Journal of Information Technology Management
ISSN-OnLine: 2980-7972
University of Tehran

The Impact of Smartphone Users' Digital Literacy on Information Security Protection Intentions

Zhenxiang Cao*

*Corresponding author, Assistant Prof., Hefei Institute For Advanced Research, School of International Trade and Economics, Anhui University of Finance and Economics, Bengbu, China. E-mail: czx@aufe.edu.cn

Liqing Peng

Instructor, Department of Human Resources, Anhui University of Science and Technology, Huainan, China. E-mail: 448339509@qq.com

Yili Chu

Assistant Prof., School of Humanistic Medicine, Anhui Medical University, Hefei, China. E-mail: true111@foxmail.com

Fan Ye

Lecturer, College of Anhui Audit, Hefei, China. E-mail: 18205580587@163.com

Journal of Information Technology Management, 2025, Vol. 17, Issue 3, pp. 148-172
Published by the University of Tehran, College of Management
doi:%20https://doi.org/10.22059/jitm.2025.377234.3694
Article Type: Research Paper

Received: January 23, 2025
Received in revised form: April 02, 2025
Accepted: June 08, 2025
Published online: August 23, 2025

Abstract

In the digital economy era, the widespread use of smartphones has brought about new information security threats, increasing the risk of data leakage from personal devices. Digital literacy, defined as the skills and knowledge needed to navigate digital life effectively, offers new perspectives and motivation for safeguarding personal information security. This study investigates the relationship between digital literacy and smartphone users' intention to protect their information security. Drawing on Protection Motivation Theory (PMT) and Technology Threat Avoidance Theory (TTAT), a theoretical model was developed to examine both the direct and indirect effects of digital literacy on users' information security protection intentions. Questionnaire data from 372 smartphone users in China were analyzed

using Structural Equation Modeling (SEM). The results reveal that digital literacy has a significant positive impact on users' response efficacy, self-efficacy, and their intention to protect information security. Moreover, digital literacy influences protection intention indirectly through self-efficacy and response efficacy. However, perceived threat, although positively influenced by digital literacy, does not have a significant effect on users' protection intention. This study offers valuable insights for policymakers, educators, and businesses in promoting a secure mobile environment and provides practical recommendations for enhancing personal information security in the digital age.

Keywords: Digital literacy, Information security protection, Second-order factor model, Smartphone

Introduction

With the rapid development and application of mobile internet technologies, mobile smart devices, particularly smartphones, have experienced a dramatic expansion in their user base due to their multifunctional capabilities. In August 2022, the China Internet Network Information Center (CNNIC) released the 50th "Statistical Report on Internet Development in China," which showed that 99.6% of internet users in China accessed the internet via mobile phones. The total number of mobile phone users reached 1.668 billion, including 455 million 5G mobile phone users (CNNIC, 2022).

The widespread adoption of smartphones has introduced new information security risks, making it increasingly easy for sensitive data stored on these devices to be compromised. While users benefit from various convenient services, they also frequently input or store sensitive personal information on their smartphones. Threats such as apps from unverified sources, malicious software, and unsecured network connections have heightened the risk of personal information being stolen or misused, posing a significant threat to mobile information security. A lack of knowledge about information security often results in low awareness among users, who frequently fail to recognize or implement appropriate protective measures. The China Consumers Association (CCA), in its "Investigation Report on Personal Information Leakage in Apps," pointed out that 64% of respondents believe that the main source of personal information security issues is the lack of users' awareness regarding information security protection (CCA, 2018).

Accompanying the emergence of a new technological revolution, the deep integration of new-generation information technologies such as big data, cloud computing, and artificial intelligence with traditional industries has promoted the transformation of social development toward digitalization and intelligence. With digital knowledge and information as its core resources, the digital economy has flourished. In the new development pattern, digital literacy has become a basic ability that the public must possess, and it represents the core literacy

required for work, study, and life in the digital economy era. The Central Cyberspace Affairs Commission of China (CCAC) has issued the "Action Plan for Improving National Digital Literacy and Skills," which clearly states that enhancing digital literacy and skills across the population is a strategic task to meet the demands of the digital era, improve national quality, and promote the all-round development of individuals (CCAC, 2021).

For individuals in the digital age, digital literacy refers to the ability to better adapt to the digitalization of daily life. Theoretically, digital literacy represents users' skills in acquiring, using, evaluating, and innovating digital information, which contributes to enhancing their capacity to address various information risks and security challenges in the digital economy era. In this context, it is worth examining whether the digital literacy of smartphone users influences their intention to protect information security, and if so, how digital literacy affects this intention. Are there any intermediary mechanisms involved? Therefore, this paper explores the relationship between digital literacy and the intention to protect information security among smartphone users, within the context of digital economy development, to provide practical guidance for personal information security protection from an endogenous dynamic perspective.

Literature Review

User information security behavior is a pivotal focal point within cybersecurity, exerting considerable influence on the efficacy of security protocols and the susceptibility of systems to cyber assaults. The Protection Motivation Theory (PMT) is a prominent framework that elucidates and predicts user information security behavior (Rogers, 1983). This theory rests upon the foundational premise that, when confronted with a perceived threat, individuals are motivated to undertake specific countermeasures to protect themselves from the impending risk. Navigating a threat scenario entails a sequential process in which an individual first evaluates the perceived susceptibility and severity of the threat. This evaluation is then extended to an assessment of available countermeasures. Ultimately, behavioral decisions are formed based on these considerations. Perceived susceptibility refers to an individual's assessment of the likelihood of experiencing a negative outcome, while perceived severity denotes the degree of harm that could result from such an outcome. Response efficacy reflects an individual's belief that a particular course of action will be effective in mitigating the threat, whereas self-efficacy refers to an individual's confidence in their ability to implement protective measures.

Technological Threat Avoidance Theory (TTAT) is suitable for explaining how individuals avoid information technology threats in voluntary situations. The theory, proposed by Liang and Xue (2009), is rooted in protection motivation theory, the health belief model, and risk analysis research. When a user perceives an IT threat and believes it can be warded off by adopting protective measures, the resulting positive willingness motivates the user to

actively avoid it. The theory conceptualizes that threat perception arises from two antecedent variables: perceived severity and perceived susceptibility. In an individual's assessment of how to respond to a threat, the effectiveness of protective measures, their cost, and the individual's ability to adopt them are all taken into account (Liang & Xue, 2010).

An early application of Protection Motivation Theory (PMT) and Technological Threat Avoidance Theory (TTAT) in the field of information security is found in the study by Siponen et al. (2007), which investigated employees' adherence to information security protocols in the workplace. This seminal research emphasized the crucial role of threat perception and response efficacy variables. Since then, PMT and TTAT have been widely applied to study information security behavior. Examples include analyses of user reactions to malware threats (Tsai et al., 2016), evaluations of password protection strategies (Vedadi & Warkentin, 2020), examinations of email security practices (Ng et al., 2009), investigations of computer desktop security behaviors (Hanus & Wu, 2016), assessments of antivirus software usage (Lee et al., 2008), and reviews of computer security behaviors in the workplace (Yoon & Kim, 2013), among others.

