The Impact Of Digital Literacy On Personal Information Security: Evidence From Vietnam

Bao Trung Phan[1], Phuong Huyen Do[1], Da Quynh Le[1]
[1]International School, Vietnam National University, Hanoi, Vietnam

[*]Corresponding author: huyendp@vnuis.edu.vn

Abstract

Research purpose:
The study is carried out to show the relationship that exists between digital literacy and personal information security among Vietnamese internet users. It provides the dimensions of digital literacy influencing information control behavior differently.

Research motivation:
The motivation of this study arises out of the fact that with the rapid growth of digitalization in Vietnam, there has been a steep rise in data breaches over the past couple of years. Dealing with how digital literacy can be manipulated to ensure personal data security is very critical to improved cybersecurity in the region.

Research design, approach, and method:
In this quantitative study, a survey will be conducted among 183 Vietnamese Internet users. SPSS and SmartPLS were applied to analyze relationships between digital literacy and information security practices.

Main findings:
Higher digital literacy is linked to better personal information management. Technical skills and policy awareness are key factors that enhance online security behaviors.

Practical/ managerial implication:
Improving digital literacy through education can strengthen information security. Policymakers should focus on awareness programs and training to mitigate cybersecurity risks.

D. Nguyen Van et al. (eds.), *Proceedings of the International Conference on Emerging Challenges: Sustainable Strategies in the Data-driven Economy (ICECH 2024)*, Advances in Economics, Business and Management Research 320,
https://doi.org/10.2991/978-94-6463-694-9_32

Keywords: Digital literacy, Informaiton security, Online information risk, Online behavior

List of abbreviations

DL	Digital literacy
ICB	Information control behavior
ICT	Information and communication technologies
PET	Privacy-Enhancing Technology
IE	Internet experience
PMT	Protection Motivation Theory

PU	Policy understanding
SP	Surveillance practices
TF	Technical familiarity
TPB	Theory of Planned Behavior

1. INTRODUCTION

The digital age is a double-edged sword. According to Tomczyk and Eger, 2020, improved ICTs have revolutionized the way people connect, access information, and run businesses, but at the same time, they introduce new complexities and challenges. First of all, it is the case that the Internet advances in a globalizing environment, helping communications across borders and exchanges of data. Interconnectedness driven by economic growth and collaboration increased the attack surface for malicious actors. In case such vulnerability exists in the systems, it can be exploited from any part of the world by criminals and can, therefore, put the personal information of every individual at risk irrespective of geographical location (Pratomo et al., 2024).

Another problem is the changing landscape of threats. The breach of data and cyber attacks are increasing concerns that picture the fragility of information security (Halim et al., 2023, Le Coze and Antonsen, 2023). The various forms of attacks include social engineering, a scam that exploits the weaknesses of human beings to con users into giving out private information (Goel et al. 2017). Added to the complication by the increasing big data analytics. In this collection, storage, and analysis of huge amounts of personal data, there are again new concerns over privacy. In such scenarios, strong security measures and enhanced awareness among the users are advocated to counter the potential misuse of the data by ill-minded elements at large (Zhang, 2018).

Personal information security is the act of providing protection to personal information against access and probable misuse by a number of ways, including providing its confidentiality, integrity, and availability. It is grossly influenced by human behavior, that is to say, awareness and good security practice will help in avoiding risks such as identity theft and the newly created social engineering attacks.

Digital literacy thus influences personal information protection by ensuring that a person has appropriate knowledge, attitudes, and behaviors to navigate safely in the digital world. Indeed, several studies have pointed out that the really significant factors contributing to the breakdown of information security are due to the human factor—user behavior and awareness, for example. The Knowledge-Attitude-Behavior model of Parsons et al. (2017) assumes that the more knowledge users acquire about security practices, the more their attitude will improve, leading to safer behaviors. In addition, raising the level of cybersecurity awareness can lower some risks, specifically against certain types of threats like social engineering, which exploits the lack of digital literacy on the part of the users (Zwilling, 2022).

In Vietnam, the rapid digitization of the whole society has raised concerns over the security of personal information within these highly exposed sectors. The sectors include retail, manufacturing, education, and finance, where there is a surge in data breaches. While recent studies in this strand emphasize the crucial role of digital literacy in protecting personal information, how such literacy is translated into security practices remains an open question across a variety of cultural contexts (Stutzman et al., 2013; Vandoninck et al., 2013). First, few studies have been done on Vietnam; second, even the available ones are incomplete in not discussing how varying degrees of proficiency in digital literacy and demographic factors may influence online behavioral patterns related to personal information security.

