). A growing body of empirical research indicates that individuals make a significant contribution to enhancing cybersecurity awareness (Abd Latif et al., 2025; Manaoogaran & Mokhtar, 2026). Existing research has found that self-efficacy, as a belief in one's own capabilities, enhances the perception of threats, thereby raising the level of cybersecurity awareness (Zainal et al., 2022; Vafaei-Zadeh et al., 2025). Consequently, within higher education institutions, the higher the self-efficacy of students, the more likely they are to proactively seek out and comprehend cybersecurity knowledge, thereby elevating their level of cybersecurity awareness (Wang & Chen, 2025). Based on the above research, the following hypothesis is formulated.

H2: Self-efficacy (SE) is positively correlated with cybersecurity awareness(CSA).

Cybersecurity awareness, defined as an individual's understanding of cyber threats, risks and protective measures, is regarded as a key factor influencing the development of cybersecurity behaviour (Alqarni, 2025). A growing body of research has found a significant positive correlation between cybersecurity awareness and cybersecurity behaviour; that is, the higher the level of cybersecurity awareness, the greater the willingness to adopt secure behaviours and the higher the degree to which these are actually implemented (de Bruin & Mersinas, 2024; Nagari & Raharja, 2025). In higher education institutions, when students' levels of cybersecurity awareness increase, they are more likely to identify online risks and feel confident in applying cybersecurity measures to protect their own online security (Ruzaili et al., 2026). Based on the above research, the following hypotheses are formulated.

H3: Cybersecurity awareness(CSA) is positively correlated with cybersecurity behaviour(CSB).

Self-efficacy not only influences the implementation of cybersecurity behaviour but also affects an individual's understanding of cybersecurity levels (Kim, 2025). For students in higher education institutions, an increase in cybersecurity awareness enhances their cybersecurity beliefs (i.e. self-efficacy), and these beliefs further encourage them to adopt practical cybersecurity behaviours (Gwenhure, 2025). Existing research has found that students with higher levels of cybersecurity awareness and self-confidence are more likely to adopt proactive cybersecurity behaviours (Booc et al., 2024). Therefore, cybersecurity awareness mediates the relationship between self-efficacy and cybersecurity behaviour. Based on the above research, the following hypothesis is formulated.

H4: Cybersecurity awareness(CSA) mediates the relationship between self-efficacy(SE) and cybersecurity behaviour(CSB).

Based on the above hypothesis, we propose a comprehensive conceptual framework regarding the influence of self-efficacy factors on cybersecurity awareness and behaviour, as shown in Figure 1.

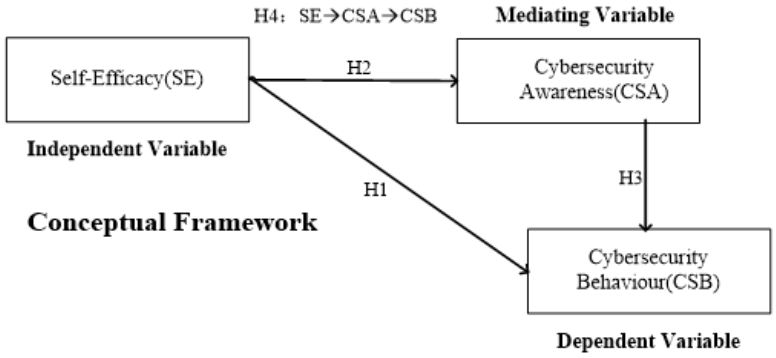

Fig.1：Conceptual Framework

3.2 Research Methods

This study employs a quantitative approach using descriptive statistical methods. The data are cross-sectional, meaning they were collected on a single occasion, with raw data gathered via a structured questionnaire. The questionnaire comprises a total of 14 items, including 4 items relating to self-efficacy, 5 items relating to cybersecurity awareness, and 5 items relating to cybersecurity behaviour. These questions were derived from previous academic research and incorporated feedback from cybersecurity experts to ensure the validity of the questionnaire. The questionnaire utilises a five-point Likert scale, where 1 = 'Strongly Disagree' and 5 = 'Strongly Agree'.