Current research on user information security behavior focuses on Protection Motivation Theory (PMT) and Technology Threat Avoidance Theory (TTAT), often adding a few other influencing factors for consideration. However, this approach overlooks users' knowledge and digital literacy. Moreover, with the rapid growth and development of the digital economy, conclusions drawn from past studies are no longer fully applicable to the current context of individual digital literacy and skills development. Therefore, this study aims to address these limitations by adopting digital literacy as the foundational framework, incorporating key elements from PMT and TTAT as intermediaries to better elucidate the relationship between digital literacy and information security behavior.

Research Hypothesis

Digital Literacy

Digital literacy is "the efficient and rational use of digital technologies and the potential of digital tools to meet the information needs of individuals and society." People can locate, organize, understand, evaluate, and create information using digital technology (Julien, 2018). There are significant benefits to possessing digital literacy, as these skills and abilities lead to more positive health outcomes. Digital literacy encompasses utilizing interactive digital tools and searchable networks while ensuring proficient and secure engagement. Moreover, it protects against cybercriminal activities, including phishing and malicious hacking (Deye, 2015). This proficiency empowers the younger generation to harness the myriad opportunities arising from digital technology while concurrently safeguarding them against its diverse perils (Göldağ, 2021).

There is no direct evidence in the existing literature supporting the positive effect of digital literacy on self-efficacy, response efficacy, perceived threat, and behavioral intention in the context of personal information security. However, Wan et al. (2008) and Hatlevik et al. (2018) found that self-efficacy and response efficacy are enhanced by increases in IT perception, IT application skills, and information literacy. Moreover, the level of knowledge influences individuals' perception of risk (Dickson, 2005). A higher level of knowledge enhances one's ability to collect, analyze, and evaluate information resources, thereby increasing awareness of information security risks. For users, the most effective patch and countermeasure against information leakage are to improve their knowledge and skill levels, becoming knowledgeable and competent users who continuously assess threats and take action to protect personal information privacy.

An individual's response to external stimuli is closely related to their fundamental literacy (Califf & Brooks, 2020). The key to strengthening privacy awareness lies in familiarity with the basics of digital technology and mastery of its application skills, rather than merely focusing on personal privacy concerns (Büchi, 2017). Given users' cognitive limitations, privacy leaks are often inevitable, resulting in suboptimal privacy protection practices. It is common for users to lack sufficient knowledge about privacy protection; thus, it is essential to enhance training in privacy-related knowledge and skills to improve their protective capabilities (Wissinger, 2017). The most serious issue in privacy security involves marginalized or vulnerable internet users who lack advanced digital skills (Smith et al., 2015). Individuals with strong media and information processing skills tend to pay more attention to personal information privacy and are better equipped to ensure its protection. Users' privacy control behaviors are significantly associated with their knowledge of information technology, awareness of institutional practices, and understanding of privacy norms (Park, 2013). Barn (2014) pointed out that the level of IT knowledge is closely related to the degree of information security risks users face when accessing data via smartphones. Büchi et al. (2017) employed a structural equation model to demonstrate that proficiency and mastery of information skills are critical in reducing user information exposure and avoiding security problems.

Under the development of the digital economy, improving users' digital literacy facilitates their access to information security resources and enhances their ability to learn relevant knowledge. As a result, they gain a clearer understanding of the information security threats associated with smartphone usage. Furthermore, improving digital literacy can encourage users to leverage digital technologies more effectively as tools for safeguarding information security, recognize the convenience and utility of adopting protective measures, and strengthen their capability to control personal information security. This, in turn, enhances their belief in reducing information security risks through protective behaviors.

Based on these, the following hypotheses are proposed:

(1) Hypothesis H1a: Digital literacy of smartphone users positively affects their perceived threat.

(2) Hypothesis H1b: Digital literacy of smartphone users positively affects their response efficacy.

(3) Hypothesis H1c: Digital literacy of smartphone users positively affects their self-efficacy.

(4) Hypothesis H1d: Digital literacy of smartphone users positively affects their information security protection intention.

Perceived Threat, Response Efficacy, and Self-Efficacy

Perceived threat is derived from TTAT and refers to the individual's perception of the threat or harm brought by information technology. In this study, perceived threat refers to smartphone users' perception and assessment of smartphone information security risks. According to Wynn et al. (2013), if the public believes they are more vulnerable to negative situations, they are more likely to take precautions to avoid negative consequences. When users believe that smartphones pose risks and threats that could harm personal information security and privacy, a threat assessment will be conducted to determine whether appropriate information security protection is needed. That is, users must be fully aware of the threats to their information security before they can achieve information security protection. Bulgurcu (2010) and Lai et al. (2012) also confirmed that when users face information security threats, they tend to be motivated to take avoidance-oriented actions and behaviors.

Response efficacy is a cognitive process, and how individuals handle risk is influenced by their perception of response efficacy (Ortiz et al., 2018). When applied to this study, it refers to smartphone users' subjective perception of whether implementing information security protection can effectively prevent information risks and enhance information security. Wissinger (2017) and Yoon et al. (2012) pointed out that response efficacy positively influences individuals' willingness to engage in information security behaviors. If users are fully aware of the advantages of technological tools and solutions for information security protection, they will be more inclined to adopt effective security measures (Ifinedo, 2014). In the context of smartphone use, users will only intend to adopt protective behaviors if they recognize the importance of information security and believe that such behaviors are beneficial to the security of their smartphones. Conversely, if users believe that their information security protection behavior does not produce the expected results, then even if they are concerned about security issues, they may lack the motivation or intention to engage in protective actions.

Self-efficacy is an individual's assessment and belief about his or her abilities. Numerous studies have found that self-efficacy significantly impacts individuals' behavioral intentions regarding information security (Esmaeili, 2014; Hanus and Wu, 2016; Workman, 2008). PMT suggests that individuals can anticipate the outcomes of their actions by evaluating their capabilities. Therefore, those with a stronger sense of self-efficacy are more confident in adopting information security practices. When users perceive that they can manage risks and believe in their capacity to do so, they are more likely to proactively use their skills to avoid such risks (Büchi et al., 2017). According to research in the field of information security behavior, enhancing self-efficacy is a key condition for the effective implementation of IT security measures. When using IT services, users with higher self-efficacy are more willing to avoid threats during their interaction with IT services. If the user believes that their information security protection behavior can effectively safeguard the smartphone, they will be more inclined to perform such protective actions.

Based on these, the hypotheses are proposed:

(1) Hypothesis H2: Perceived threat of smartphone users positively affects their information security protection intention.

(2) Hypothesis H3: Response efficacy of smartphone users positively affects their information security protection intention.

(3) Hypothesis H4: Self-efficacy of smartphone users positively affects their information security protection intention.