This research will attempt to fill these lacunas by investigating the relationship between digital literacy and personal information security within the context of Vietnam. It identifies significant drivers behind users' behavior in terms of information control, such as technical proficiency, awareness of institutional surveillance, policy understanding, and internet experience. Digital literacy decomposed into core components is the way how a more profound insight into the role digital proficiency plays in affecting personal information control and privacy protection can be gained. It further ascertains demographic characteristics that may shape online security behaviors.

2. LITERATURE REVIEW

2.1. Digital literacy

Definitionally, the DL has come a long way since its very definition in the late century. From being defined as the ability to understand and use information on a computer, notably through the Internet, it evolved to cover a raft of skills deemed crucial in traversing the complex digital landscape characterizing the 21st century. Gilster laid the foundation in 1997 by defining DL in terms of the navigation of online content, which later scholars would expand into broader competencies.

By the time the 21st century really got underway, Bawden in 2001 redefined DL as more than an ability to read and comprehend information online, including such skills as information retrieval, evaluation, and management. This was further extended by Eshet with her model, whereby key skills identified were photo-visual literacy, reproduction literacy, branching literacy, information literacy, and socio-emotional literacy. These extensions stress the step up from mere technical competency to a more holistic and integrative concept of DL, which now encompasses cognitive and social skills for digital navigation.

Other scholars also dimension the multifaceted nature of DL, especially in the development of aspects pertaining to communication, expression, social participation, and personal information security. Afif et al (2023). defined DL as "the ability to access and use information effectively within a digital environment," adding that DL is about being able to "critically access, understand, evaluate, and use information within a digital space.". Göldağ (2021), however, separates DL from computer literacy, which he defines as a focus on information understanding rather than that on the technology itself.

It is also strongly upheld by present research that cognitive and social-emotional skills go hand in hand with technical proficiency in digital literacy. In this respect, the development of DL has become quite an essential task, as technology has invaded every sphere of life. This very prominent role is played by educational institutions in equipping people with those skills. According to Göldağ (2021), positive attitudes toward technology can further enhance the development of DL; conversely, negative perceptions set both back. More concretely, DL is a comprehensive concept that requires a mix of knowledge, skills, and attitudes for moving around in the digital world effectively and responsibly.

2.2. Personal information security

Personal information security has been growing as a significant area of concern in this digital information age, and is increasingly focused on human factors that contribute to security. Various studies have pointed out the role of human behavior in information security breaches. According to Parsons et al. (2017) naive and unintentional behaviors by computer users are the most frequent cause of information security recorded. Similarly, in an Internet user, awareness and knowledge have the most effect on overall information security. This realization therefore increases the need to understand and improve the human part of information security.

The Knowledge-Attitude-Behavior model gives a basic framework for studying the links between an individual's knowledge about information security policies and attitude towards those policies, and how behaviors emanate. Parsons et al. (2017) suggested that as the knowledge of the employees increases regarding safe information security practices, attitude towards security policies also increases which finally leads to improved security behaviours. Since this model claims individual, organizational and intervention factors may have strong effects on personal information security knowledge, attitude and behaviour, it is considered a comprehensive approach for improving personal information security.

Awareness and Motivation are two most crucial factors for enhancing personal information security. According to Zwilling, 2022, the behaviors influenced by low cyber security awareness, such as not heeding security alerts or the use of unsecured networks, have extensive effects on the security of information. On the other hand, high awareness is characterized by an understanding of cyber threats and being able to take precautionary measures. Furthermore, Parsons et al. (2017) commented that the employees would be motivated to adopt secure behaviors; management holds an important place in identifying and fostering what motivates their staff. Metalidou (2014), also commented that general awareness campaigns by themselves would not be enough, expecting that what is really needed is a much more user-involving approach to be able to influence user awareness and behavior effectively.

It can thus be said that in personal information security, social engineering attacks are a more complex landscape. They exploit human vulnerabilities by targeting people to extract sensitive information through habit, motive, and cognitive bias exploitation. This therefore calls for the human factors in information security to be addressed by organizations through comprehensive awareness programs, education, and training. Laybats and Tredinnick (2016) posit information security not to merely contain technical solutions but encompass much broader management of the confidentiality, integrity, and availability of information. In so doing, improving personal information security, therefore, will have an enhanced need to give out one's digital literacy.