The subjects of this study are students currently enrolled at higher education institutions in Nantong City, Jiangsu Province, China. A stratified sampling method was employed, and demographic data were collected. The minimum required sample size was determined using Yamane's formula (Yamane, 1973), calculated as follows:

$$n = \frac{N}{1 + Ne^2} \tag{1}$$

$$n = \frac{143905}{1 + 143905 \times 0.05^2} = 389.8912 \approx 399 \tag{2}$$

Where n = sample size

N = population size = 143905

e = error (0.05) reliability level 95%

Calculations indicate that a sample size of approximately 399 participants is required to obtain a representative and statistically significant sample. To better support the findings of this study, a total of 604 questionnaires were distributed, yielding 467 valid responses.

This study utilised SPSS and AMOS for data analysis. SPSS was employed for data pre-processing and basic statistical tests, including descriptive statistics, reliability analysis and Exploratory Factor Analysis (EFA), to assess the internal consistency of the scales and lay the foundation for the construction of the conceptual framework of this study. AMOS was used for confirmatory factor analysis (CFA) and structural equation modeling (SEM) to test the construct validity of the three variables SE, CSA, and CSB in this study, and to construct the 'SE→CSA→CSB' model. The mediating effects were verified using a combination of confidence intervals and the Bootstrap method. The integration of these two methodologies ensured the rigour of this study and the reliability of its conclusions.

4. Data Analysis and Results

4.1 Sample Description

The subjects of this study are students at higher education institutions in Nantong City, Jiangsu Province, China. As shown in Table 1, the demographic characteristics of the respondents indicate that, of the 467 respondents, 237 were male (50.7%) and 230 were female (49.3%), with little difference between the two groups. The majority of students were in Year 1 and Year 2, accounting for 66% of the total. Furthermore, 264 students had passed the National Computer Rank Examination, representing 56.5% of the sample.

Table 1. Sample Description

No	Demographic Characteristics	Category	Frequency (people)	percentage
1	Gender	Male	237	50.70%
		Female	230	49.30%
2	Grade	Grade 1	139	29.80%
		Grade 2	169	36.20%
		Grade 3	108	23.10%
		Grade 4	51	10.90%
3	National Computer Ranking Examination	No	203	43.50%
		Level 1	206	44.10%
		Level 2	48	10.30%
		Level 3	10	21.00%

4.2 Reliability and Validity Tests

This study conducted reliability and validity tests on the three variables of self-efficacy (SE), cybersecurity awareness (CSA) and cybersecurity behaviour (CSB). The results of these tests are shown in Table 2.

4.2.1 Reliability Analysis

Reliability is used to measure the stability and internal consistency of questionnaire items. This study selected Cronbach's α coefficient and combined reliability (CR) as evaluation indicators. As shown in Table 2, the Cronbach's α coefficients for the three variables SE, CSA, and CSB are 0.874, 0.874, and 0.849, respectively, all greater than 0.7 (Nunnally, 1978), indicating internal consistency of the questionnaire items. Furthermore, the CR values for the three variables SE, CSA, and CSB are 0.875, 0.878, and 0.850, respectively, all satisfying≥0.6 (Hair et al., 2010). This further validates the reliability level of the questionnaire.

4.2.2 Convergent Validity Analysis

Convergent validity is achieved when all items in the measurement model are statistically significant. Convergent validity can be verified by calculating the loading factor, Item R^2, error variance and average variance extracted (AVE). As shown in Table 2, the loading factors for all items range from 0.65 to 0.83, all of which are greater than 0.6 (Haire et al., 2019). Furthermore, the corresponding Item R^2 values range from 0.42 to 0.69, all exceeding 0.4 (Haire et al., 2019), indicating that all items possess strong explanatory power for the latent variable. The Error Variance values for SE, CSA and CSB range from 0.09 to 0.20, indicating that the error variances for each item are positive and within a reasonable range. Measurement error is controlled within an acceptable range, the items are highly explained by the latent variables, and measurement quality is good (Hair et al., 2010). Furthermore, the AVE values for SE, CSA and CSB were 0.636, 0.591 and 0.532 respectively, all exceeding 0.5 (Fornell & Larcker,

1981). This indicates that each latent variable explains more than half of the item variance, demonstrating good convergent validity.