Research Model Construction

This study constructs a comprehensive theoretical model (see Figure 1) based on Protection Motivation Theory (PMT), Technology Threat Avoidance Theory (TTAT), and digital literacy theory. The model postulates that digital literacy directly influences smartphone users' intention to protect information security, and indirectly affects this intention through the mediating roles of self-efficacy, response efficacy, and perceived threat.

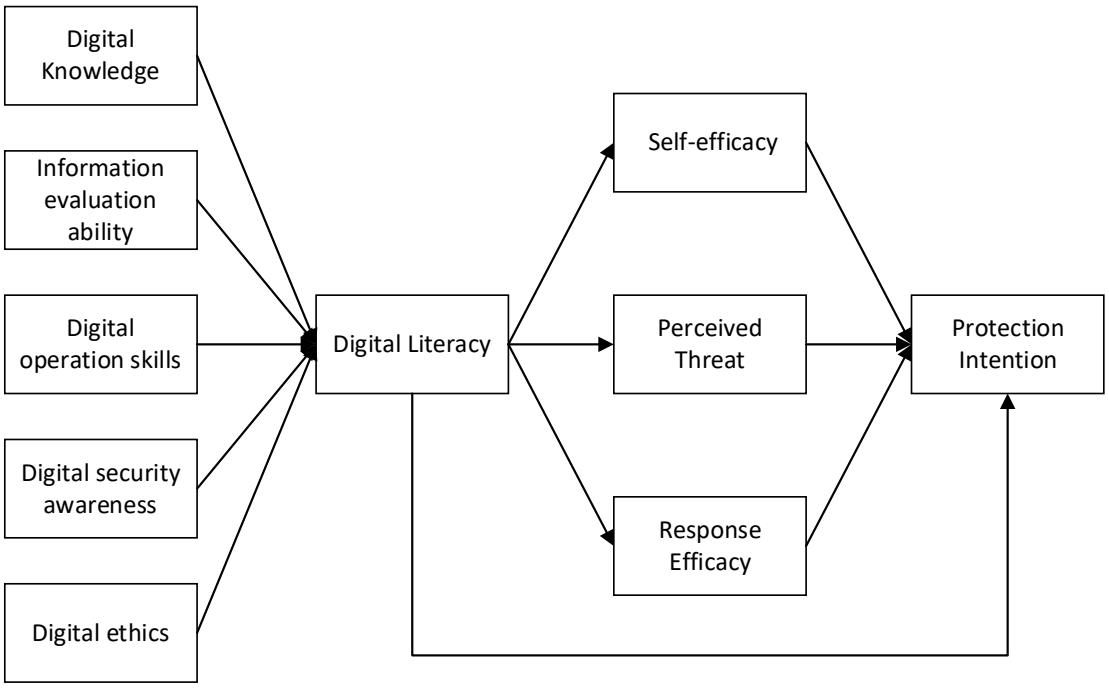

Figure 1. Research model

Methodology

This study employs a quantitative research design to explore the impact of digital literacy of smartphone users on their intention to protect information security. The research framework is based on the integration of PMT, TTAT, and digital literacy theory. Together, these theories help explain how digital literacy influences users' psychological processes, including perceived threat, response efficacy, and self-efficacy, ultimately shaping their behavioral intention to protect information security.

To ensure robustness and minimize potential biases, this study uses a questionnaire survey method coupled with Structural Equation Modeling (SEM) for data analysis. The questionnaire approach allows for efficient and extensive data collection, capturing diverse user experiences and behaviors concerning smartphone information security. SEM, with its ability to handle complex relationships between multiple variables, offers a powerful tool to test the proposed hypotheses and assess both direct and indirect effects among the constructs, thereby enhancing the reliability and validity of the findings.

Sample Selection

A non-probability sampling method was employed to select participants for this study. Given the widespread use of smartphones, the target population was defined as individuals aged 18 and above who actively use smartphones. Participants were recruited through multiple channels, including social media platforms, online forums, and local communities in Hefei

and Huainan, China, to ensure a wide reach and diversity of the sample. To ensure the representativeness and relevance of the sample, the inclusion criteria were as follows: (1) being a current smartphone user, (2) having a basic understanding of information security, and (3) being at least 18 years old. These criteria ensured that the participants had relevant experiences and knowledge to provide meaningful responses regarding digital literacy and information security protection intentions.

Data Collection

Pre-survey

To ensure the validity and cultural appropriateness of the questionnaire, a comprehensive pre-survey process was conducted. The initial questionnaire consisted of 35 items covering key constructs such as digital literacy, perceived threat, response efficacy, self-efficacy, and protection intention. The questionnaire was tailored to the context of smartphone users and their information security behaviors. The pre-survey involved professional translation and back-translation to maintain the integrity of the original items while ensuring cultural relevance. Field experts in digital literacy and information security reviewed the translated items to verify their alignment with the measured concepts and cultural sensitivity. A pilot test was conducted with 40 smartphone users from diverse backgrounds. These participants evaluated the clarity of the items, the relevance of the questions to their information security experiences, and the overall structure of the survey. Constructive feedback was collected, and revisions were made accordingly. Ambiguous or complex items were simplified, and redundant or irrelevant questions were removed. After the pilot study and subsequent revisions, a 30-item questionnaire was finalized for the main survey.

Official Data Collection

Before participating in the survey, all participants were provided with an informed consent form explaining the study's purpose, the voluntary nature of participation, and the confidentiality of their responses. Participants were required to acknowledge their consent by checking a box before accessing the questionnaire, ensuring ethical compliance. They were assured of the anonymity of their responses and informed that their data would be used solely for research purposes. Data were securely stored with restricted access to the research team, and participants were informed of their right to withdraw from the study at any time without consequences. The primary data collection method was an online survey. The official questionnaire was distributed from August to November 2022. A total of 405 completed surveys were collected through online platforms and a small number of paper questionnaires distributed in Hefei and Huainan, China. An initial screening process was conducted to ensure data quality. Questionnaires with any unanswered items, inconsistent responses, or those completed in less than 8 minutes (indicating a lack of thoughtful engagement) or more than

30 minutes (suggesting potential comprehension issues or distractions) were discarded. Additionally, duplicate entries from the same IP address were removed to ensure the validity of the responses. After applying these screening criteria, 372 valid questionnaires remained for analysis. The survey comprised 30 items, resulting in a ratio of observations to variables of 12.4. This ratio exceeds the recommended minimum of 5:1 (Hair et al., 2018), indicating that the sample size was sufficient for conducting factor analysis and SEM. Demographic characteristics of the sample (including gender, age, education, and occupation distributions) are presented in Table 1.

