Int. j. adv. multidisc. res. stud. 2026; 6(4):1749-1760

Received: 10-07-2026
Accepted: 20-08-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Security Culture in the Digital Space

[1] Dr. Ha Vu Tuyen, [2] Nguyen Thi Van Anh, [3] Tran Thi Phuong Dong

[1, 2, 3] Vinh Phuc College of Engineering Technology, No. 55B Hung Vuong Street, Vinh Yen Ward, Phu Tho Province, Vietnam

DOI: https://doi.org/10.62225/2583049X.2026.6.4.7265

Corresponding Author: **Dr. Ha Vu Tuyen**

Abstract

By October 2025, Vietnam had 85.6 million Internet users, equivalent to 84.2% of its population. As the digital space becomes an everyday living environment, its safety depends not only on technical infrastructure and legislation but also on how individuals and organisations perceive, evaluate and respond to risk, that is, on security culture. This article clarifies the concept of security culture in the digital space, distinguishes it from the neighbouring notions of "cultural security" and "online codes of conduct", and proposes a four-layer analytical framework comprising awareness; values and norms; behaviour and skills; and institutions. Using a qualitative analysis of secondary sources for the period 2018-2026 (legal and policy documents, annual survey reports of the National Cybersecurity Association, DataReportal data and the ITU Global Cybersecurity Index), the study finds that Vietnam's institutional layer has developed rapidly and coherently, whereas the normative and behavioural layers have changed more slowly. In 2025, the share of users who fell victim to online fraud dropped from 0.45% to 0.18%, yet only 32.12% of victims reported the incident to the authorities, and 52.30% of surveyed organisations reported damage from cyberattacks. The pattern can be summarised as "institutions lead, habits lag". The article proposes five groups of measures: Replacing one-way awareness campaigns with habit formation; building community norms on reporting, data protection and information sharing; developing organisational security culture; embedding digital security education in training programmes, particularly in vocational education; and establishing periodic, standardised measurement of security culture.

Keywords: Security Culture, Digital Space, Cybersecurity, Online Fraud, Personal Data Protection, Vocational Education, Vietnam

1. Introduction

Over the past decade, the digital space in Vietnam has shifted from a supplementary information channel to the place where most everyday activities happen. People receive salaries, pay tuition fees and taxes, book medical appointments, buy and sell goods, look for jobs, complete administrative procedures and keep in touch with their families through digital platforms. Public agencies process administrative procedures online, manufacturers run connected production lines, and schools organise teaching and student management on networked systems. According to DataReportal (2026) [7], by October 2025 Vietnam had 85.6 million Internet users (84.2% of the population), 79.0 million active social media user identities and around 137 million cellular connections. At this scale, the digital space can no longer be treated as a "virtual world" separate from real life. Every risk that arises there leaves concrete consequences for people's assets, reputation, mental well-being and for social order.

Resolution No. 57-NQ/TW of 22 December 2024 of the Politburo on breakthroughs in science, technology, innovation and national digital transformation identifies safeguarding national sovereignty in cyberspace, cybersecurity, data security and the information safety of organisations and individuals as a cross-cutting requirement that cannot be separated from digital transformation. In line with this orientation, the legal framework has been completed at a rapid pace. The Law on Personal Data Protection (Law No. 91/2025/QH15) took effect on 1 January 2026, and the Law on Cybersecurity 2025 (Law No. 116/2025/QH15), which merges the Law on Cybersecurity 2018 and the Law on Network Information Security 2015, took effect on 1 July 2026. Internationally, Vietnam scored 99.74 out of 100 in the 2024 Global Cybersecurity Index (GCI) of the International Telecommunication Union (ITU), placing it among the 46 "role-modelling" countries in Tier 1.

The damage figures, however, tell a different story. The National Cybersecurity Association (NCA) estimated that online fraud

cost Vietnamese users about VND 18,900 billion in 2024, with roughly one victim for every 220 users (NCA, 2024) [20]. In 2025, information systems in the country faced around 552,000 cyberattacks, and more than half of the organisations surveyed reported having suffered damage (NCA, 2026a) [22]. Most of these incidents did not originate from sophisticated technical exploits but from ordinary actions: Clicking an unfamiliar link, installing an application on the instructions of a caller, reading out a one-time password to someone claiming to be a police officer, or reusing one password across many accounts. At the global level, the Verizon 2024 Data Breach Investigations Report found that about 68% of breaches involved a non-malicious human element, such as an error or a person falling for a social engineering attack (Verizon, 2024) [31].

The gap between a highly rated institutional foundation and persistently high losses raises a central question: What makes legal rules and technical advice turn into voluntary, everyday behaviour? International experience suggests that the answer lies in culture, more specifically in security culture, understood as the shared system of awareness, values, norms and habits that shapes how members of a community deal with risk. Even Vietnam's GCI 2024 profile hints at this. Four of the five pillars (legal, technical, organisational and cooperation) received full marks; the only pillar that fell short of the maximum was capacity development (19.74 out of 20), the pillar most directly concerned with people.

Domestic research on security in cyberspace has so far focused mainly on legal, technical, or ideological and cultural protection perspectives. The notion of "security culture in the digital space" as a whole, encompassing awareness, norms, behaviour and institutions, has not yet been clarified theoretically, nor has it been used as a framework to assess the current situation systematically. Addressing this gap, the article pursues three objectives: (i) to clarify the meaning, structure and characteristics of security culture in the digital space in the Vietnamese context; (ii) to provide an in-depth analysis of the state of digital security culture in Vietnam between 2018 and 2026, layer by layer, identifying achievements, shortcomings and their causes; and (iii) to propose groups of measures for building digital security culture, with particular attention to the role of vocational education institutions. The article does not estimate a quantitative model. It relies on the analysis, synthesis and cross-checking of secondary sources in order to provide an overall picture that can serve as a basis for subsequent empirical studies.

2. Literature review and theoretical framework

2.1 Review of related studies

The concept of "security culture" first emerged in the fields of nuclear safety and occupational safety and was transferred to information security in the early 2000s. The most influential approach builds on Schein's (2010) [28] three-level model of organisational culture, which distinguishes visible artefacts (structures, processes and observable behaviour), espoused values (strategies, goals and philosophies) and basic underlying assumptions (beliefs that are taken for granted, rarely voiced, yet decisive for behaviour). Van Niekerk and Von Solms (2010) [30] added a "knowledge" level to this model, arguing that in information security employees cannot hold the right assumptions or act correctly without a minimum understanding of risk. In their view, an information security culture cannot be created merely by issuing policies; policies become effective only when they are internalised as values and habits.

On this basis, Da Veiga and Eloff (2010) [4] developed a framework and assessment instrument for information security culture in organisations. Their framework covers leadership and governance, security policies, risk management, awareness and training, trust, privacy and technical controls, and it demonstrates that security culture can be measured and monitored over time. The European Union Agency for Network and Information Security (ENISA, 2017) [8] describes cybersecurity culture as the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity, as manifested in their behaviour with information technologies. ENISA stresses that culture-building programmes should be grounded in behavioural science, have measurable objectives and be re-evaluated after each cycle.