4.2.3 Discriminant Validity Analysis

Discriminant validity refers to the degree of distinction between latent variables; this study employed the Fornell-Larcker criterion for assessment. As shown in Tables 2 and 3, the for SE, CSA and CSB were 0.798, 0.768 and 0.729 respectively, all of which were higher than the correlation coefficients between the latent variables (Fornell & Larcker, 1981). This indicates that the three variables are well distinguished from one another and do not measure the same concept, thereby further ensuring the structural validity of the questionnaire.

Table 2. Results of Validity and Reliability Test

Variable	Item	Convergent Validity					Discriminant Validity		Reliability	
		Loading Factor	Item R^2	Error Variance	CR	AVE	Convergent Validity (AVE>0.5)	$\sqrt{AVE}$	Discriminant Validity ($\sqrt{AVE}$ >correlations)	α	Description
SE	SE4	0.83	0.66	0.09	0.875	0.636	Yes	0.798	Yes	0.874	Yes
	SE3	0.77	0.60	0.12							
	SE2	0.77	0.59	0.12							
	SE1	0.81	0.69	0.10							
CSA	CSA1	0.79	0.63	0.11	0.878	0.591	Yes	0.768	Yes	0.874	Yes
	CSA2	0.83	0.69	0.09							
	CSA3	0.79	0.62	0.11							
	CSA4	0.65	0.42	0.20							
	CSA5	0.77	0.60	0.12							
CSB	CSB1	0.75	0.56	0.13	0.850	0.532	Yes	0.729	Yes	0.849	Yes
	CSB2	0.72	0.52	0.15							
	CSB3	0.66	0.43	0.19							
	CSB4	0.77	0.60	0.12							
	CSB5	0.74	0.54	0.14							

Table 3. The square root value of AVE for discriminant validity

Code	SE	CSA	CSB
SE	0.798		
CSA	0.287	0.768	
CSB	0.362	0.384	0.729

4.3 Structural Equation Modelling

This study constructed a structural equation model comprising self-efficacy (SE) → cyber security awareness (CSA) → cyber security behaviour (CSB). As shown in Figure 2, the results indicate that $\chi^2/df = 1.091$ (<3.0) (Marsh & Hocevar, 1985), CFI = 0.998 (>0.9) (Bentler, 1990), and RMSEA = 0.014 (<0.08) (Browne et al., 1993), all of which meet the criteria for ideal fit, indicating that the model fits the data well. Path analysis revealed that the direct effect of SE → CSB remained significant ($\beta = 0.29$, $p < 0.001$), SE→CSA ($\beta=0.47$, $p<0.001$) and CSA→CSB ($\beta=0.51$, $p<0.001$) both exhibited significant positive predictive effects (Cohen, 1988; Hair et al., 2010).