Table 1. Demographic characteristics of the sample

Constructs	Category	Frequency	Percentage
Gender	Male	207	55.65%
	Female	165	44.35%
Age	18-26	151	40.59%
	27-35	137	36.83%
	35-45	59	15.86%
	>46	25	6.72%
Education	High School and below	27	7.26%
	College	133	35.75%
	Bachelor	119	31.99%
	Master and above	93	25.00%
Occupation	Student	146	39.25%
	Corporate employees	143	38.44%
	Party and government organs and institutions staff	52	13.98%
	Others	31	8.33%

Data Analysis

Data analysis was conducted using a combination of statistical methods. SPSS 24.0 was employed for preliminary analysis, including descriptive statistics and correlation analyses. Confirmatory Factor Analysis (CFA) and SEM were performed using AMOS 24.0 to assess the measurement model's validity and test the hypothesized relationships. The bootstrapping method with 5,000 resamples was applied to test the significance of the mediating effects. To address potential common method bias, Harman's single-factor test was performed.

Measurements

The survey questionnaire primarily centers on the measurement scales utilized to assess indicators, including digital literacy, perceived threat, response efficacy, self-efficacy, and protection intention. Each scale uses a Likert scale format ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) for responses. (1) Digital Literacy: The digital literacy scale was constructed based on the European Union digital literacy framework, the United Nations Educational, Scientific, and Cultural Organization (UNESCO) global digital literacy framework, and the digital literacy scales developed by Ng (2012). It evaluates five key dimensions of digital literacy: digital knowledge, information evaluation ability, digital operational skills, digital security awareness, and digital ethics. (2) Perceived Threat: The perceived threat scale, adapted from Xu et al. (2012) and Verkijika (2018), includes three

items assessing users' perception of information security risks associated with smartphone use. (3) Response Efficacy: The response efficacy scale, adapted from Thompson (2017) and Jansen and van Schaik (2019), includes three items evaluating users' belief in the effectiveness of security measures. (4) Self-efficacy: The self-efficacy scale, adapted from Wissinger (2017) and Bélanger and Crossler (2019), includes four items assessing users' confidence in their ability to protect their information security. (5) Protection Intention: The protection intention scale, adapted from Dinev et al. (2009), includes four items measuring users' intention to take security measures for their smartphones. The specific item design of each latent variable is shown in Table 2:

Table 2. Measurement variable design

variable	Problems
Digital knowledge	I understand the basics of big data, artificial intelligence, the Internet of Things, and other digital technologies.
	I understand the basic characteristics, current status, and future trends of major digital technologies.
	I am familiar with digital tools, software devices, and digital resources commonly used in social life.
Information evaluation ability	I can recognize reliable and unreliable sources of information on the web.
	I know how to assess the accuracy and credibility of online information.
	I can find the information I need to solve problems on the web.
	I verify and validate the information I get from the internet.
Digital operation skills	I am familiar with how to install, update, and uninstall apps on smartphones.
	I am proficient in using a cell phone for daily work and life affairs.
	I can use various functions of my smartphone proficiently.
Digital security awareness	I understand the basic concepts and principles of cybersecurity.
	I understand the importance of securing personal data in an online environment.
	I know how to protect against malware and virus attacks.
Digital ethics	I respect the privacy and rights of others on the internet.
	I abide by the code of ethics of the internet and refrain from spreading inaccurate information and malicious remarks.
	I use legal and legitimate software and resources on the web.
Perceived threat	I think there is a security threat to the personal information stored on smartphones.
	I am concerned that using a smartphone in a public networked environment could lead to information leakage.
	I think smartphone apps may be stealing my data.
Response efficacy	My efforts to secure personal information on my smartphone are paying off.
	Utilizing digital security technology or tools can better secure my personal information on my smartphone.
	The adoption of security measures can effectively protect personal information.
Self-efficacy	Taking precautions to secure personal information on my smartphone is relatively easy.
	I can effectively utilize digital technologies and tools for smartphone information security.
	I can find ways to deal with the risk of personal information on my smartphone.
	I know how to distinguish and assess the security and risk of personal information on smartphones.
Protection intention	I will take security measures to prevent breaches on smartphones.
	I actively use digital technologies and tools to secure personal information on my smartphone.
	I am willing to use security software to keep my smartphone safe.
	I take the initiative to understand and learn about smartphone information security.

Results

The Test of CMV

Harman's single-factor test is a common method for assessing Common Method Variance (CMV), with the criterion that the first principal factor should explain less than 40% of the variance (Hu et al., 2021). In this study, the percentage is 32.93%, indicating that the data passes the test.

Reliability and Validity Analysis

In this study, Cronbach's Alpha coefficient (a) and composite reliability (CR) values were used for reliability testing. The results are shown in Table 3. If $a > 0.8$, it means that the scale has high intrinsic reliability. If $a > 0.7$, it means that the scale has good intrinsic reliability. It is generally required that the CR value of the variables should be greater than 0.7. The a value and CR value of the questionnaire scale in this paper are both greater than 0.8; therefore, the questionnaire demonstrates good reliability.

Table 3. Factor loadings, Cronbach's alpha (a), CR, and Average Variance Extracted (AVE)

Variables	codes	Factor loadings	a	CR	AVE
Digital knowledge	A1	0.817	0.822	0.825	0.612
	A2	0.712			
	A3	0.813			
Information evaluation ability	B1	0.731	0.829	0.829	0.548
	B2	0.740			
	B3	0.751			
	B4	0.738			
Digital operation skills	C1	0.749	0.813	0.813	0.592
	C2	0.799			
	C3	0.760			
Digital security awareness	D1	0.768	0.807	0.808	0.584
	D2	0.792			
	D3	0.732			
Digital ethics	E1	0.771	0.830	0.831	0.621
	E2	0.778			
	E3	0.815			
Self-efficacy	F1	0.695	0.801	0.809	0.516
	F2	0.668			
	F3	0.815			
	F4	0.685			
Perceived threat	G1	0.768	0.806	0.809	0.585
	G2	0.746			
	G3	0.780			
Response efficacy	H1	0.812	0.825	0.828	0.617
	H2	0.720			
	H3	0.820			
Protection intention	I1	0.808	0.800	0.805	0.510
	I2	0.670			
	I3	0.716			
	I4	0.652			

Validity is generally verified using convergent validity and discriminant validity. Convergent validity is tested by factor loadings and AVE, with factor loadings judged based on a threshold value of 0.6, and AVE values required to be greater than 0.5. As shown in Table 3, the factor loadings and AVE values in this study meet the requirements, indicating that the model has good convergent validity. Discriminant validity was assessed using the square root of the AVE and the correlation coefficients between the latent variables. As shown in Table 4, the diagonal elements represent the square root of AVE, and the off-diagonal correlation coefficients are all smaller than the corresponding diagonal values, indicating that the model has good discriminant validity.