A second strand of research explains why awareness does not automatically translate into behaviour. Bada, Sasse and Nurse (2019) [2] show that many cybersecurity awareness campaigns in Europe fail because they merely provide information, ignore the cost of changing habits, lack concrete and easy-to-follow guidance, and sometimes rely on fear appeals that lead recipients to avoid the message rather than act on it. Hadlington (2017) [11] finds that risky online behaviour is associated with impulsivity and Internet addiction, implying that the heaviest users are not necessarily the safest. A systematic review by Uchendu *et al*. (2021) [29] identifies top management support, security policy, training and awareness, accountability and employee participation as the factors most frequently associated with a strong cybersecurity culture, while noting that most studies remain at the organisational level and that community-level and national-level studies are scarce.

A third strand draws on behavioural theories to explain why people do or do not follow security advice. Protection Motivation Theory (Rogers, 1975) [27] holds that people take protective action when they perceive a threat as serious and likely (threat appraisal) and believe that the recommended response is effective and within their ability (coping appraisal). Applied to security policy compliance, Herath and Rao (2009) [12] show that employees' intentions to comply depend not only on perceived threat severity but also on response efficacy, self-efficacy, perceived certainty of detection and the norms of colleagues and superiors. The Theory of Planned Behaviour (Ajzen, 1991) [1] similarly explains intention through attitudes, subjective norms and perceived behavioural control. Both theories suggest that awareness of threats is only one of several determinants; social norms and the perceived ease of the protective action are equally important. This insight is central to the argument of this article, because it implies that security culture cannot be built by information alone but requires changes in norms and in the environment in which choices are made.

A fourth, related strand comes from the literature on digital citizenship. Ribble (2015) [26] identifies digital safety and security, digital rights and responsibilities, and digital etiquette among the core elements of digital citizenship to be taught in schools. This perspective is useful because it places security within a broader set of civic competences and highlights the role of formal education in forming lasting habits from an early age.

In Vietnam, Le Quang Thanh and Nguyen Quoc Khanh

(2025) [14] systematise the theory and practice of applying cybersecurity law. More recent studies have begun to look at users. Nguyen Thi Thanh Huyen *et al*. (2026) [23] survey students' awareness of online fraud, while Vu Thi Minh Tam (2026) [33] assesses response mechanisms to deepfake-based disinformation on social media and notes that domestic research on the topic remains largely at the level of technical detection or isolated phenomena. There is also a substantial body of literature on "cultural and ideological security", which focuses on protecting ideological foundations and cultural values against hostile activities in cyberspace.

Overall, the international literature provides a fairly solid theoretical basis for security culture at the organisational level but remains thin at the community and national levels. In Vietnam, the phrase "security culture in the digital space" appears frequently in policy guidance and public communication but has not been structured into an analytical tool, and data on user behaviour are scattered across many sources. This article seeks to fill part of that gap.

2.2 The digital space and security in the digital space

The Law on Cybersecurity 2018 defines cyberspace as the network of information technology infrastructure, including telecommunications networks, the Internet, computer networks, information systems, information processing and control systems and databases, where people carry out social activities unconstrained by space and time. The term "digital space" is increasingly used in Party and State documents with a somewhat broader meaning: Beyond connectivity infrastructure, it encompasses data, digital platforms, digital services and the entire set of social relations established through them. In this article the two terms are used almost interchangeably, with "digital space" emphasising the dimension of a human living environment.

The Law on Cybersecurity 2025 standardises the concept of cybersecurity as the stability, security and safety of cyberspace, including the protection of information systems and the assurance that information, data and activities in cyberspace do not harm national security, social order and safety, or the lawful rights and interests of agencies, organisations and individuals. For the first time, "data security" is recognised as an independent legal concept (Article 2, Clause 3). Bringing cybersecurity and information safety under one unified concept signals that digital security concerns every user, from keeping one's own password safe to refraining from sharing other people's data.

Security in the digital space operates at three interlinked levels. At the individual level, it concerns the safety of a person's assets, data, identity, reputation and mental well-being. At the organisational level, it concerns the confidentiality, integrity and availability of information systems and data, as well as business continuity. At the national level, it concerns sovereignty in cyberspace, social order and safety, and society's trust in the digital environment. A compromised personal account can become an entry point into an organisation's system, while a data breach at an organisation supplies the "raw material" for fraud targeting millions of individuals.

2.3 Security culture in the digital space: Concept, structure and characteristics

Distinguishing related concepts: Before offering a definition, it is necessary to distinguish "security culture" from two concepts with which it is often conflated. "Cultural security" refers to the stable and healthy state of cultural and spiritual life and of social ideology, together with the activities that protect that state from harm; here, culture is the object being protected. In "security culture", by contrast, culture is the subject and the resource: It is what people believe, value and habitually do that enables them to protect themselves and their community. The two notions are related but not identical. A society may have firm ideological foundations while many of its members still readily read out their one-time passwords to fraudsters. The second concept to be distinguished is the "culture of conduct on social media", codified in the Code of Conduct on Social Networks issued with Decision No. 874/QĐ-BTTTT of 17 June 2021. This code mainly regulates relations between people (respect, courtesy, not insulting others, not spreading false information), while security culture regulates the relationship between people and risk. A culture of online conduct is part of security culture but does not cover it entirely.

Definition: Drawing on Schein (2010) [28], Van Niekerk and Von Solms (2010) [30] and ENISA (2017) [8], and situating the concept within Vietnam's legal context, this article proposes the following definition: *Security culture in the digital space is the system of awareness, values, norms, behavioural habits and institutions shared and sustained by a community (individuals, organisations and society) that guides how its members identify, assess, prevent and respond to security risks when participating in the digital space, while respecting the lawful rights and interests of others and the common interests of the nation.*

This definition emphasises the communal nature of security culture, which is "shared and sustained" rather than being the private expertise of specialists. It includes both a defensive dimension (protecting oneself) and a responsibility dimension (not harming others and not becoming a link in the spread of risk). It also combines mental elements (awareness, values) with materialised elements (behaviour, institutions), because culture truly exists only when it is expressed in action and supported by institutions.

Structure: Security culture in the digital space can be analysed in four layers (Table 1).

Table 1: The four-layer structure of security culture in the digital space

Layer	Content	Observable indicators
Awareness	Knowledge of risks, attack methods, legal rights and obligations, and the value of data	Ability to recognise scams, knowledge of the law, ability to distinguish true from false information
Values and norms	What the community regards as right and worth doing; tacit assumptions about risk, trust and responsibility	Attitudes towards reporting incidents, respect for privacy, verifying before sharing, boundaries for sharing personal information
Behaviour and skills	Everyday safe practices and the ability to carry them out	Password management, multi-factor authentication, software updates, verification before transferring money; victim rates, share of organisations suffering damage
Institutions	Laws, policies, organisational structures, education programmes, internal rules, platform responsibilities	Completeness of the legal framework, international indices (GCI), training programmes, reporting mechanisms

Source: Proposed by the authors based on Schein (2010) [28], Van Niekerk and Von Solms (2010) [30] and ENISA (2017) [8]

The four layers interact. Institutions send signals about what is permitted, what is sanctioned and who is responsible; awareness enables people to understand those signals; values and norms determine whether people want to act correctly when no one is watching; and behaviour is the ultimate, substantive measure of security culture. Following Schein's logic, the layer of values and norms, especially tacit assumptions, is the hardest to change but also the one that determines how durable behaviour will be. A regulation can be issued in a year; a community habit takes many years to form.