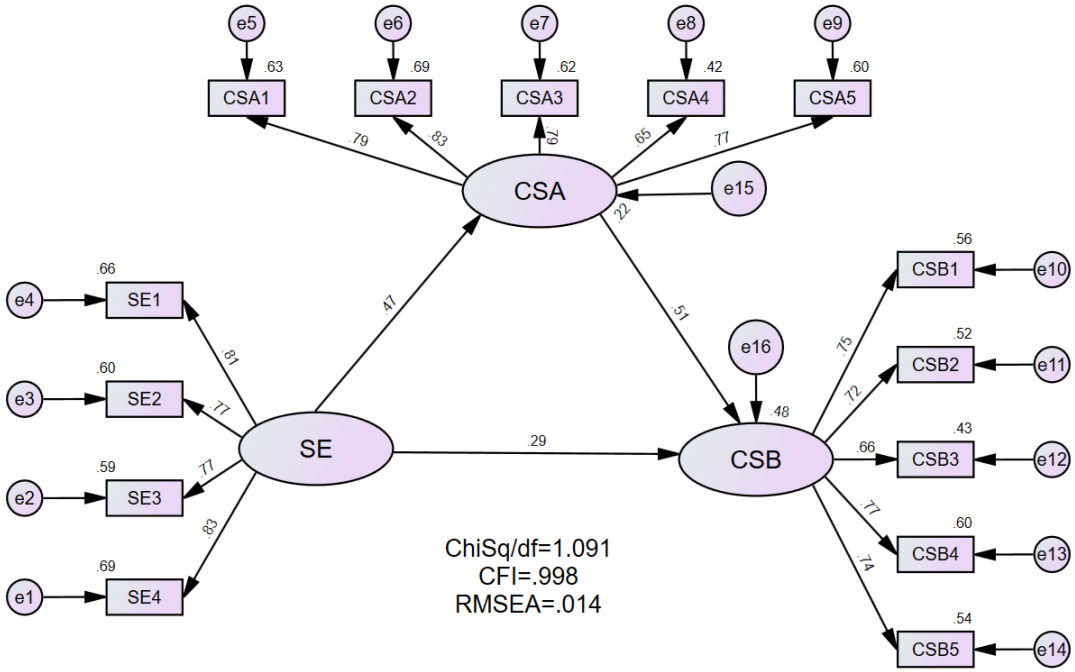

Fig.2: Structural Equation Modeling for this study

As shown in Table 4, the bootstrap confidence interval method in AMOS was used to test the mediation effect. The point estimate for the indirect effect SE→CSA→CSB was 0.231, SE = 0.041, Z = 5.634 (p = 0.002), and the bias-corrected and 95% percentile confidence intervals were (0.157, 0.321) and (0.155, 0.318), respectively, neither of which included 0, indicating that the indirect effect was significant (Preacher & Hayes, 2008). After controlling for mediation, the point estimate for the direct effect of SE on CSB was 0.278, SE = 0.065, Z = 4.277 (p = 0.002), and the bias-corrected and 95% percentile confidence intervals were both (0.154, 0.404), neither of which included 0, indicating that the effect was also significant. The point estimate for the total effect was 0.509, SE = 0.062, Z = 8.210 (p = 0.003), with bias-corrected 95% confidence intervals of (0.387, 0.628) and (0.393, 0.636), excluding 0. Since both the indirect and direct effects were significant and aligned, CSA partially mediated between SE and CSB, accounting for approximately 45.4% of the total effect.

Table 4. Mediating Effect Test of CSA between SE and CSB

Path relationship	Point Estimate	Product of coefficient		Bootstrapping					
				Bias-corrected			Percentile		
		SE	Z	Lower	Upper	P	Lower	Upper	P
Indirect Effects									
SE→CSA→CSB	0.231	0.041	5.634	0.157	0.321	0.002	0.155	0.318	0.002
Direct Effects									
SE→CSB	0.278	0.065	4.277	0.154	0.404	0.002	0.154	0.404	0.002
Total Effects									
	0.509	0.062	8.210	0.387	0.628	0.003	0.393	0.636	0.002

4.4 Hypothesis Testing

This study conducted hypothesis testing on the relationship between three variables: self-efficacy (SE), cybersecurity awareness (CSA), and cybersecurity behavior (CSB). The results are shown in Table 5.

Hypothesis H1 proposes that SE → CSB has a positive effect. Std.Estimate(β)=0.289, S.E.=0.05, C.R.=5.599, p<0.001. The effect is significant and consistent with the hypothesis, therefore H1 is supported. Hypothesis H2 proposes that SE → CSA has a positive effect. Std.Estimate(β)=0.467, S.E.=0.045, C.R.=8.872, p<0.001. The effect is significant, therefore H2 is supported. Hypothesis H3, which proposes a positive effect of CSA→CSB, has a Std.Estimate(β)=0.513, S.E.=0.063, C.R.=9.093, p<0.001, indicating a significant effect and supporting hypothesis H3. As shown in Table 4, hypothesis H4, which proposes the path SE→CSA→CSB, suggests that cybersecurity awareness partially mediates the relationship between self-efficacy and cybersecurity awareness.

All hypotheses passed statistical tests, and the critical ratios (C.R.) for each path were greater than 3.29 (p<0.001), indicating that the positive associations between variables in the model have high statistical reliability (Hair et al., 2010).