Table 4. Results of discriminant validity analysis

	Digital ethics	Perceived threat	Response efficacy	Self-efficacy	Protection intention	Digital operation skills	Digital security awareness	Information evaluation ability	Digital knowledge
Digital ethics	0.788								
Perceived threat	0.515	0.765							
Response efficacy	0.48	0.398	0.785						
Self-efficacy	0.439	0.344	0.473	0.718					
Protection intention	0.44	0.417	0.484	0.532	0.714				
Digital operation skills	0.499	0.442	0.469	0.495	0.51	0.769			
Digital security awareness	0.515	0.505	0.333	0.422	0.453	0.519	0.764		
Information evaluation ability	0.536	0.595	0.412	0.399	0.436	0.685	0.647	0.740	
Digital knowledge	0.585	0.484	0.459	0.458	0.459	0.514	0.524	0.589	0.782

Confirmatory Factor Analysis of Digital Literacy

First-order Confirmatory factor analysis of digital literacy

We conducted a confirmatory factor analysis (CFA) of the five dimensions of digital literacy using AMOS software. The first-order CFA model is shown in Figure 2. The results showed that the factor loadings ranged from 0.71 to 0.82. The CR values of the latent variables were all greater than 0.6, and the AVE values were all above 0.5. Thus, the model demonstrated good internal consistency and convergent validity. The model fit indices of the first-order

CFA are presented in Table 5, indicating that the model has a good overall fit and the parameter estimates are robust.

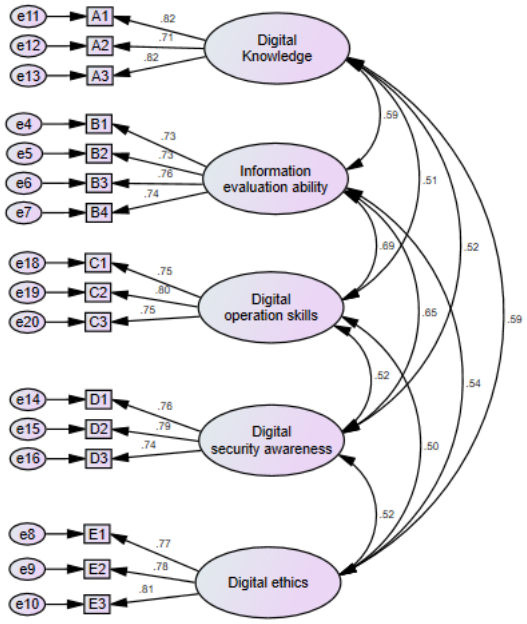

Figure 2. First-order confirmatory factor model diagram

Table 5. Fit indices of the first-order confirmatory factor model

Fitting Indicator	CMIN/DF	GFI	TLI	RMR	SRMR	IFI	CFI	PGFI
Adaptation Standard	<3.00	>0.90	>0.90	<0.05	<0.05	>0.90	>0.90	>0.50
Actual value	2.098	0.939	0.952	0.025	0.033	0.963	0.962	0.649
Fitting Judgment	Qualified	Qualified	Qualified	Qualified	Qualified	Qualified	Qualified	Qualified

Second-Order Confirmatory Factor Analysis of Digital Literacy

The high correlation coefficients among digital knowledge, information evaluation ability, digital operation skills, digital security awareness, and digital ethics indicate the existence of a higher-order latent construct. Therefore, a second-order factor model was constructed based on the first-order model, and a second-order confirmatory factor analysis was conducted. The path diagram is shown in Figure 3. The factor loadings representing the influence of digital literacy on its five dimensions are all greater than 0.6. Among them, users generally consider information evaluation ability the most important aspect of digital literacy, with a factor loading of 0.85. This is followed by digital operation skills (0.75), digital security awareness

(0.74), and digital knowledge (0.72). Digital ethics is considered the least influential factor, with a loading of 0.69.

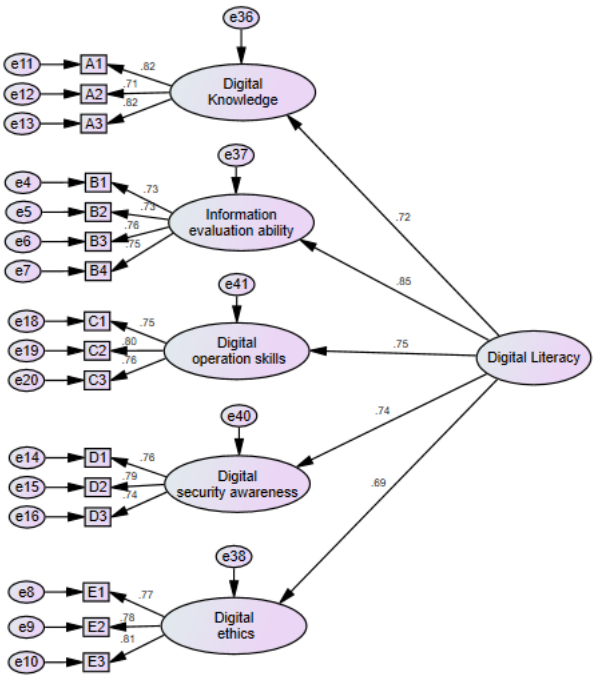

Figure 3. Second-order validation factor model diagram

The second-order validation factor loadings of the model ranged from 0.68 to 0.85, the CRs of the latent variables were all above 0.6, and the average AVE values were all greater than 0.5. Thus, the construct reliability and convergent validity of the model were considered acceptable. The overall model fit indices, as presented in Table 6, all met the recommended thresholds. Therefore, the second-order validation factor model is valid and reliable.

Table 6. Second-order validated factorial model fitting metrics

Fitting Indicator	CMIN/DF	GFI	TLI	RMR	SRMR	IFI	CFI	PGFI
Adaptation Standard	<3.00	>0.90	>0.90	<0.05	<0.05	>0.90	>0.90	>0.50
Actual value	2.129	0.935	0.950	0.029	0.039	0.959	0.959	0.681
Fitting Judgment	Qualified	Qualified	Qualified	Qualified	Qualified	Qualified	Qualified	Qualified

Model Validation

Based on the research hypotheses as the theoretical foundation, a structural equation model of the impact of digital literacy on smartphone users' intention to protect information security is constructed (as shown in Figure 4).