The four layers can also be read against the behavioural theories reviewed above. The awareness layer corresponds largely to threat appraisal in Protection Motivation Theory. The layer of values and norms corresponds to subjective norms in the Theory of Planned Behaviour, that is, people's perception of what others expect of them and what others actually do. The behaviour and skills layer reflects self-efficacy and perceived behavioural control. The institutional layer shapes all three by defining sanctions, assigning responsibilities and designing the choice environment. This correspondence gives the framework a theoretical basis and suggests where interventions are most likely to work: Where awareness is already high but behaviour lags, the bottleneck is more likely to lie in norms or in the perceived difficulty of acting safely than in a lack of information.

Characteristics: Compared with security culture in traditional domains, security culture in the digital space has several distinctive characteristics.

High interdependence. In the digital space, one person's carelessness can harm many others. A hijacked social media account is used to defraud the owner's entire friend list; a malware-infected computer becomes part of a botnet attacking other systems. Digital security therefore has the character of a public good, and the level of safety of a community is often determined by its weakest links.

Rapid change. Generative artificial intelligence allows fraudsters to fake voices, images and texts at very low cost, so warning signs taught one year may be useless the next. Digital security culture must therefore rest on stable principles of conduct, such as always verifying through an independent channel before transferring money or providing information, rather than on lists of specific "tips".

Two-way relationship between rights and responsibilities. The Law on Personal Data Protection 2025 grants data subjects numerous rights, including the right to be informed, to consent or withdraw consent, and to access, correct and request deletion of their data. These rights matter only if people know about and exercise them, and they come with the responsibility not to infringe on other people's data. Digital security culture is thus closely linked to legal culture and civic consciousness.

Cultural specificity. Every community has particular values that may serve as resources or turn into weaknesses. In Vietnam, the tradition of "the whole people protecting national security", the spirit of mutual support, and strong family and community ties are valuable resources for building digital security culture. Yet politeness, reluctance to cause trouble, and deference towards public authorities can also be exploited by fraudsters, as the analysis below shows.

2.4 Analytical framework

Based on the four-layer structure, the article analyses the state of digital security culture in Vietnam in the following order: (1) the context and scale of the digital space; (2) the institutional layer; (3) the awareness layer; (4) the layer of values and norms; (5) the layer of behaviour and skills, at both individual and organisational levels; and (6) a specific group, namely young people and students, including learners in vocational education institutions. For each layer, the article uses indicators observable in secondary sources and then synthesises them to assess the degree of alignment between layers. The central analytical assumption is that security culture is strong when the four layers develop in a relatively balanced way; when one layer develops far ahead of the others, a mismatch emerges that reduces the effectiveness of the system as a whole.

3. Methodology and data sources

The article employs a qualitative research design based on the analysis of secondary documents, combined with synthesis, comparison over time and cross-checking between sources. No quantitative model is estimated.

The sources fall into four groups. The first comprises Party documents and State legislation on cybersecurity, personal data protection, social media conduct and digital competence issued between 2015 and 2026. The second comprises the annual cybersecurity survey reports of the National Cybersecurity Association (NCA) for individual users (2024, with more than 59,000 respondents; 2025, with 60,300 respondents) and for organisations and enterprises (2025, with more than 5,300 entities), accessed through officially released summaries published in the press. The third comprises international data, including DataReportal's Digital 2024, Digital 2025 and Digital 2026 reports on Vietnam, the ITU Global Cybersecurity Index 2024 and the Verizon 2024 Data Breach Investigations Report. The fourth comprises domestic and international academic studies on information security culture, together with information

released by the Ministry of Public Security and cybersecurity firms.

Information from these sources was coded according to the four layers of the analytical framework, compared over time (mainly between 2024 and 2025), and then cross-checked across layers to assess their alignment.

Several data limitations should be acknowledged. The NCA surveys were conducted online with voluntary participation, so the samples are skewed towards users interested in cybersecurity and do not fully represent groups that use the Internet less. Estimates of fraud losses are produced with different methods (the NCA extrapolates from survey responses, while the Ministry of Public Security counts recorded cases), so they cannot be compared directly. Some press summaries also contain minor inconsistencies in how ratios are expressed. The figures are therefore used mainly to identify trends and orders of magnitude rather than to draw causal conclusions, and the origin and method of each figure are stated where necessary.

4. The state of security culture in Vietnam's digital space

4.1 Context: The digital space as a universal living environment

Table 2 summarises the main indicators used in the analysis.

Table 2: Selected indicators of the digital space and cybersecurity in Vietnam

Indicator	Value	Period	Source
Internet users	78.44 million (79.1% of population)	01/2024	DataReportal (2024) [5]
Internet users	85.6 million (84.2% of population)	10/2025	DataReportal (2026) [7]
Social media user identities	72.70 million (73.3%) → 79.0 million (77.6%)	01/2024 → 10/2025	DataReportal (2024, 2026) [5, 7]
Cellular connections	137 million (134% of population)	End of 2025	DataReportal (2026) [7]
Global Cybersecurity Index (GCI) score	99.74/100; capacity development pillar 19.74/20	2024	ITU (2024) [13]
Share of users who were online fraud victims	0.45% → 0.18%	2024 → 2025	NCA (2024, 2025) [20, 21]
Online fraud losses	About VND 18,900 billion (survey-based estimate)	2024	NCA (2024) [20]
Online fraud losses	Over VND 6,000 billion (recorded cases)	Jan-Nov 2025	Ministry of Public Security
Share of victims reporting to authorities	32.12%	2025	NCA (2025) [21]
Cyberattacks on information systems	About 552,000 (down 19.38%)	2025	NCA (2026a) [22]
Share of organisations damaged by cyberattacks	52.30%	2025	NCA (2026a) [22]
Compromised accounts	4.5 million (12.6% of global total)	H1 2025	VNPT Cyber Immunity (2025) [32]

Source: Compiled by the authors. Note: NCA and Ministry of Public Security loss figures use different methods and are not directly comparable

In less than two years, the number of Internet users rose from 78.44 million to 85.6 million. The number of cellular connections exceeds the population (134%), which reflects a high degree of digitalisation but also once facilitated the use of anonymous "junk" SIM cards for fraud before subscriber information was standardised. When almost the entire adult population is online, society's "attack surface" coincides with the population itself. The newest participants, such as older people, residents of rural and mountainous areas and young children, usually have the least experience and the weakest skills, so security culture cannot be built only for "proficient" urban users.

For the new Phu Tho Province, formed on 1 July 2025 by merging the former provinces of Phu Tho, Vinh Phuc and Hoa Binh, this context is particularly salient. The province combines concentrated industrial parks and a large young workforce with extensive mountainous areas inhabited by many ethnic minority communities. Differences in access conditions and digital skills between population groups must therefore be taken into account when building digital security culture at the local level.

4.2 The institutional layer: Rapid, coherent development and a shift towards people

Between 2018 and 2026, the institutional layer underwent the most significant change. Table 3 summarises the main documents.