2.3. Protection Motivation Theory and Theory of Planned Behavior

Protection Motivation Theory (PMT) postulates that for cognitive processes to translate into protective actions, beliefs of the severity of the threat, the vulnerability of individuals to it, and the feasibility and effectiveness of the proposed protective action must be sufficiently salient (Marikyan, D., & Papagiannidis, S. 2023). This theory has been widely applied in management information systems and mainly technological threats come through phishing, malware, and cyber-attacks, among others (Ifinedo 2012; Verkijika 2018). Examples of protectional behavior include compliance with information security policies, password strength, and backup of data (Crossler 2010; Chenoweth et al. 2009). Nevertheless, the importance of PMT constructs may vary according to the security application; for instance, self-efficacy will bear more influence on backup intention than perceived threat severity (Crossler, 2010; Tsai et al., 2016). This inconsistency could be due to the varied perceptions by different individuals of threats and their consequences in different contexts (Ifinedo, 2012; Marikyan et al., 2022). Hence, PMT represents another constructive conceptual framework to discuss what stimulates people to engage in protective behaviors toward technology-related threats.
Theory of Planned Behavior (TPB) views the intention to perform a behavior as the most important determinant of the actual performance of that behavior, but this already has three components: attitude, subjective norms, and perceived behavioral control (Ajzen I., 1991). As represented in the study of Farooq et al (2019) on students' intentions concerning the adoption of security measures, an attitude refers to general feelings or personal motivation towards conducting a certain behavior and hence usually functions as the most powerful predictor of the intention of the particular behavior (Farooq et al., 2019, Jansen, J. and Van Schaik, P., 2017). Subjective norms refer to the "perceived social pressure from significant others to perform a behavior." In a couple of studies, subjective norms had an insignificant relationship to behavioral intention. This is possibly because of indifference or unclear expectations from their peers who may be unaware of other's practices of personal information security. In contrast, perceived behavioral control, which is similar to self-efficacy, is markedly related to behavioral intention since those who perceive themselves as capable of performing a certain behavior are more likely to intend to do so (Farooq et al 2019).

2.4. Previous resesearch

Digital literacy was defined as the ability to act in relation to digital technology, including accessing, understanding, evaluating, and using information critically and responsibly in digital environments (Afif et al., 2023). Among the rest, digital literacy includes many different elements such as the ability to use digital tools and applications, evaluate information sources, protect personal information, develop safe online communication skills, and handle online risk situations (Luthfia et al., 2021, Hussein and Hussein, 2020).
A 2013 study conducted by Sofie Vandoninck and colleagues recorded that users with higher digital skills levels tend to take matters into their own hands when facing online problems, such as deleting messages and blocking senders in case of bullying. This proves that digital literacy is effective in guiding the user along a proactive line of action within the online environment, thus avoiding different associated risks.
User habits and behavior in the online environment directly influence the level of personal information security. Some kinds of behaviors can enhance the risk of cyber-attack or information theft, including: publishing sensitive personal information in social networks; online communication with strangers; opening links or files from unknown places; and weak passwords, or repeating them (Stutzman et al., 2013, Benzer and Karal, 2023).
On the contrary, safe practices within the cyber setting will minimize the risks of information leakage and thereby guarantee that personal information is kept confidential. Such practices include: Downloading anti-virus software and updating them regularly, using strong passwords that are changed periodically, thoroughly scanning links and attachments before opening them, and Limiting access Access to social networks with personal information should be limited to the least number possible.
We can deduce a close relationship between digital literacy and information security from the reports relating digital literacy to behavior in the cyber environment and behavior to information security (Benzer and Karal, 2023, Podhradsky et al., 2014). In most cases, users of higher digital literacy often exert safer behaviors over the online media (Vandoninck et al., 2013). They can identify any threats like malicious websites or emails with phishing contents (Elrayah and Jamil, 2023, Benzer and Karal, 2023). Moreover, with digital literacy, they are able to update their knowledge regarding cybersecurity, making appropriate choices for protecting one's personal information (Burns and Roberts, 2013, Park, 2013).
Although digital literacy is relevant to ensure information security, reality shows that many users still lack appropriate digital literacy to be secure while browsing the internet. Due to this fact, cyber-attacks, personal data theft, and spreading false information increases.
Previous studies also noted that digital literacy has played a relevant role in the protection of personal information on online platforms. This is in relation to what was established by Stutzman et al., 2012; Vandoninck et al., 2013. However, specific studies about how digital proficiency influences the security of personal information within the context of Vietnam have not been provided. Therefore, new research can also take advantage of this to explore

behavioral issues and understanding among internet users in Vietnam in the context of a dynamically developing network environment and amid growing threats to information security. Investigation into this subject may be of use in delivering useful insights relevant to tackling several emergent challenges that are being brought about by data privacy and cybersecurity concerns.

This present study gives a new direction by measuring the digital proficiency of the respondents by a culturally adapted assessment tool, which considers the local context and practices. Various studies identified positive and negative aspects of digital literacy in personal information security; however, utilization and implementation of the same effectively have yet to be achieved (Stutzman et al., 2012).

This research work will contribute to bridging these knowledge gaps and improve knowledge on the role of digital literacy in the protection of personal information in Vietnam. It will then try to put forward more effective strategies and measures that can raise the network safety of domestic internet users in light of their very particular needs and the trends in technology which shape the landscape." The contribution of this research is that it will provide an in-depth understanding of the relationship that exists between digital literacy and personal information security in the context of Vietnam. This may be used to inform further targeted interventions and policies with a view to enhancing the level of digital literacy and the protection of personal information online in Vietnam.