Table 5. Hypothesis Testing Path Coefficients

H.	Hypothesized Path	Std.Estimate(β)	S.E.	C.R.	P-value	Sig.	Supported
H1	SE→CSB	0.289	0.05	5.599	<0.001	***	Yes
H2	SE→CSA	0.467	0.045	8.872	<0.001	***	Yes
H3	CSA→CSB	0.513	0.063	9.093	<0.001	***	Yes

Note: S.E. = Standard Error; C.R. = Critical Ratio; *** $p < 0.001$

5. Discussion and Conclusion

This study took students from higher education institutions in Nantong, Jiangsu Province, China, as its research subjects and used AMOS and SPSS to empirically examine the relationships between self-efficacy, cybersecurity awareness and cybersecurity behaviour. The results indicate that students' self-efficacy has a significant direct positive influence on cybersecurity behaviour ($\beta = 0.289$, $p < 0.001$). Furthermore, students' self-efficacy significantly promotes an increase in cybersecurity awareness ($\beta = 0.467$, $p < 0.001$), whilst cybersecurity awareness, in turn, has a further positive influence on cybersecurity behaviour ($\beta = 0.513$, $p < 0.001$). All research hypotheses were supported, and the model fit indices ($\chi^2/df = 1.091$, CFI = 0.998, RMSEA = 0.014) indicate that the model fits the data extremely well.

From a theoretical perspective, the findings of this study validate the applicability of self-efficacy in the field of cybersecurity, namely that students' confidence in their ability to respond to cyber threats is a key factor in enhancing their cybersecurity behaviour. Furthermore, this study clarifies the partial mediating role of cybersecurity awareness between self-efficacy and cybersecurity behaviour (mediation effect size = 0.231, accounting for 45.4% of the total effect), demonstrating that the model exhibits a mediating effect: students in higher education institutions improve their cybersecurity behaviour by enhancing their awareness of cybersecurity risks. This finding fills a gap in research regarding students in higher education institutions in Nantong City, Jiangsu Province, China, within the field of cybersecurity.

This study is of particular practical significance for students at higher education institutions in Nantong, Jiangsu Province, China. As a key educational hub in China's Yangtze River Delta, Nantong should place even greater emphasis on cybersecurity. Research indicates that relying solely on students' own perceptions is insufficient to fully improve their cybersecurity behaviour when faced with cyber threats. Therefore, higher education institutions should implement relevant cybersecurity training to raise students' awareness of cybersecurity, thereby strengthening their cybersecurity behaviour.

6. Limitations

This study has the following limitations, which may be addressed in future research.

Firstly, there are limitations regarding sample representativeness. The study focused solely on students from higher education institutions in Nantong City, Jiangsu Province, China. As the sample originates from a single geographical area and does not cover internet users from different educational levels, professional backgrounds or regions, the generalisability of the conclusions remains to be tested. In future, the sample scope could be expanded to include universities in the Yangtze River Delta region and even nationwide.

Secondly, limitations regarding variable measurement. This study utilised cross-sectional data to measure self-efficacy, cybersecurity awareness and behaviour; consequently, it was unable to capture dynamic changes between variables or establish causal effects over the long term. Furthermore, the analysis focused solely on direct and mediating effects between variables, without incorporating moderating variables (such as cybersecurity experience), which may have resulted in the omission of key boundary conditions.

Thirdly, methodological limitations. The use of structural equation modelling to test hypotheses falls within the realm of correlational analysis; whilst it can verify the pathways of influence between variables, it cannot strictly establish causal relationships. Furthermore, as all data is derived from student self-reports, social desirability bias may be present; future research could enhance measurement validity by combining objective behavioural data (such as cybersecurity operation logs) or employing experimental methods.

References

Abd Latif, S. F., Sulaiman, N. S., Abd Aziz, N. S., Yacob, A., & Nasir, A. (2025). Development of Cybersecurity Awareness Model Based on Protection Motivation Theory (PMT) for Digital IR 4.0 in Malaysia. *International Journal of Advanced Computer Science & Applications, 16*(3).

Abdul, R. A., & Mat, S. M. (2024). Enhancing cybersecurity awareness through gamification: design an interactive cybersecurity learning platform for multimedia university students. *Journal of Informatics and Web Engineering, 3*(3), 21-40.

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications, 2*, 100031.

Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. *Crime Science, 13*(1), 29.

al Kalbani, H., & al Kalbani, A. (2025). Cybersecurity Awareness and Behavior among Faculty and Students in E-learning Environments.

Al Zaidy, A. (2025). Measuring Cybersecurity Awareness of Students: a Study of State College Students. *Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 2*(3), 17-40.