Table 3: Main documents shaping the institutional layer of digital security culture

Year	Document	Relevance to security culture
2018	Law on Cybersecurity No. 24/2018/QH14	Legal framework for protecting national security and social order in cyberspace
2020	Decision No. 1907/QĐ-TTg	Scheme on raising awareness and popularising information security skills, 2021-2025
2021	Decision No. 874/QĐ-BTTTT	Code of Conduct on Social Networks
2024	Decree No. 147/2024/NĐ-CP	Management of Internet services and online information; verification of social media accounts
2024	Resolution No. 57-NQ/TW	Cybersecurity and data security as a cross-cutting requirement of digital transformation
2025	Circular No. 02/2025/TT-BGDĐT	Digital Competence Framework for Learners, including a safety domain
2025	Law on Personal Data Protection No. 91/2025/QH15 (effective 1/1/2026)	Rights of data subjects; ban on buying and selling personal data
2025	Law on Cybersecurity No. 116/2025/QH15 (effective 1/7/2026)	Merges the 2018 Cybersecurity Law and 2015 Network Information Security Law; codifies data security; bans the misuse of AI and deepfakes for impersonation; protects children online
2026	Decision No. 468/QĐ-TTg	Programme on protecting and supporting children online, 2026-2030
2026	Decree No. 330/2026/NĐ-CP (effective 19/8/2026)	Administrative sanctions in cybersecurity and personal data protection

Source: Compiled by the authors

The most visible trend is the expansion of coverage. Provisions on cybersecurity and information safety used to be spread across two separate laws, sometimes with overlapping implementation. By 2025, Vietnam had a unified law (the Law on Cybersecurity 2025, with 8 chapters and 45 articles), a dedicated law on personal data protection (5 chapters, 39 articles) and a decree on administrative sanctions in the fields of cybersecurity and personal data protection (Decree No. 330/2026/NĐ-CP, effective from 19 August 2026). New issues such as the misuse of artificial intelligence and deepfakes to impersonate a person's image or voice, and the protection of children in cyberspace, have been written into law. The Law on Cybersecurity 2025 also sets deadlines for social media platforms to remove violating content in emergency situations, clarifying the responsibilities of service providers.

This expansion has been accompanied by a shift in emphasis from "managing systems" to "protecting people". The Law on Cybersecurity 2025 was introduced with the motto of putting people at the centre, taking security as the foundation and sustainable development as the goal. The Law on Personal Data Protection prohibits the buying and selling of personal data (except where otherwise provided by law) and bars social networks from requiring users to submit images or videos of identity documents for authentication. Soon after the Law on Cybersecurity 2025 was passed, the Prime Minister approved the Programme on "Protecting and supporting children to develop safely in the online environment for 2026-2030" (Decision No. 468/QĐ-TTg of 23 March 2026). These are important institutional signals: They tell citizens that their data and safety have value and are protected by law.

Alongside binding legislation, "softer" people-oriented instruments have also appeared: The Code of Conduct on Social Networks (2021), the Scheme on raising awareness and popularising information security skills for 2021-2025 (Decision No. 1907/QĐ-TTg), and the Digital Competence Framework for Learners (Circular No. 02/2025/TT-BGDĐT), in which safety is one of the competence domains. These instruments act directly on the awareness and skills layers.

The results of these efforts have been recognised internationally. In the GCI 2024, Vietnam scored 99.74 and joined the 46 Tier 1 "role-modelling" countries, alongside many developed economies. Four of the five pillars received full marks. In the fourth GCI (2020), Vietnam ranked 25th out of 182 countries, so its position has improved markedly within a few years.

Nevertheless, the GCI measures national commitment (laws, dedicated agencies, strategies and programmes), not citizens' behaviour. A high GCI score shows that the institutional "hardware" is largely in place but does not prove that the cultural "software" has caught up, and the pillar closest to people is precisely the only one that did not reach the maximum score. Moreover, several key documents only took effect in 2026, while the path from legal effect to general public understanding and then to habit usually takes years. The density of new regulations also challenges legal dissemination: Citizens and even grassroots officials find it hard to keep up, and rules that are not understood are unlikely to become voluntary norms.

Implementation at the local level deserves particular attention. Since 1 July 2025, Vietnam has operated a two-tier local government system, with the district level abolished and communes and wards taking on many additional tasks. Commune-level authorities and police are now the closest point of contact between the State and citizens on matters of digital security, from receiving reports of fraud to disseminating warnings. Their capacity, however, varies considerably between urban wards and remote mountainous communes. Whether the new legal framework reaches ordinary users therefore depends heavily on the resources, skills and working methods of these grassroots actors. A law that is well designed at the central level may remain largely unknown in a village where no one has been trained to explain it.

In addition, the institutional layer still leans towards prohibition and sanction. Rules state clearly what is forbidden and what penalties apply, but provide fewer positive mechanisms that make safe behaviour easier, such as standardised safe-by-default settings for platforms, simple reporting channels, or recognition for communities and organisations that perform well. In the terms of Protection Motivation Theory, institutions have done much to raise perceived threat severity and the certainty of sanctions but less to strengthen people's coping appraisal, their belief that protective action is effective and within their reach.

4.3 The awareness layer: Clearly improved but uneven and not yet durable

There are several signs that public awareness of risks in the digital space has improved in recent years.

The clearest sign is the decline in the share of online fraud victims. According to NCA surveys, in 2024 about one in every 220 users was a victim (0.45%); in 2025 the rate fell to 0.18%, the first decline after several years of continuous increase (NCA, 2024, 2025) [20, 21]. Although the survey limitations call for caution, a fall of more than half is substantial. Several factors contributed, including technical and regulatory measures such as biometric authentication for online money transfers from mid-2024, the standardisation of mobile subscriber information and account verification for social networks under Decree No. 147/2024/NĐ-CP. Even so, the role of widespread public communication cannot be dismissed.

Awareness-raising channels have also diversified. In addition to traditional communication through the political system, the press and community loudspeakers, there are now the NCA's "Anti-online fraud" campaigns run with social media platforms, the "Real or Fake, Verified" programme produced by Vietnam Television together with the Department of Cybersecurity and High-Tech Crime Prevention (Ministry of Public Security), and seminars on fake news and deepfakes held at universities. Such partnerships help messages reach young users who rarely follow official channels.

However, awareness has not yet been fully converted into behaviour. The NCA's 2024 survey found that 31.36% of users admitted to having downloaded software from links sent via email, text messages or social media, a behaviour that has been warned against repeatedly for years (NCA, 2024) [20]. This is consistent with the observation of Bada *et al*. (2019) [2] that knowing a behaviour is dangerous is not enough for people to abandon it, especially when the behaviour is convenient and habitual.

Current awareness is also more "event-driven" than systematic. Users are warned about specific scams, such as fake delivery workers, fake electricity company staff or

recruitment for "easy work, high pay" collaborator jobs. This approach is useful in the short term but is easily overtaken when fraudsters change their scripts. Forecasts for 2026 all emphasise that fraud will become more sophisticated thanks to artificial intelligence and deepfakes, so that cues such as mismatched lip movements or unnatural lighting in videos are increasingly hard to detect. Durable awareness requires a shift from "knowing tips" to "holding principles": No State agency asks citizens to transfer money or read out authentication codes over the phone, and every unusual request involving money must be verified through an independent channel.

Awareness also varies between population groups. The sources used do not provide group-specific data, but the way fraudsters choose their scripts reflects these differences. Older people are targeted with scenarios impersonating authorities or relatives in emergencies; young workers and students are targeted with fake recruitment, investment schemes and paid "online tasks"; and residents of rural and mountainous areas have more difficulty accessing written warnings. Awareness programmes therefore need to be tailored to each group.

4.4 The layer of values and norms: Emerging, with significant gaps

The layer of values and norms is difficult to observe directly, but it can be inferred from certain collective behavioural patterns. The article focuses on three: Norms of reporting, norms concerning personal data, and norms of information sharing.