Figure 1: Concept model of the study:

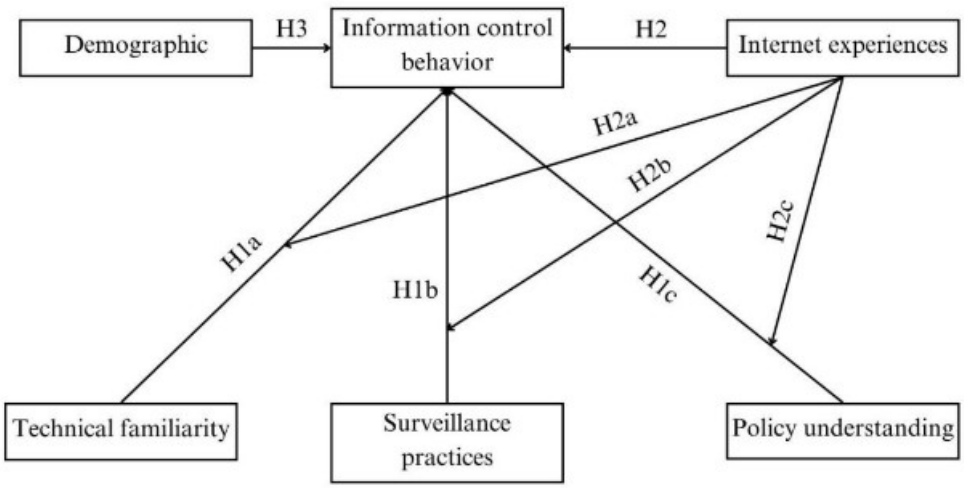

Table 1: Hypothesis:

Hypoheses		
H1a		Technical familiarity has a positive impact on Information control behavior
H1b		Awareness of institutional surveillance has a positive impact on Information control behavior.
H1c		Policy understanding has a positive impact on Information control behavior
H2		Internet experience has a positive impact on Information control behavior
	H2a	The interaction between technical familiarity and internet experiences impact positive on information control behavior
	H2b	the interaction between surveillance practice and internet experiences impact positive on information control behavior
	H2c	the interaction between policy understanding and internet experiences impact positive on information control behavior

H3 Individual demographic characteristics that affect Information control behavior.

3. METHODOLOGY

This was a quantitative study based on 219 responses to the online questionnaire, comprising 41 questions, administered via Google Forms. After the removal of consecutive replicate responses to questions (for example, the five questions about technical familiarity all being answered as "very familiar") and removals of unclear or improbable answers (for example, inability to recall the number of years of internet use), 183 valid responses were retained for analysis.

This described research methodology would stand on the shoulders of available literature to study how different dimensions of DL influence ICB. According to Saridakis et al. (2016), all security breaches emanate from a human cause; hence, there is a need to understand in depth the role of DL to influence ICB. Meanwhile, this study also adopts the model from Park 2013 to identify the effect of DL on the ability to safeguard and control financial information. Descriptive data with respect to the different dimensions related to the research problem was collected through the questionnaire: demographic data of the participants, digital literacy knowledge, experience with the Internet, and information control behavior. It thus covered such areas as:

- Demographic information: General data regarding age, sex, level of education, etc. have been collected to set a background for the analysis.
- Digital Literacy Knowledge: This was the independent variable. *Technical familiarity* of participants was measured with five items on a 6-point Likert scale, ranging from 1 = not at all familiar to 6 = very familiar. Moreover, eight true-false items measured *surveillance awareness*, and seven true-false items measured *policy understanding*. These were coded later, whereby correct answers had a score of 1 and wrong answers a score of 0.
- Information Control Behavior: This was the dependent variable and was further categorized into *social* and *technical dimensions*. All items regarding what the respondents reported doing about several information control behaviors were measured on a 6-point scale ranging from "never" to "very often."
- Internet experience: This was operationalized through two dimensions. These were the length of use of the internet in hours and years of experience. A single 6-point scale, 1 = one location and 6 = more than six locations, captured the variability of internet access locations used by the respondents.

The two major tools used in data analysis were SPSS and SmartPLS. SPSS helped in the presentation of descriptive statistics of demographic characteristics and distribution of responses with measures such as mean, median, mode, and standard deviation. SmartPLS aided in the calculation of the PLS SEM model and allowed the probing of causal interrelations among digital literacy, personal information security, and other factors, setting up the impact of digital literacy on personal information security in Vietnam.