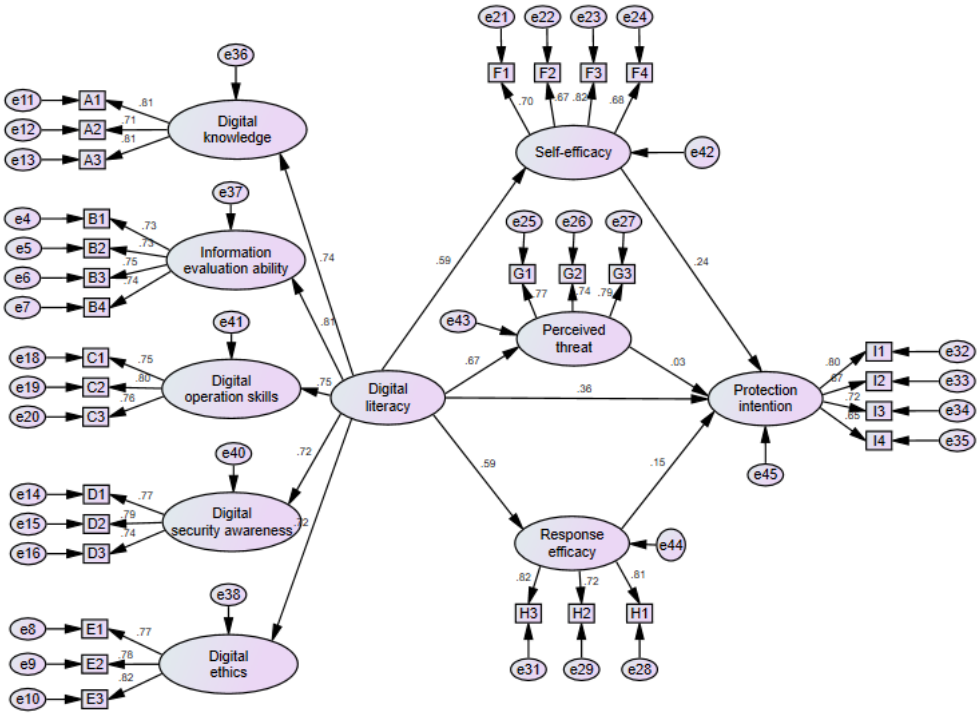

Figure 4. Structural equation model diagram

The overall fit of the model is shown in Table 7, and the overall fitness indexes all meet the criteria. Therefore, the hypothetical model proposed in this study and the actual data fit well, and the measurement model is valid.

Table 7. Overall model fitness metrics for model validation factor analysis

Fitting Indicator	CMIN/DF	GFI	TLI	RMR	SRMR	IFI	CFI	PGFI
Adaptation Standard	<3.00	>0.90	>0.90	<0.05	<0.05	>0.90	>0.90	>0.50
Actual value	1.601	0.903	0.948	0.037	0.048	0.953	0.953	0.763
Fitting Judgment	Qualified	Qualified	Qualified	Qualified	Qualified	Qualified	Qualified	Qualified

Research hypothesis testing

Direct Effects Test

Using structural equation modeling to test the direct effect relationships yielded the path coefficient analysis results, as shown in Table 8. The results indicate that digital literacy has a significant direct effect on response efficacy, perceived threat, and self-efficacy, suggesting that enhancing the digital literacy of smartphone users can improve their information security

response efficacy, perceived threat, and self-efficacy. Digital literacy, response efficacy, and self-efficacy also exhibit significant direct effects on users' intentions to protect information security. However, the direct effect of perceived threat on protection intention is not significant, indicating that the perception of information security threats on mobile smart devices does not influence users' protection intentions. Hypotheses H1a, H1b, H1c, H1d, H3, and H4 are supported, while H2 is not supported.

Table 8. Results of model path coefficient analysis

Paths			Estimate	S.E.	C.R.	P	Hypotheses
Digital literacy	--->	Response efficacy	0.590	0.101	8.353	***	supported
Digital literacy	--->	Perceived threat	0.669	0.094	8.844	***	supported
Digital literacy	--->	Self-efficacy	0.594	0.093	7.861	***	supported
Digital literacy	--->	Protection intention	0.361	0.16	3.133	**	supported
Response efficacy	--->	Protection intention	0.155	0.069	2.185	*	supported
Perceived threat	--->	Protection intention	0.028	0.091	0.349	0.727	rejected
Self-efficacy	--->	Protection intention	0.241	0.083	3.288	**	supported

Mediation Effect Test

Based on these results, the mediating effect of digital literacy on the intention to protect was further tested. The bootstrap method was used to test the significance of the mediating effects of response efficacy, perceived threat, and self-efficacy (Hayes, 2009).

As shown in Table 9, the direct effect, total indirect effect, and total effect of digital literacy on the intention to protect were all significantly positive. The direct effect of digital literacy on the intention to protect was 0.361, while the indirect effect was 0.253. Among the three specific indirect effects, the pathways digital literacy → self-efficacy → protection intention and digital literacy → response efficacy → protection intention reached a significant level, while the pathway digital literacy → perceived threat → protection intention did not reach a significance level. Self-efficacy and response efficacy were found to partially mediate the relationship between digital literacy and intention to protect, respectively, while perceived threat did not mediate this relationship.

Table 9. Direct, indirect, and total effects

Effects	Estimated value	SE	Bias-corrected 95% confidence interval	
			Lower	Upper
Direct effect	0.361	0.131	0.107	0.625
Indirect effects	0.253	0.098	0.071	0.456
Total effect	0.614	0.068	0.463	0.729
Specific indirect effects				
Digital literacy-Self efficacy-Protection intention	0.143	0.050	0.057	0.259
Digital literacy - Response efficacy - Protection intention	0.091	0.046	0.004	0.190
Digital literacy - Perceived threat - Protection intention	0.019	0.061	-0.099	0.143

Discussion

This study reveals that enhancing smartphone users' digital literacy plays a crucial role in strengthening their response efficacy and self-efficacy, which in turn significantly reinforces their intention to protect information security. These findings provide meaningful insights into cybersecurity-related user behavior and offer practical implications for policymakers, educators, and businesses aiming to foster a more secure mobile environment.

First, the findings underscore the foundational importance of digital literacy in the context of smartphone information security (Sirlin et al., 2021). Digital literacy encompasses more than just operational or technical skills; it includes the ability to locate, evaluate, and appropriately apply information, recognize digital risks, and engage in responsible and secure behaviors online. As users' digital literacy improves, they become more confident in their ability to manage cyber risks and more likely to prioritize protective behaviors (Göldağ, 2021; Pawlicka et al., 2022). Users with higher levels of digital literacy are better equipped to evaluate the feasibility of security actions, identify the necessary knowledge and tools to mitigate risks, and ultimately enhance their intention to protect personal data (Tinmaz et al., 2022; Audrin & Audrin, 2022).

Second, the study finds that improved digital literacy enhances users' response efficacy, their belief in the effectiveness of security measures in mitigating cyber threats (Fischer-Preßler et al., 2022). Response efficacy is a key component of Protection Motivation Theory and influences how individuals assess and respond to potential risks (Norman et al., 2015). Users who believe that certain protective behaviors, such as using complex passwords or regularly updating software, can significantly reduce risk are more likely to adopt those measures (Chen & Yuan, 2022). Digitally literate users are better able to recognize the value of these practices and more capable of implementing them effectively. Hence, greater digital literacy contributes to a stronger belief in the effectiveness of protective actions, which in turn promotes more consistent and deliberate information security behavior.