Weak reporting norms: According to the NCA's 2025 survey, only 32.12% of online fraud victims said they had reported the incident to the authorities, and about 12.03% accepted the loss and took no further action (NCA, 2025) [21]. In other words, roughly two thirds of incidents never reach the competent authorities. The consequences go beyond victims' difficulty in recovering their assets: The authorities lack the data needed to investigate, take action and warn the community early. Behind these figures lie widely shared cultural assumptions, such as reluctance to deal with procedures, shame at "having been fooled", and the belief that small losses are not worth reporting or that reporting will not bring the money back. In a strong security culture, reporting an incident is regarded as responsible behaviour towards the community rather than an admission of personal failure. In Vietnam, that norm is still taking shape.

Personal data are not yet valued accordingly: The NCA's 2024 survey shows that users attributed leaks of their personal data to providing information when shopping online (73.99%), to the use of services (67.00%) and to sharing information on social media (62.13%) (NCA, 2024) [20]. The first two causes fall under the responsibility of the organisations that collect and process data, but the third directly reflects user habits: Posting photos of identity documents, boarding passes, vehicle number plates and children's school details, or sharing real-time locations. In many communities, sharing achievements and family stories online is a normal social practice; in the absence of norms on privacy boundaries, this very practice becomes a data source for fraudsters. Norms concerning data relate not only to one's own data but also to the data of others. "Exposing" people online by publishing their personal information, or collecting and trading lists of customers, students and parents, still occurs. Statistics from the Department of Cybersecurity and High-Tech Crime Prevention show that in the first half of 2025 alone, the authorities detected and handled 56 cases involving the illegal sale of personal data. The ban on trading personal data in the 2025 law is an important step, but for it to take root, society needs to come to regard personal data as an asset and privacy as a value deserving respect.

Sharing norms favour speed: Social media encourages immediate sharing and immediate commenting, so verifying before sharing is often seen as slow. University seminars on fake news have observed that the pressure to share quickly and a lack of experience lead many students to become unwitting links in the spread of misleading information. Cases in which individuals have been fined for posting false information to attract views show that the boundary between freedom of expression and civic responsibility online is not yet clearly understood. The Code of Conduct on Social Networks sets out general principles but lacks concrete norms for common situations, particularly for content generated by artificial intelligence.

A cultural paradox: Good values are exploited: The NCA's 2025 survey found that the most common type of fraud was impersonation of the police or other authorities, followed by fake prize or gift notifications and investment scams promising high returns (NCA, 2025) [21]. The rise of impersonation of public authorities to first place deserves reflection from a cultural perspective. Fraudsters are not exploiting technical vulnerabilities; they are exploiting citizens' respect for, trust in and apprehension towards law enforcement. People fear being "involved in a case" and worry about their family's reputation, so they comply without daring to ask questions. In a similar way, family affection is exploited in scenarios such as "your relative has been taken to the emergency room" or "your child has had an accident at school". This suggests that building security culture does not mean making people less trusting. It means helping them place their trust correctly: Trusting institutions while verifying through official channels, and caring for relatives while calling them back directly before transferring money. Verified trust, rather than suspicion of everything, is the core value to be cultivated.

Norms within families and workplaces: Norms are formed not only at the level of society as a whole but also in small groups where people spend most of their time. In many families, digital safety is rarely discussed; older members are reluctant to ask younger ones for help, and younger members assume their parents "know enough". In many workplaces, sharing a colleague's login to "get the job done" is seen as cooperative rather than risky, and pointing out a colleague's unsafe practice may be perceived as impolite. These micro-norms matter because, as the Theory of Planned Behaviour suggests, people are strongly influenced by what those around them consider normal. A national campaign that conflicts with the everyday norms of a family or a work team is unlikely to change behaviour. Conversely, when a family agrees on a simple rule, such as "always call back before transferring money", or a work team treats reporting a suspicious email as a normal routine, safe behaviour becomes self-reinforcing.

4.5 The layer of behaviour and skills: Large losses, with the human factor as the weak link

At the individual level: Although the victim rate has fallen,

losses remain large. The NCA estimated fraud losses of about VND 18,900 billion in 2024 (NCA, 2024) [20]. According to the Ministry of Public Security, losses from online fraud in the first eleven months of 2025 still exceeded VND 6,000 billion. As explained in the methodology section, the two figures are calculated differently (extrapolation from a survey versus recorded cases), so one cannot conclude that losses fell threefold. What can be said with confidence is that losses still amount to thousands of billions of dong per year, mostly arising from users themselves transferring money or disclosing information under the manipulation of fraudsters.

Most common scams rely on social engineering rather than technical intrusion. Fraudsters create a sense of urgency, fear ("your account is linked to a money-laundering ring") or opportunity ("only a few places left"), and then push the victim to act immediately without time to consult anyone. Protecting oneself does not require advanced technical skills, only the habit of pausing, checking and verifying through an independent channel. The fact that this habit is not yet widespread shows that basic self-protection skills remain a weak link.

The same applies to account and password management. Data from VNPT Cyber Immunity show that in the first half of 2025 Vietnam recorded about 155 million leaked data records and 4.5 million compromised accounts, accounting for 12.6% of the global total; in 2024, about 14.5 million accounts were leaked, or 12% of the global total. Since Vietnam accounts for only about 1.2% of the world's population, its share of compromised accounts is many times its share of population. When a leaked password is reused across services, an incident in one place can lead to the loss of control over many other accounts.

At the organisational level: The NCA's 2025 report on organisations and enterprises shows that information systems in Vietnam faced about 552,000 cyberattacks, a decrease of 19.38% compared with 2024; nevertheless, 52.30% of surveyed organisations reported damage from cyberattacks (NCA, 2026a) [22]. The number of attacks fell, but risk did not decline accordingly, because attacks are becoming more targeted. While ransomware was the dominant threat in 2024, the most damaging incidents in 2025 involved intrusion and data theft. The suspected intrusion and theft of personal data at the National Credit Information Centre (CIC) in September 2025 shows that even organisations holding the most sensitive data are not immune.

Notably, according to VNPT, more than 70% of attacks on organisational systems were carried out through the use of system accounts. In most cases, attackers did not "break down the door" but "used the key", that is, valid accounts stolen from or tricked out of employees. This is clear evidence that employees' security culture, from choosing strong passwords and enabling multi-factor authentication to not sharing accounts and staying alert to phishing emails, is decisive for organisational security. An organisation that invests heavily in firewalls but allows staff to share simple passwords remains highly vulnerable.

In many organisations, cybersecurity is still regarded as the sole responsibility of the IT department. Leaders rarely take part in training or drills; regulations are issued but seldom checked; and employees are not encouraged to report anomalies. Yet visible support and role modelling by senior management is the factor most frequently cited in research on cybersecurity culture (Uchendu *et al*., 2021) [29]. Without it, training programmes tend to become a formality.

Small and medium-sized enterprises (SMEs), which make up the vast majority of Vietnamese businesses, face particular difficulties. Most lack a dedicated security officer, have limited budgets and rely on staff who handle IT tasks alongside other duties. For them, the shift of attackers from ransomware towards data theft is especially worrying, because data theft is often detected late, if at all, and its consequences fall on customers whose data are later used for fraud. The entry into force of the Law on Personal Data Protection raises the stakes further, since enterprises are now legally responsible for protecting the personal data they collect. For SMEs, building security culture is less about sophisticated technology than about a few disciplined practices adopted by everyone: Multi-factor authentication, separate accounts for each employee, regular backups and a habit of asking before clicking.