4. RESULTS AND DISCUSSION

4.1. Data Analysis

The demographic profile of the respondents showed that the maximum, 75.96% of the sample, were below 22 years of age. The second most prominent age bracket was from 22 to 40 years. The third most prominent group included the people over 40 years, which formed the smallest proportion of the respondents at only 2.18%. Among the less than 22 years old respondents, most of the respondents were students. Of these, 89.62% had completed High school or equivalent, 5.46% had a Bachelor's degree or equivalent, and only a very small fraction of 4.92% had a Master's degree or higher. Considering the gender distribution of the participants, male responders were leading at a ratio of 62.84%, while female responders had 37.16% of the sample.

On average, participants reported 10.87 years of Internet experience, using an average of 9.43 hours online daily, visiting an average of 3.77 various sites online. Various types of Internet connections were reported, among which were cable, DSL, and 3G, 4G, and 5G.

The sample was predominantly young, consisting mainly of students, with a high percentage of males. Additionally, respondents had considerable experience with the Internet, accessing several sites via a variety of connection types. The reliability of the survey instrument shows there is reasonable consistency of response received from the sample population.

Table 2. Descriptive Statistics (N=183)

		Mean (%)	St. Dev
Age	Under 22 years	75.96	
	22 – 40 years	21.86	0.488
	Over 40 years	2.18	
Gender	Male	62.84	0.485
	Female	37.16	
Education	High school diploma or equivalent	89.62	
	Bachelor's degree or equivalent	5.46	
	Master's degree or higher	4.92	0.497
Internet experience	Number of Internet use: Years of Internet use	10.87	3.93
	Number of Internet use: Hours of daily Internet use	9.43	4.31
	Number of Internet access sites	3.77	1.60
	Type of Internet connection:		
	Cable	23.50%	
	DSL	7.10%	
	3G, 4G, and 5G	69.40%	

Sources: Author's synthetic.

The reliability of the survey instrument, assessed through Cronbach's Alpha coefficient of ICB, PU, SP, and TF, were found to be greater than 0.6 ($\alpha > .60$) , indicating a moderate level of internal consistency reliability. In the contrast IE had Cronbach's Alpha coefficient smaller than 0.6 (0.253 and 0.319, respectively)

Table 3. Cronbach's alpha

	Cronbach's alpha
IE	0.253
ICB	**0.858**
PU	**0.619**
SP	**0.684**
TF	**0.879**

Sources: Author's synthetic

Table 4.3 presents the limited comprehension of users in all three areas. Findings reveal that over 42.62% of users possess a basic or better level of understanding, with only 4 individuals (2.19%) demonstrating an excellent grasp. Users generally comprehend the collection and use of personal information online (M = 5.86, SD = 1.52), but approximately 29.85% misunderstood fundamental data governance activities aspects. Only one respondent (0.55%) answered policy-related questions accurately, achieving an average score of 4.82 (SD = 1.28). Additionally, most respondents demonstrated a moderate understanding of basic technical terms (M=20.33, SD=6.31). To clarify, Table

4.3.1 indicates that the understanding of basic technical aspects remains relatively low, with average scores ranging from 2.77 to 2.89, except for BCC understanding, which is moderately average at 3.43. On the other hand, the comprehension level of Surveillance practices is generally high to very high, with average scores ranging from 0.6 to 0.92. However, understanding of website policy and information management is slightly lacking, with an average score of 0.46 (SD=0.5). Legal knowledge across various aspects is generally high, with average scores ranging from 0.67 to 0.86, except for privacy and control, where it's notably lower. The Vietnamese government's online personal information policies are widely misunderstood, with an average score of 0.37 (SD=0.47).

Table 4. Descriptive Statistics of Main Variables Used in Analyses

	Mean	SD	Min	Max
Digital literacy:				
Technical familiarity	20.33	6.31	8	39
Surveillance practices	5.86	1.52	2	8
Policy understanding	4.82	1.28	1	7
Information control skill:				
Social dimension	19.46	5.87	7	38
Tech dimension	12.41	4.23	4	24

Sources: Author's synthetic.

Table 5. Descriptive Statistics of Digital literacy:

	Mean	SD
Technical familiarity		
Generic Internet		
HTML	2.77	1.08
Preference setting	2.77	1.20
ISP	2.85	1.17
Cache	2.89	1.16
BCC	3.43	1.37
Privacy risk		
Phishing	2.79	1.24
Privacy protection		
P3P	2.79	1.24
Surveillance practices:		
Companies today can place an online advertisement that targets you based on information collected on your web-browsing behavior	0.92	0.28
A company can tell you that you have opened an email even if you do not respond	0.60	0.49
When you go to a website, it can collect information about you even if you do not register	0.65	0.48