Alqarni, A. (2025). The relationship between cybersecurity awareness and data protection behaviors among Saudi secondary school students: the mediating role of cyber threat perception and the moderating role of internet usage duration. *Humanities and Social Sciences Communications, 12*(1), 1837.

Amin, M. S., Prybutok, V., & Rishat, M. A. S. A. (2025). The Role of Self-Efficacy in IT Employee Cybersecurity Safety Behavior. *International Journal of Human–Computer Interaction*, 1-23.

Bahmanova, A., & Lace, N. (2024). The high stakes of cyber resilience: What key business assets can SMEs afford to lose? *Journal of Service, Innovation and Sustainable Development, 5*(1), 12-29.

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological bulletin, 107*(2), 238.

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human behavior, 87*, 87-97.

Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences, 14*(6), 588.

Booc, N. B. B., Budiongan, K., & Carballo, R. (2024). Cybersecurity awareness, and cybersecurity behavior of high school students in Davao City: A mediation role of perceived behavioral control. *European Journal of Applied Science, Engineering and Technology, 2*(3), 4-9.

Bottyán, L. (2023). Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences, 13*(3), 1-11.

Browne, M. W., Cudeck, R., Bollen, K. A., & Long, J. S. (1993). Alternative ways of assessing model fit. *Testing structural equation models, 154*(4), 136-162.

China Internet Network Information Centre (CNNIC). (2024). Survey Report on the Current State of Cybersecurity Among Chinese University Students. Beijing: China Internet Network Information Centre.

CIIC. (2025). The Current State of Cybersecurity Awareness Among University Students and Strategies for Enhancement. China.org.cn, 23-07-2025. https://news.china.com.cn/2025-07/23/content_105320335.shtml

Cohen, J. (1988). Statistical power analysis for the behavioral sciences New York. NY: Academic, 54, 77-155.

Cong, B., Ye, Z., Jia, Q. N., Wu, Z., Feng, Y., Li, M., ... & Yang, Q. (2025). Personality traits Influence Internet Privacy Concerns through Social Anxiety and Privacy-Preserving Self-Efficacy. *Scientific Reports, 15*(1), 17414.

Danilavičius, V. (2025). Cybersecurity prevention analysis and guidelines in the banking sector. *Journal of Management Changes in the Digital Era, 2*(1), 207-218.

de Bruin, M., & Mersinas, K. (2024). Individual and Contextual Variables of Cyber Security Behaviour--An empirical analysis of national culture, industry, organisation, and individual variables of (in) secure human behaviour. *arXiv preprint arXiv:2405.16215*.

Fornell, Claes, and David F. Larcker. "Evaluating structural equation models with unobservable variables and measurement error." *Journal of marketing research* 18.1 (1981): 39-50.

Goh, M. L., Chow, M. M., Gan, S.-W., & Tang, C. X. (2025). Predicting e-wallet continuation behaviour among university students: Testing an integrated theoretical framework. *Journal of Logistics, Informatics and Service Science, 12*(2), 276-292.

Gustara, M., Cahyadi, E. R., & Sartono, B. (2025). Analysis of Cybersecurity Awareness and Behavior Among Students of IPB University: An Integration of Protection Motivation Theory and Theory of Planned Behavior. *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE), 8*(3), 13552-13565.

Gwenhure, A. K. (2025). University students' security behavior against email phishing attacks: insights from the health belief model. *Journal of Cybersecurity, 11*(1), tyaf034.

Hair Jr, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis. In *Multivariate data analysis* (pp. 785-785).

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis.

Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behavior among college students based on protection motivation theory: evidence from China. *Frontiers in Public Health, 13*, 1677024.

Jangid, D. (2025). Cybersecurity awareness among college students: A study on knowledge, behavior, and risk. ResearchGate. (Preprint). Retrieved from https://www.researchgate.net/publication/397887250_Cybersecurity_Awareness_among_College_Students_A_Study_on_Knowledge_Behavior_and_Risk

Khan, S., Rahman, H. M. M., Khan, N., & Lenga, O. T. S. (2025). Factors influencing digital security in Malaysia's journey through Industry Revolution 5.0. *Journal of Logistics, Informatics and Service Science, 12*(6), 157-185.