4.6 Young people, students and vocational learners

Young people are the heaviest and most technically proficient users of the digital space, but that does not make them the safest. International research shows that confidence in technical skills can be accompanied by complacency about risk (Hadlington, 2017) [11]. In Vietnam, studies of students' awareness of online fraud and of their trust in information about deepfakes (Nguyen Thi Thanh Huyen *et al*., 2026; Vu Thi Minh Tam, 2026) [23, 33] all recommend integrating fake-news detection and digital safety skills into training programmes.

Learners in vocational education institutions have characteristics that deserve separate attention. They enter the labour market early; many study and work at the same time, and they frequently look for part-time jobs and post-graduation employment via social media. This makes them a target group for fake recruitment, paid "online tasks" and offers of well-paid jobs abroad. For them, the most valuable lesson in digital security is not the theory of encryption but how to check whether a job advertisement or a company is genuine. The consequences of falling for such offers can go far beyond financial loss: In the most serious cases reported in the media, young people lured by promises of well-paid work abroad have ended up being forced to work for online fraud operations. Vocational institutions, which maintain close relationships with employers and labour agencies, are well placed to teach learners how to verify recruiters through official channels and to warn them about the typical warning signs of such offers.

Most vocational learners in provinces with industrial parks, such as Phu Tho, will work in factories and manufacturing enterprises, many of them foreign-invested. There they operate networked machinery and handle production data, technical drawings and customer information. The security culture they bring from school becomes part of the security culture of the enterprise. When more than 70% of attacks on organisations go through system accounts, every careful employee is an additional layer of defence.

Meanwhile, training programmes in many vocational institutions still focus mainly on occupational skills. Content on safety in the digital environment, where it exists, is usually embedded in an IT course or an induction session with limited time. The Digital Competence Framework for Learners (Circular No. 02/2025/TT-BGDĐT), in which safety is one competence domain, provides a basis for

standardising this content, particularly since State management of vocational education was transferred to the Ministry of Education and Training in 2025. Vocational teachers, especially those in non-IT occupations, have not received systematic training in digital security either, even though how teachers manage class accounts, handle learners' personal information or react to a suspicious message in a class group chat all constitute "hidden lessons" in security culture.

These characteristics show that vocational education institutions are not only places that need protection but can also become an important anchor for building digital security culture, because they directly train the technical workforce for industrial parks and enterprises.

4.7 Discussion: Explaining the gap between institutions and habits

Why has the institutional layer moved so far ahead of the others? Three explanations emerge from the analysis.

The first concerns the different speeds at which the layers can change. Institutions are produced by a relatively small number of actors (the Party, the National Assembly, the Government and ministries) through deliberate decisions. Norms and habits, by contrast, are produced by tens of millions of people through repeated everyday interactions. Within a few years, a determined State can produce a comprehensive legal framework; it cannot, in the same period, change how tens of millions of people react to a phone call from a stranger. Some lag is therefore inevitable, and it would be unrealistic to expect the behavioural layer to catch up immediately.

The second explanation concerns the content of the interventions. Most measures directed at citizens so far have aimed at raising awareness of threats. In terms of Protection Motivation Theory, they strengthen threat appraisal. The evidence reviewed in Section 4.3 suggests that threat awareness has indeed improved. However, people act on threats only when they also believe that a protective response is effective and easy to carry out, and when the people around them behave in the same way (Herath & Rao, 2009; Ajzen, 1991) [12, 1]. Interventions that make protective behaviour easier (safe defaults, simple reporting channels) and that build supportive norms in families, schools and workplaces have been less common. This helps to explain why the share of victims has fallen while reporting rates remain low and risky habits such as downloading software from links persist.

The third explanation concerns measurement. Institutions are easy to count: One can list laws, decrees and programmes and benchmark them internationally, as the GCI does. Norms and habits are harder to observe and, in Vietnam, are measured mainly through voluntary online surveys. What is not measured systematically tends to receive less policy attention. The absence of a standardised index of security culture therefore contributes to the imbalance by making progress, or the lack of it, in the normative and behavioural layers less visible to policymakers.

These explanations also suggest that the gap is not a sign of institutional failure. Rather, the institutional foundation now in place is a necessary condition for the next stage, in which policy attention should shift towards norms, habits and the conditions that make safe behaviour easy. The international experience reviewed in Section 2.1 points in the same direction: Countries and organisations that have succeeded in building security culture combine clear rules with leadership commitment, practical training and continuous measurement.

4.8 Overall assessment

Achievements: Digital security culture in Vietnam made positive progress between 2018 and 2026. The institutional layer developed quickly and coherently, kept pace with many new issues and has been recognised internationally. The awareness layer improved markedly, as shown by the fall in the share of online fraud victims in 2025 and the diversification of communication channels. Some new norms have also emerged, such as awareness of rights over personal data and greater caution towards information from strangers.

Shortcomings: The most striking feature is the unbalanced development across layers, which can be summarised as "institutions lead, habits lag". Many people know the risks but still behave dangerously out of convenience. Community norms on reporting and information sharing are weak: About two thirds of fraud victims do not report, and speed of sharing still takes priority over verification. Organisational security culture is weak, with more than half of surveyed organisations reporting damage and most attacks passing through valid accounts. Awareness and skills are uneven across population groups, regions and age groups. Digital security education is not yet organised systematically in schools, especially in vocational education, and there is a lack of periodic, standardised tools for measuring security culture and evaluating policy effectiveness.

Causes: Objectively, technology, especially generative artificial intelligence, changes much faster than human habits; cybercrime is transnational and organised, which makes tracing and asset recovery difficult; and rapid digitalisation has brought many population groups online before they could acquire self-protection skills. Subjectively, public communication still relies heavily on one-way, campaign-based information provision that is not designed on behavioural science principles; legal dissemination has not kept pace with the issuance of new regulations; many organisations treat security as a matter for the technical department rather than a leadership responsibility; the responsibility of digital platforms for safe-by-default product design is not commensurate with their role; and digital security education lacks clear learning outcomes, time allocation and assessment methods across levels and qualifications.

5. Measures for building security culture in the digital space

Based on the analysis, the article proposes five groups of measures aimed at narrowing the gap between the institutional layer and the layers of awareness, norms and behaviour. Table 4 summarises the measures, the main actors and suggested monitoring indicators.

Table 4: Summary of proposed measures, main actors and monitoring indicators

S. No	Group of measures	Target layer	Main actors	Suggested indicators
1	Habit formation instead of one-way communication	Behaviour and skills	Ministry of Public Security, media, platforms, banks, mobile operators	Victim rate; click rate in phishing simulations; share of accounts with multi-factor authentication
2	Community norms on reporting, data and sharing	Values and norms	Police, local authorities, schools, families, community groups	Share of victims reporting; share of users who verify before sharing
3	Organisational security culture	All four layers within organisations	Heads of agencies and enterprises, IT units, employees	Share of organisations damaged; periodic culture assessment scores
4	Digital security education, focus on vocational education	Awareness and skills	Ministry of Education and Training, vocational institutions, teachers, enterprises	Share of programmes with defined learning outcomes; learner assessment results
5	Measurement and whole-population mobilisation	Institutions	Government, provinces, research institutions, NCA, commune-level police	Existence of a periodic national and provincial index; number of community models

Source: Proposed by the authors

5.1 From one-way communication to habit formation

The ultimate goal of awareness programmes is not for people to "know" but for them to "do" naturally. This requires applying behavioural science principles to the design of messages and activities.