Popular search engine sites, such as Google, track the sites you come from and go to	0.79	0.41
E-commerce sites, such as Amazon or Netflix, may exchange your personal information with law enforcement and credit bureau	0.72	0.45
What a computer user clicks while online surfing can be recorded as a trail	0.90	0.31
Most online merchants monitor and record your browsing on their sites	0.85	0.37
When a website has a privacy policy, it means the site will not share your information with other websites or companies	0.46	0.50
Policy understanding:		
Government policy restricts how long websites can keep the information they gather about you	0.77	0.43
It is legal for an online store to charge different people different prices at the same time of day	0.67	0.47
A website is legally allowed to share information about you with affiliates without telling you the names of the affiliates	0.63	0.48
By law, e-commerce sites, such as Amazon, are required to give you the opportunity to see the information they gather about you	0.67	0.47
Privacy laws require website policies to have easy-to-understand rules and the same format	0.86	0.48
Vietnam government agencies can collect information about you online without your knowledge and consent	0.37	0.47
When I give personal information to an online banking site such as citibank.com, privacy laws say the site has no right to share that information, even with companies it owns	0.85	0.34

Sources: Author's synthetic.

The second part in Table 4.3 shows 2 dimension of information control. Overall, the sample respondents adopted one or more types of control strategies. On the technical side, the average score of 12.41 shows that most users rarely adopt or use technology through web browsers or privacy-enhancing technology (PET). In the social aspect, public participation is still quite low at M = 19.46 (SD =5.87). Specifically, according to table 4.3.2, it's evident that internet users demonstrate minimal engagement with actions such as erasing cookies, lodging complaints with agencies, requesting removal from marketing lists, refusing data sharing, and abstaining from purchases, as indicated by the low mean values ranging from 2.23 to 2.90 (SD ranging from 1.07 to 1.25). However, the behavior of utilizing secondary email addresses to safeguard personal information stands out as the most prevalent concern, with a mean value of 3.35 (SD = 1.50).

Table 6. Distribution of Individual Skill Measures.

	Mean	**SD**
Social dimension		
Stopped visiting particular websites because you fear they might deposit unwanted programs on your computers	3.25	1.23
Given false or inaccurate email addresses or fake names to websites because of privacy concerns	3.11	1.30

Decided not to make an online purchase because you were unsure of how information would be used	2.44	1.11
Chose not to register on a website because it asked you for personal information to get into the site	3.00	1.27
Complained to a consumer or government agency about marketing practices of particular websites	2.23	1.07
Asked a website to remove your name and address from any lists used for marketing purposes	2.43	1.25
Asked not to share your personal information with other companies	2.90	1.47
Use an email address that is not your main address, in order to avoid giving a website real information about yourself	3.35	1.50
Tech dimension		
Cleared your web browser history	3.31	1.29
Used filters to block or manage unwanted email	3.19	1.32
Erased some or all of the cookies on your computer	2.85	1.345
Used software that hides your computer's identity from websites you visit	3.06	1.403

Sources: Author's synthetic.

The result, as seen in table 4.4, is clear that out of all the constructs' relationships studied, only three of them were statistically positive in correlation since their p-value is less than .05, while the rest are not significant since $p > 0.05$ as shown by Hair et al. 2023. The t-values computed in hypotheses H1a, H1b, and H1c all ranged above 1.96 (> 1.96), indicating, according to Hair et al. (2023), that they are significant relationships. Based on these findings, the results increase incrementally the nuanced effect understanding of the factors of Technical Familiarity, Surveillance Awareness, and Policy Understanding on Information Control Behavior. The effect size ranged from 0.02 to less than 0.15, all statistically significant with p-values less than .05 and t-values greater than 1.96. The other way around, H2 and H3 are rejected. In support of this argument, a 2013 study by Park proved knowledge, as measured by technical familiarity, had a positive effect on both the social and technical aspects of information control. Internet experiences, which are indicated by the years of use and daily usage, supported information control, with male users displaying higher levels. On the other hand, however, education had no significant impact on information control.

Table 7. Summary of Hypotheses Testing

Hypotheses	Path	T statistics	P values	f-square	Decision
H1a	PU → ICB	**2.382**	**0.017**	**0.021**	**Supported**
H1b	SP → ICB	**4.027**	**0.000**	**0.069**	**Supported**
H1c	TF → ICB	**3.27**	**0.001**	**0.052**	**Supported**
H2	IE → ICB	0.727	0.467	0.005	Not Supported
H2a	IE x PU → ICB	0.013	0.990	0.000	Not Supported
H2b	IE x SP → ICB	0.79	0.430	0.009	Not Supported
H2c	IE x TF → ICB	0.141	0.888	0.000	Not Supported
H3	Age → ICB	1.91	0.056	0.023	Not Supported
	Education → ICB	0.095	0.924	0.000	Not Supported
	Gender → ICB	0.075	0.940	0.000	Not Supported

Sources: Author's synthetic.