Third, while the study shows that digital literacy increases users' perception of cybersecurity threats, this heightened awareness does not significantly impact their behavioral intention to protect information security. This finding aligns with prior studies (Blythe & Coventry, 2018; Heidt et al., 2019), suggesting that awareness alone may not be sufficient to drive behavioral change. Although users with higher digital literacy can more readily identify threats such as phishing, malware, and identity theft (Pattinson et al., 2015; Park, 2013), this awareness does not always translate into action. Psychological inertia may cause users to continue with past behavior patterns despite knowledge of risks. Additionally, time constraints, cognitive load, and social influences may reduce users' ability or motivation to act upon their awareness (Albrechtsen & Hovden, 2010). Furthermore, users may exhibit optimism bias or avoidance tendencies, believing that serious information security incidents are unlikely to happen to them (Shepherd & Kay, 2012). These findings suggest that raising threat awareness should be paired with strategies that reduce psychological barriers and promote actionable behavior.

Fourth, the study confirms that digital literacy has a strong positive effect on self-efficacy, the belief in one's ability to effectively handle cybersecurity challenges (Taba et al., 2022). Self-efficacy is a critical determinant of behavior, particularly in complex and dynamic contexts such as cybersecurity (Coklar & Tatli, 2020). Users with high digital literacy tend to possess better problem-solving skills and a broader understanding of security tools and strategies. This technical competence enhances their confidence and increases the likelihood that they will engage in protective actions. In other words, digital literacy empowers users not only with knowledge but also with a sense of capability, which is essential for proactive information security behavior.

These findings offer several important implications for practice:

First, policymakers should recognize the foundational role of digital literacy in national cybersecurity strategies. Given that digital literacy directly influences users' security intentions through self-efficacy and response efficacy, educational and public policy initiatives should prioritize comprehensive digital literacy training. This includes not only basic technical skills, but also critical thinking abilities such as evaluating the credibility of online information and recognizing security threats. Governments can integrate digital literacy modules into school curricula, adult education programs, and community workshops, especially targeting vulnerable populations such as older adults and rural residents who may be at greater risk of information security breaches. Policymakers should also consider leveraging real-time behavioral data (Rouhani et al., 2018) and use it to design targeted interventions that address specific user needs and challenges in cybersecurity.

Second, businesses, especially those in the digital service and smartphone application industries, should embed user-centered cybersecurity features into their design processes.

While users with higher digital literacy are more likely to adopt security measures, their effectiveness can be enhanced through better system defaults, clearer interface cues, and proactive security alerts. Organizations can also provide interactive guidance and personalized feedback to encourage the development of self-efficacy and reinforce the perceived effectiveness of protective behaviors.

Third, cybersecurity awareness campaigns should move beyond threat-based messaging and instead focus on capability-building. As this study shows, perceived threats alone do not significantly influence users' protection intentions. Therefore, campaigns that overemphasize fear may not lead to actual behavioral change. Instead, messaging should empower users with actionable steps, highlight the benefits of security measures, and build confidence in their ability to execute protective behaviors effectively.

Fourth, smartphone manufacturers and mobile software developers should provide embedded digital literacy tools and privacy dashboards. Features such as real-time risk assessments, simplified security settings, and transparent data usage reports can reinforce users' security self-efficacy. By reducing the technical barriers to secure usage, digital environments can better accommodate users with varying levels of literacy, promoting inclusive information security engagement.

Finally, digital literacy programs should be adaptive and ongoing. As technologies evolve rapidly, static forms of training may soon become outdated. Stakeholders in education, technology, and policy must establish mechanisms for continuous learning and skill renewal. Collaborative efforts across public, private, and academic sectors can ensure that digital literacy development remains aligned with emerging security challenges and societal needs.

Conclusion

In the context of the digital economy's rapid advancement, the prevalent use of smartphones has introduced significant information security challenges. This study has explored the relationship between digital literacy and smartphone users' intention to protect information security, aiming to provide insights into enhancing personal information security in the digital age.

The research has constructed a theoretical model integrating protection motivation theory and digital literacy theory, and has proposed corresponding hypotheses. Through a survey of smartphone users and subsequent data analysis using structural equation modeling, several key findings have emerged. Firstly, digital literacy is found to have a direct positive impact on users' intention to protect information security. This suggests that as users' digital literacy improves, they are more likely to take proactive measures to safeguard their personal information. Secondly, digital literacy also indirectly influences users' protection intention

through self-efficacy and response efficacy. This implies that enhancing users' belief in their ability to effectively protect their information and their confidence in the effectiveness of protective measures can further strengthen their intention to act. However, despite digital literacy positively affecting users' perception of threats, this heightened awareness does not significantly influence their intention to protect information security, indicating that awareness alone may not be sufficient to drive behavioral change.

The findings of this study may have several implications. For policymakers, the results highlight the importance of incorporating comprehensive digital literacy training into educational and public policy initiatives. This training should not only cover basic technical skills but also critical thinking abilities, such as evaluating online information credibility and recognizing security threats. Businesses, particularly those in the digital service and smartphone application industries, should design user-centered cybersecurity features and provide interactive guidance and personalized feedback to encourage the development of self-efficacy and reinforce the perceived effectiveness of protective behaviors. Cybersecurity awareness campaigns should focus on capability-building rather than merely emphasizing threats, empowering users with actionable steps and building their confidence in executing protective behaviors. Smartphone manufacturers and mobile software developers are encouraged to provide embedded digital literacy tools and privacy dashboards to reduce the technical barriers to secure usage and promote inclusive information security engagement. Lastly, digital literacy programs should be adaptive and ongoing to keep pace with rapidly evolving technologies.

Overall, this study provides a new perspective for understanding personal information security protection behavior in the digital age and offers practical guidance for improving users' intention to protect information security. Future research could further explore the dynamic nature of digital literacy and its long-term impact on information security behavior, as well as investigate the effectiveness of different digital literacy interventions in enhancing users' protection intentions and actual behaviors.

Data Availability

The datasets used and analyzed during the current research are available from the corresponding author on reasonable request.

Conflict of interest

The author declared no potential conflicts of interest concerning the research, authorship, and/or publication of this article.

Funding

This study was supported by the Key Project of Scientific Research in Universities of Anhui Province: "Construction of a Digital-Intelligent Information Ecosystem for National Strategic Emerging Industry Clusters in Anhui: Driving Mechanism, Core Elements, and Operational Mechanism (Project Number: 2024AH052135).

References

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection: An intervention study. *Computers & Security*, *29*(4), 432–445.

Audrin, C., & Audrin, B. (2022). Key factors in digital literacy in learning and education: A systematic literature review using text mining. *Education and Information Technologies*, *27*(6), 7395–7419.

Barn, B. S., Barn, R., & Tan, J. (2014). Young people and smartphones: An empirical study on information security. In *Proceedings of the 47th Hawaii International Conference on System Sciences* (pp. 4504–4514). IEEE.

Bélanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34–49.

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.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261–1278.

Bulgurcu, B. (2010). Antecedents and outcomes of information privacy concerns in online social networking: A theoretical perspective. *Information Systems*, *2*(2), 153–163.