Messages should be short, concrete and immediately actionable, and they should be repeated consistently across channels. Instead of listing dozens of scams, communication should focus on a few core principles that are easy to remember, such as a three-step rule of "Stop, Check, Verify" before any request to transfer money, provide information or install an application. Excessive fear appeals should be avoided because, as Bada *et al*. (2019) [2] show, they tend to make recipients disengage rather than act.

People need opportunities to practise rather than simply listen. Controlled phishing simulations (fake emails and messages sent under supervision) in agencies and schools, with immediate feedback for participants, and simulated scenarios during class can be used. Research on organisational security culture shows that experiential learning is far more effective than learning from documents.

The environment should also be designed so that safe behaviour becomes the easiest choice. This is the responsibility of platforms, banks, mobile network operators and providers of online public services: Enabling multi-factor authentication by default, displaying warnings when users transfer money to accounts flagged as suspicious, and introducing deliberate delays for unusually large transactions so that users have time to reflect.

5.2 Building community norms on reporting, data and information sharing

The first priority is the norm that "reporting is a civic responsibility". Messages should emphasise that reporting is not only about recovering assets but about protecting others, and that being deceived is nothing to be ashamed of. At the same time, reporting procedures should be simplified through a single contact point, the option to report online through the national electronic identification application, and feedback on the progress of each case. When people see that reporting is easy and produces results, the norm will gradually take hold.

Norms of respect for personal data should be communicated through everyday situations: Not posting photos of identity documents, not sharing children's information carelessly, and not disseminating other people's personal information for any purpose. Agencies, schools and enterprises must lead by example by collecting only the minimum data necessary, being transparent about its purpose and protecting the data of learners, employees and customers.

The Code of Conduct on Social Networks should be updated with concrete norms for content generated by artificial intelligence, such as labelling synthetic content and not using other people's images or voices without consent. Class groups and residential community groups can adopt their own "group rules" requiring verification before sharing.

Finally, traditional cultural values should be channelled in the right direction. Respect for public authorities should be accompanied by the knowledge that law enforcement agencies do not handle cases over the phone or social media and never ask citizens to transfer money. Family affection should be accompanied by the habit of calling relatives back directly before acting on any request involving money. Families, and especially younger members, can act as "digital guides" for their grandparents and parents.

5.3 Developing security culture in agencies, organisations and enterprises

Leaders must initiate and model security behaviour. Heads of agencies and units should direct and participate in training and drills themselves, and treat digital security as a governance indicator rather than merely a technical task. Compliance with information security rules can be included among the criteria for evaluating staff.

A few basic "digital hygiene" measures with low cost and high effectiveness should be made mandatory: Multi-factor authentication for all accounts with system access; password policies and access management based on the principle of least privilege; and a simple, no-blame incident reporting procedure. This is the most direct way to reduce the share of attacks that pass through valid accounts.

Organisational security culture should be measured periodically, for example using validated frameworks such as that of Da Veiga and Eloff (2010) [4] or ENISA's (2017) [8] guidance, adapted to Vietnamese conditions. Measurement shows organisations which layer (awareness, norms or behaviour) is weakest, so that they can choose appropriate interventions.

5.4 Embedding digital security education systematically, with a focus on vocational education

Education is the most sustainable path to cultural change because it influences people early and over the long term. The first step is to translate the safety domain of the Digital Competence Framework for Learners (Circular No. 02/2025/TT-BGDĐT) into learning outcomes, content,

time allocation and assessment methods for each level of training, including elementary, intermediate and college levels in the vocational education system. Content should be tied to the real situations learners will face: Looking for work safely, protecting personal and bank accounts, recognising fake news and deepfakes, and protecting the data of the enterprises where they do internships.

Digital security should also be integrated into occupational modules. Learners in electrical, electronic, mechanical and automation trades should be introduced to the security of industrial control systems; learners in accounting, office administration and commerce should practise protecting customer data and recognising fraudulent payment requests sent by email. Integration of this kind makes digital security part of occupational competence rather than a separate subject.

Teachers and managers need training in digital security as part of the competence standards for vocational teachers. Institutions should adopt rules on protecting learners' personal data, rules for using class groups on social media, and procedures for responding when learners are targeted by fraud. Youth Union and Student Association chapters and student clubs can organise fake-news detection contests, "digital volunteer" teams to help older people, and joint programmes with commune-level police, thereby building learners' skills while spreading security culture into the community. Partnerships with enterprises should also extend to digital security: Enterprises share their rules and real-life incidents, and institutions build them into internship programmes, so that graduates enter the workplace with habits that fit their employer's security culture.

5.5 Establishing measurement and mobilising the whole population in the digital space

One weakness identified in this article is the absence of periodic, standardised tools for measuring security culture. Existing surveys, such as those of the NCA, are valuable but rely on voluntary online participation. A national and provincial index of digital security culture should be developed, measuring the four layers (awareness, norms, behaviour and institutions) with representative samples, conducted periodically and published openly. Such an index would help evaluate policy effectiveness and encourage positive competition between localities and sectors.

At the same time, the national movement of "the whole people protecting national security" can be extended to the digital space through models such as "cyber-safe residential areas", community digital technology teams that help residents configure security settings, and fraud-alert groups in neighbourhoods and villages, with commune-level police at their core. When every residential area and every family has someone knowledgeable about digital security, the prevention network will be denser and more durable than any single campaign.

5.6 Sequencing and implementation

The five groups of measures differ in the time they need to produce results, so their implementation should be sequenced. In the short term (2026-2027), priority can be given to measures that are inexpensive and quick to apply: Simplifying reporting procedures, making multi-factor authentication mandatory in public agencies and schools, updating communication messages around a few core principles, and integrating short practical modules on digital safety into existing vocational and university programmes. In the medium term (2027-2030), efforts can turn to measures that require coordination and investment: Developing learning outcomes and assessment tools based on the Digital Competence Framework, training teachers, institutionalising periodic security culture assessments in organisations, and piloting a provincial index of digital security culture. Phu Tho, with its combination of industrial parks, a large vocational training network and diverse mountainous communities, could be a suitable province for such a pilot. In the longer term, the goal is for safe behaviour to become a social norm that is reproduced through families, schools and workplaces without depending on campaigns. Throughout, results should be monitored with the indicators suggested in Table 4, so that measures can be adjusted based on evidence rather than assumptions.

6. Conclusion

Security culture in the digital space differs from cultural security and is broader than the culture of conduct on social media. A four-layer approach makes it clear that digital security is not only a technical or legal matter but also a question of what people believe, value and habitually do.

The analysis shows that Vietnam has achieved important results, especially in the institutional layer, with a relatively complete legal framework and an enhanced international standing (a GCI 2024 score of 99.74), together with clear progress in the awareness layer (the share of online fraud victims fell from 0.45% in 2024 to 0.18% in 2025). However, the normative and behavioural layers have changed more slowly: About two thirds of victims do not report incidents, more than half of surveyed organisations have suffered damage from cyberattacks, most attacks pass through valid user accounts, and fraud losses still amount to thousands of billions of dong per year. The unbalanced pattern in which "institutions lead, habits lag" is the defining feature of digital security culture in Vietnam today.