4.2. Discussion

The more digital Vietnamese youth become, the more deficits in knowledge of personal information security there seem to be. This paper presents the levels of digital literacy related to personal information security in Vietnam's digital environment. The sample was demographically young, with a large proportion of its members below 22 years of age. This notwithstanding, the internet experience among the respondents in this study was strong, with substantial daily

online activity and extended exposure to the internet. This could be an indication that Vietnamese youth are introduced to the internet early, but the access may not be continuous.

The level of understanding of the issues of personal information security was relatively low among such highly exposed individuals. The technical knowledge did not correlate with the indicators of supervisory practices, policy understanding, and information control behavior. Still, the respondents demonstrated a relatively high level of awareness of the legal aspects of digital activities and supervision practices, thus some attention toward the legality of conducted actions in the digital environment.

The research also found mixed levels of knowledge on the security of personal information. While respondents manifested a good understanding of issues such as online data collection practices, there were gaps in core data governance activities, which would further make them vulnerable to online data theft. These findings underline the requirement for further awareness in these important subjects.

5. CONCLUSION

This present research result shows that digital literacy has a positive effect on personal information security, though not as highly significant as expected. The separate sub-elements of the elements of digital literacy-Technical Familiarity, Perception of Surveillance, and Policy Knowledge-have been proven to have a positive influence on information control behavior in prior research by Park (2013) and Nguyen (2024). Contrary to Park's findings, within the framework of this study, IE did not significantly impact personal information security. It means that although digital literacy is crucial, a longer exposition of the Internet doesn't necessarily lead to better information security behavior control.

The research analysis inferred that the vigilance of Vietnamese people has increased, especially in the post-COVID-19 period, partly due to the government’s efforts to send SMS messages to people’s phones to warn them about fraudulent activities. However, the research sample was biased towards students and those residing and working in Hanoi, an economically and socially developed area with abundant exposure to the internet and digital media. The sample was not representative of areas with aging populations and lower levels of digital literacy, thus failing to achieve the research objective of capturing a national perspective. In addition, the measure used from Park's 2013 study is not really suitable for the environment and context in Vietnam in 2024, which leads to three out of five main variables having Cronbach alpha less than 0.7 (of which 2 variables have Cronbach alpha greater than 0.6), so only three out of eight hypothesis is supported.

The COVID-19 pandemic accelerated the use of digital devices and the internet in daily life among Vietnamese people. The shift to such utilization has really enabled a wide range of online activities, ranging from remote work and online learning to digital shopping; it increases users' exposure to the digital environment where online frauds have become one of the most common and cunning white-collar crimes. From phishing emails, fraudulent messages to scam schemes on social media, users are up against an increasingly broad array of threats that require exceptionally strong skills and knowledge in personal information security.

Graver still, the Vietnamese government has stepped up monitoring and raised public awareness of the situation. The most prominent of them has been the issuance of SMS alerts as a sustained effort to inform citizens of the potential to be scammed and ways through which they can avoid becoming victims of such crimes. Such campaigns have demonstrated that public awareness of cybersecurity threats has risen; nonetheless, its efficacy needs to be underlined by an increase in digital literacy covering safe usage of technology and familiarity with the signs of fraud.

Therefore, by enhancing digital literacy, it inherently means that personal information will be better protected in Vietnam. Besides helping citizens understand ways of using the digital world securely, it equips them with such skills that they can detect and respond to online threats on time. Improved digital literacy may thus enable users to better protect their personal information and reduce the risk of falling victim to various, increasingly complex scams.

6. REFERENCES

AFIF, N. S., BASA, P. M. & ZAKHARIA, A. 2023. Analysis of digital literacy in the use of the internet in students. Jurnal Scientia, 12, 2714-2718.

AJZEN, I. (1991). The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes.

BAWDEN, D. 2001. Information and digital literacies: a review of concepts. Journal of documentation, 57, 218-259.

BENZER, A. İ. & KARAL, Y. 2023. Pre-Service Teachers’ Information Security Awareness: An Analysis Based on the Knowl edge—Attit ude—Behavi or Model. Educational Academic Research, 10-22.

BURNS, S. & ROBERTS, L. 2013. Applying the theory of planned behaviour to predicting online safety behaviour. Crime Prevention and Community Safety, 15, 48-64.

CHENOWETH, T., MINCH, R. & GATTIKER, T. (2009). Application of Protection Motivation Theory to Adoption of Protective Technologies.

CROSSLER, R.E. (2010). Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data.

ESHET, Y. 2004. Digital literacy: A conceptual framework for survival skills in the digital era. Journal of educational multimedia and hypermedia, 13, 93-106.

FAROOQ, A., JESKE, D., & ISOAHO, J. (2019). Predicting students' security behavior using information-motivation-behavioral skills model. In ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings 34 (pp. 238-252). Springer International Publishing.