Kim, S. (2025). Impact of Cybersecurity Self-Efficacy on Digital Economic Behaviors Among Older Adults. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing, 62*, 00469580251370933.

Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Thwarting instant messaging phishing attacks: the role of self-efficacy and the mediating effect of attitude towards online sharing of personal information. *International Journal of Environmental Research and Public Health, 20*(4), 3514.

Lim, K. B., Low, K. H., Yeo, S. F., & Tan, C. L. (2025). Factors Influencing Generation Z's Adoption of AI in Banking: An Extended Technology Acceptance Model Approach. *Journal of Logistics, Informatics and Service Science, 12*(4), 178-192.

Manaoogaran, H., & Mokhtar, N. F. (2026). Sailing into Cyber Awareness: Exploring Determinants of Security Behaviour Among Seafarers. *Journal of Advanced Research in Business and Management Studies, 42*(1), 66-73.

Marsh, H. W., & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First-and higher order factor models and their invariance across groups. *Psychological bulletin, 97*(3), 562.

Moallem, A. (2018, June). Cyber security awareness among college students. In *International conference on applied human factors and ergonomics* (pp. 79-87). Cham: Springer International Publishing.

Nagari, S. F., & Raharja, S. (2025). Cyber Security Awareness, Knowledge and Behavior of Digital Banking Users in Salatiga. *Asia Pacific Fraud Journal, 10*(1), 15-29.

Nun, S. H., Moganadas, S. R., & Goh, M. L. (2025). The Path to E-Loyalty: Examining the Effects of E-Service Quality and Customer Value on E-Satisfaction Among Malaysian University Students. *Journal of Logistics, Informatics and Service Science, 12*(4), 1-17.

Nunnally, J. C. (1978). Psychometric Theory 2nd ed: Mcgraw hill book company.

Oanh, N. T. T., & Cuong, D. B. X. (2025). Digital Natives in Artificial Intelligence-Enhanced Marketplaces: Unraveling the Psychological Mechanisms Between Artificial Intelligence Adoption and Purchase Behavior Among Generation Z. *Journal of Logistics, Informatics and Service Science, 12*(11), 55-71.

Parkinson, J., David, P., & Rundle-Thiele, S. (2017). Self-efficacy or perceived behavioural control: Which influences consumers' physical activity and healthful eating behaviour maintenance?. *Journal of Consumer Behaviour, 16*(5), 413-423.

Paudel, S. R., & Acharya, N. (2024). Factors affecting behavioral intention to use ChatGPT: Mediating role of attitude. *Journal of Service, Innovation and Sustainable Development, 5*(2), 143-162.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior research methods, 40*(3), 879-891.

Ruzaili, H., Katuk, N., Zaini, K. M., & Abdullah, W. (2026). Phishing awareness and preventive measures among university students: knowledge, behaviors, and victimisation perspectives. *Millenium-Journal of Education, Technologies, and Health*, (29), e43489-e43489.

Vafaei-Zadeh, A., Nikbin, D., Teoh, K. Y., & Hanifah, H. (2025). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. *International Journal of Bank Marketing, 43*(3), 476-505.

Wang, H. Y., & Chen, H. M. (2025). Exploring Digital Confidence and Cybersecurity Awareness: A Study of Taiwanese University Students. *Frontiers in Social Thoughts and Humanity, 2*(03), 1-5.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*, 25-35.

Xu, J., & Xu, Y. (2025). The impact of self-efficacy on psychological resilience in EFL learners: a serial mediation model. *BMC psychology, 13*(1), 858.

Yamane, T. (1973). Statistics: An introductory analysis.

Yue, Q. (2024). Research on the Social Psychological Causes and Countermeasures of College Students' Network Violence. *Advances in Psychology, 14*, 0. https://www.hanspub.org/journal/paperinformation?paperID=103383

Zainal, N. C., Puad, M. H. M., & Sani, N. F. M. (2022). Moderating effect of self-efficacy in the relationship between knowledge, attitude and environment behavior of cybersecurity awareness. *Asian Social Science, 18*(1), 1-55.

Zheng, S Q. (2025). A Study on the Influence of Cybersecurity Awareness and Self-Efficacy on Anti-Fraud Behaviors. Thesis submitted to the Department of Industrial Management, I-Shou University, 1-71.