Califf, C. B., & Brooks, S. (2020). An empirical study of techno-stressors, literacy facilitation, burnout, and turnover intention as experienced by K-12 teachers. *Computers & Education*, *157*, Article 103971.

Chen, H., & Yuan, Y. (2022). The impact of ignorance and bias on information security protection motivation: A case of e-waste handling. *Internet Research*, *33*(6), 2244–2275.

China Consumers Association. (2018). *Investigation report on personal information leakage in apps*. https://www.cca.org.cn/Detail?catalogId=475803785949253&contentType=article&contentId=526001653121093

China Internet Network Information Center. (2022). *Statistical report on internet development in China* (50th ed.). https://www.cnnic.net.cn/NMediaFile/2023/0807/MAIN1691371428732J4U9HYW1ZL.pdf

Coklar, A. N., & Tatli, A. (2020). Evaluation of digital citizenship levels of teachers in the context of information literacy and internet and computer use self-efficacy. *Asian Journal of Contemporary Education*, *4*(2), 80–90.

Deye, S. U. N. N. Y. (2015). Promoting digital literacy among students and educators. In *National Conference of State Legislatures*. https://www.ncsl.org/Portals/1/Documents/educ/digLiteracy_final.pdf

Dickson, D. (2005). The case for a 'deficit model' of science communication. *SciDev.net, 27*, 1–6.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391–412.

Esmaeili, M. (2014). *Assessment of users' information security behavior in smartphone networks* (Master's thesis). Eastern Michigan University.

Fischer-Preßler, D., Bonaretti, D., & Fischbach, K. (2022). A protection-motivation perspective to explain intention to use and continue to use mobile warning systems. *Business & Information Systems Engineering, 64*(2), 167–182.

Göldağ, B. (2021). Investigation of the relationship between digital literacy levels and digital data security awareness levels of university students. *E-International Journal of Educational Research, 12*(3), 82–100.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2018). *Multivariate data analysis* (8th ed.). Cengage.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*(1), 2–16.

Hatlevik, O. E., Throndsen, I., Loi, M., & Gudmundsdottir, G. B. (2018). Students' ICT self-efficacy and computer and information literacy: Determinants and relationships. *Computers & Education, 118*, 107–119.

Hayes, A. F. (2009). Beyond Baron and Kenny: Statistical mediation analysis in the new millennium. *Communication Monographs, 76*(4), 408–420.

Heidt, M., Olt, C. M., & Buxmann, P. (2019). To (psychologically) own data is to protect data: How psychological ownership determines protective behavior in a work and private context.

Hu, Q., Lu, Y., Pan, Z., Gong, Y., & Yang, Z. (2021). Can AI artifacts influence human cognition? The effects of artificial autonomy in intelligent personal assistants. *International Journal of Information Management, 56*, Article 102250.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79.

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies, 123*, 40–55.

Julien, H. (2018). Digital literacy in theory and practice. In M. Khosrow-Pour (Ed.), *Encyclopedia of information science and technology* (4th ed., pp. 2243–2252). IGI Global.

Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*(2), 353–363.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445–454.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71–90.

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 1.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815–825.

Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education, 59*(3), 1065–1078.

Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2015). Protection motivation theory. In *Predicting and changing health behaviour: Research and practice with social cognition models* (3rd ed., pp. 70–106). Open University Press.

Ortiz, J., Chih, W. H., & Tsai, F. S. (2018). Information privacy, consumer alienation, and lurking behavior in social networking sites. *Computers in Human Behavior, 80*, 143–157.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security behavior: An Australian web-based study. In *Human aspects of information security, privacy, and trust: Third international conference, HAS 2015, held as part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings* (Vol. 3, pp. 231–241). Springer International Publishing.

Pawlicka, A., Tomaszewska, R., Krause, E., Jaroszewska-Choraś, D., Pawlicki, M., & Choraś, M. (2022). Has the pandemic made us more digitally literate? Innovative association rule mining study of the relationships between shifts in digital skills and cybersecurity awareness occurring whilst working remotely during the COVID-19 pandemic. *Journal of Ambient Intelligence and Humanized Computing*, 1–11.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social psychology: A source book* (pp. 153–176).

Rouhani, S., Zamenian, S., & Rotbie, S. (2018). A prototyping and evaluation of hospital dashboard through the end-user computing satisfaction model (EUCS). *Journal of Information Technology Management, 10*(3), 43–60.

Shepherd, S., & Kay, A. C. (2012). On the perpetuation of ignorance: System dependence, system justification, and the motivated avoidance of sociopolitical information. *Journal of Personality and Social Psychology, 102*(2), 264–280.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. In *New approaches for security, privacy and trust in complex environments: Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007), 14–16 May 2007, Sandton, South Africa* (Vol. 22, pp. 133–144). Springer US.

Sirlin, N., Epstein, Z., Arechar, A. A., & Rand, D. G. (2021). Digital literacy is associated with more discerning accuracy judgments but not sharing intentions. *Proceedings of the National Academy of Sciences*.

Smith, J., Hewitt, B., & Skrbiš, Z. (2015). Digital socialization: Young people's changing value orientations towards internet use between adolescence and early adulthood. *Information, Communication & Society, 18*(9), 1022–1038.

Taba, M., Allen, T. B., Caldwell, P. H., Skinner, S. R., Kang, M., McCaffery, K., & Scott, K. M. (2022). Adolescents' self-efficacy and digital health literacy: A cross-sectional mixed methods study. *BMC Public Health, 22*(1), 1223.

The Central Cyberspace Affairs Commission of China. (2021). *Action plan for improving national digital literacy and skills*. https://www.cac.gov.cn/2021-11/05/c_1637708867754305.htm

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376–391.

Tinmaz, H., Lee, Y. T., Fanea-Ivanovici, M., & Baber, H. (2022). A systematic review on digital literacy. *Smart Learning Environments, 9*(1), Article 1.

Tsai, H. S., Jiang, M., Alhabash, S., et al. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138–150.

Vedadi, A., & Warkentin, M. (2020). Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. *Journal of the Association for Information Systems, 21*(2), 428–459.

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security, 77*, 860–870.

Wan, Z., Wang, Y., & Haggerty, N. (2008). Why people benefit from e-learning differently: The effects of psychological processes on e-learning outcomes. *Information & Management, 45*(8), 513–521.

Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy, 11*(2), 378–389.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816.

Wynn, D., Williams, C., Karahanna, E., & Madupalli, R. (2013). Preventive adoption of information security behaviors. *Information Systems Journal*.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. In *Proceedings of the International Conference on Information Systems (ICIS), 2012, Orlando, USA*.

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People, 26*(4), 401–419.

Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education, 23*(4), 407–416.

Bibliographic information of this paper for citing:

Cao, Zhenxiang; Peng, Liqing; Chu, Yili & Ye, Fan (2025). The Impact of Smartphone Users' Digital Literacy on Information Security Protection Intentions. *Journal of Information Technology Management*, 17 (3), 148-172. https://doi.org/10.22059/jitm.2025.377234.3694