FAROOQ, A., NDIEGE, J. R. A., & ISOAHO, J. (2019, SEPTEMBER). Factors affecting security behavior of kenyan students: an integration of protection motivation theory and theory of planned behavior. In 2019 IEEE AFRICON (pp. 1-8). IEEE.

GILSTER, P., & GLISTER, P. (1997). Digital literacy (p. 1). New York: Wiley Computer Pub.

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, 82-100.

HAIR, J. F., PAGE, M., BRUNSVELD, N., MERKLE, A., & CLETON, N. (2023). Essentials of Business Research Methods. Taylor & Francis.

HALIM, Z., DURYA, N. P. M. A., KRAUGUSTEELIANA, K., SUHERLAN, S. & ALFISYAHRIN, A. L. 2023. Ethics-Based Leadership in Managing Information Security and Data Privacy. Jurnal Minfo Polgan, 12, 1819-1828.

HUSSEIN, M. T. & HUSSEIN, R. M. 2020. Involving american schools in enhancing children's digital literacy and raising awareness of risks associated with internet usage. International Journal of Advanced Computer Science and Applications, 11.

IFINEDO, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers and Security, 31 (1), 83–95.

JANSEN, J., & VAN SCHAIK, P. (2017). Comparing three models to explain precautionary online behavioural intentions. Information & Computer Security, 25(2), 165-180.

LAYBATS, C. & TREDINNICK, L. 2016. Information security. SAGE Publications Sage UK: London, England.

LE COZE, J.-C. & ANTONSEN, S. 2023. Safety in the Digital Age: Sociotechnical Perspectives on Algorithms and Machine Learning, Springer Nature.

LUTHFIA, A., WIBOWO, D., WIDYAKUSUMASTUTI, M. A. & ANGELINE, M. 2021. The role of digital literacy on online opportunity and online risk in Indonesian youth. Asian Journal for Public Opinion Research, 9, 142-160.

MARIKYAN, D., & PAPAGIANNIDIS, S. (2023). Protection Motivation Theory: A review. In S. Papagiannidis (Ed.), TheoryHub Book: This handbook is based on the online theory resource: TheoryHub (pp. 78 93)

MARIKYAN, D., PAPAGIANNIDIS, S., RANA, O.F. & RANJAN, R. (2022). Blockchain adoption: A study of cognitive factors underpinning decision making. Computers in Human Behavior, 131, 107207.

METALIDOU, E., MARINAGI, C., TRIVELLAS, P., EBERHAGEN, N., SKOURLAS, C., & GIANNAKOPOULOS, G. 2014. The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424-428.

NGUYEN, T. T., TRAN, T. N. H., DO, T. H. M., DINH, T. K. L., NGUYEN, T. U. N., & DANG, T. M. K. (2024). Digital literacy, online security behaviors and E-payment intention. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(2), 100292.

PARK, Y. J. 2013. Digital literacy and privacy behavior online. Communication research, 40, 215-236.

PARSONS, K., CALIC, D., PATTINSON, M., BUTAVICIUS, M., MCCORMAC, A., & ZWAANS, T. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51.

PODHRADSKY, A. L., LEBLANC, L. J. & BARTOLACCI, M. R. 2014. Personal Denial of Service Attacks (PDOS) and Online Misbehavior: The Need for Cyber Ethics and Information Security Education on University Campuses. J. Cyber Secur. Mobil., 3, 339-356.

PRATOMO, A. B., SANTOSO, J., NUGROHO, A., FILDANSYAH, R. & VANDIKA, A. Y. 2024. Analysis of Data Privacy Policy, Data Processing Ethics, and Technology Ethics Awareness on User Privacy Protection in West Java. West Science Social and Humanities Studies, 2, 412-422.

VANDONINCK, S., D'HAENENS, L. & ROE, K. 2013. Online risks: Coping strategies of less resilient children and teenagers across Europe. Journal of children and media, 7, 60-78.

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

SARIDAKIS, G., BENSON, V., EZINGEARD, J. N., & TENNAKOON, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technological Forecasting and Social Change, 102, 320-330.

STUTZMAN, F. D., GROSS, R. & ACQUISTI, A. 2013. Silent listeners: The evolution of privacy and disclosure on Facebook. Journal of privacy and confidentiality, 4, 2.

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.

TSAI, H.S., JIANG, M., ALHABASH, S., LAROSE, R., RIFON, N.J. & COTTEN, S.R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. Computers & Security, 59, 138-150.

ZHANG, D. Big data security and privacy protection. 8th international conference on management and computer science (ICMCS 2018), 2018. Atlantis Press, 275-278.

ZWILLING, M., KLIEN, G., LESJAK, D., WIECHETEK, Ł., CETIN, F., & BASIM, H. N. 2022. Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97.