To close this gap, the emphasis needs to shift from issuing regulations and running campaigns to forming habits and norms, from regarding security as a matter for experts to treating it as the responsibility of every person and organisation, and from event-driven campaigns to systematic education and periodic measurement. Vocational education institutions have a special role to play because they directly train the technical workforce for industrial parks, where a good security habit on the part of a single worker can prevent a major incident.

This study has several limitations. The analysis relies entirely on secondary sources, many of which come from voluntary online surveys whose methods are not fully published, and some aspects of the values and norms layer are inferred indirectly from collective behaviour. Future research could develop a measurement scale for digital security culture based on the proposed four-layer framework and conduct empirical surveys of specific groups, such as learners and teachers at vocational education institutions in Phu Tho Province, in order to test the framework and provide evidence for policymaking.

7. References

1. Ajzen I. The theory of planned behavior. Organizational Behavior and Human Decision Processes. 1991; 50(2):179-211. Doi: https://doi.org/10.1016/0749-5978(91)90020-T

2. Bada M, Sasse AM, Nurse JRC. Cyber security awareness campaigns: Why do they fail to change behaviour, 2019? arXiv:1901.02672. Doi: https://doi.org/10.48550/arXiv.1901.02672
3. Communist Party of Vietnam Central Committee. Resolution No. 57-NQ/TW of 22 December 2024 of the Politburo on breakthroughs in science, technology, innovation and national digital transformation [Nghị quyết số 57-NQ/TW], 2024.
4. Da Veiga A, Eloff JHP. A framework and assessment instrument for information security culture. Computers & Security. 2010; 29(2):196-207. Doi: https://doi.org/10.1016/j.cose.2009.09.002
5. DataReportal. Digital 2024: Vietnam, 2024. https://datareportal.com/reports/digital-2024-vietnam
6. DataReportal. Digital 2025: Vietnam, 2025. https://datareportal.com/reports/digital-2025-vietnam
7. DataReportal. Digital 2026: Vietnam, 2026. https://datareportal.com/reports/digital-2026-vietnam
8. ENISA. Cyber security culture in organisations. European Union Agency for Network and Information Security, 2017.
9. Government of Vietnam. Decree No. 147/2024/NĐ-CP of 9 November 2024 on the management, provision and use of Internet services and online information, 2024.
10. Government of Vietnam. Decree No. 330/2026/NĐ-CP on administrative sanctions in the fields of cybersecurity and personal data protection, 2026.
11. Hadlington L. Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon. 2017; 3(7):e00346. Doi: https://doi.org/10.1016/j.heliyon.2017.e00346
12. Herath T, Rao HR. Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems. 2009; 18(2):106-125. Doi: https://doi.org/10.1057/ejis.2009.6
13. International Telecommunication Union. Global Cybersecurity Index 2024 (5th ed.). ITU, 2024.
14. Le Quang Thanh, Nguyen Quoc Khanh. Áp dụng pháp luật an ninh mạng ở Việt Nam: Lý luận và thực tiễn [Applying cybersecurity law in Vietnam: Theory and practice]. People's Police University, 2025.
15. Ministry of Education and Training. Circular No. 02/2025/TT-BGDĐT of 24 January 2025 on the Digital Competence Framework for Learners, 2025.
16. Ministry of Information and Communications. Decision No. 874/QĐ-BTTTT of 17 June 2021 promulgating the Code of Conduct on Social Networks, 2021.
17. National Assembly of Vietnam. Law on Cybersecurity No. 24/2018/QH14, 2018.
18. National Assembly of Vietnam. Law on Personal Data Protection No. 91/2025/QH15 of 26 June 2025, 2025a.
19. National Assembly of Vietnam. Law on Cybersecurity No. 116/2025/QH15 of 10 December 2025, 2025b.
20. National Cybersecurity Association [NCA]. Cybersecurity report 2024: Individual users [Báo cáo tổng kết an ninh mạng năm 2024 khu vực người dùng cá nhân], released 16 December 2024, 2024. Summary at: https://baodautu.vn/nguoi-dung-viet-nam-thiet-hai-khoang-18900-ty-dong-do-lua-dao-truc-tuyen-d232577.html
21. National Cybersecurity Association [NCA]. Cybersecurity research and survey report 2025: Individual users [Báo cáo nghiên cứu, khảo sát an ninh mạng năm 2025 khu vực người dùng cá nhân], 2025. Summary at: https://vietnamnet.vn/chi-32-12-nan-nhan-bi-lua-dao-truc-tuyen-co-bao-co-quan-chuc-nang-2479618.html
22. National Cybersecurity Association [NCA]. Cybersecurity report 2025: Organisations and enterprises [Báo cáo tổng kết an ninh mạng năm 2025 khu vực tổ chức, doanh nghiệp], released 13 January 2026, 2026a. Summary at: https://nhandan.vn/viet-nam-phai-doi-mat-voi-khoang-552000-cuoc-tan-cong-mang-trong-nam-2025-post936719.html
23. Nguyen Thi Thanh Huyen, Le Thi N, Nguyen Huyen T. Nhận thức của sinh viên về các hành vi lừa đảo trên không gian mạng trong bối cảnh công nghệ số: Nghiên cứu tại Trường Đại học Lao động - Xã hội [Students' awareness of online fraud in the digital technology context: A study at the University of Labour and Social Affairs]. Tạp chí Giáo dục [Journal of Education], 2026. https://tcgd.tapchigiaoduc.edu.vn/index.php/tapchi/article/view/5368
24. Prime Minister of Vietnam. Decision No. 1907/QĐ-TTg of 23 November 2020 approving the Scheme on raising awareness and popularising information security skills for 2021-2025, 2020.
25. Prime Minister of Vietnam. Decision No. 468/QĐ-TTg of 23 March 2026 approving the Programme on protecting and supporting children to develop safely in the online environment for 2026-2030, 2026.
26. Ribble M. Digital citizenship in schools: Nine elements all students should know (3rd ed.). International Society for Technology in Education, 2015.
27. Rogers RW. A protection motivation theory of fear appeals and attitude change. The Journal of Psychology. 1975; 91(1):93-114. Doi: https://doi.org/10.1080/00223980.1975.9915803
28. Schein EH. Organizational culture and leadership (4th ed.). Jossey-Bass, 2010.
29. Uchendu B, Nurse JRC, Bada M, Furnell S. Developing a cyber security culture: Current practices and future needs. Computers & Security. 2021; 109:102387. Doi: https://doi.org/10.1016/j.cose.2021.102387
30. Van Niekerk JF, Von Solms R. Information security culture: A management perspective. Computers & Security. 2010; 29(4):476-486. Doi: https://doi.org/10.1016/j.cose.2009.10.005
31. Verizon. 2024 Data Breach Investigations Report. Verizon Business, 2024.
32. VNPT Cyber Immunity. Vietnam cybersecurity situation report, first half of 2025, 2025. Summary at: https://vneconomy.vn/ransomware-gay-thiet-hai-hon-10-trieu-usd-tai-viet-nam-nua-dau-2025.htm
33. Vu Thi Minh Tam. Đánh giá cơ chế ứng phó với tin giả do deepfake trên mạng xã hội tại Việt Nam và đề xuất các khuyến nghị liên quan [Assessing response mechanisms to deepfake-based fake news on social media in Vietnam and related recommendations]. Tạp chí Giáo dục và Xã hội [Journal of Education and Society], (January 2026, Issue 1), 2026, 247-252.