

Knowledge of artificial intelligence, social media and cybersecurity among young people in Myanmar

Zin Ko Lin
Master of Business Administration
Lincoln University College
zinkolin.hr@gmail.com

Thin Yanant
University of Information
Technology
Yangon, Myanmar
thinyanantonline@gmail.com

Hlaing Htake Khaung Tin
University of Information
Technology
Yangon, Myanmar
hlainghtakekhaungtin@gmail.com

Abstract: *AI is making it difficult to teach cybersecurity using phony text, fake audio and manipulated video. This study analyzes these difficulties for Myanmar youth via secondary literature. It is based on scholarly articles, information on workplace risks and research conducted in Myanmar. It asks three questions: what is occurring, what may be the issue and how to respond. Discussion on phishing, impersonation, internet fraud, malware and ransomware. Basis is worldwide evidence and Myanmar/youth evidence. This shows out that internet literacy, validation procedures and trusted aid seeking might affect safe conduct. It provides a framework for connecting danger exposure, educational skills and preventive measures in local contexts. This has not been tested with this framework. It is presented just for debate and further investigation. They provide realistic validation exercises, teaching resources that are easy to grasp, security measures for businesses, and safe methods to get support. This paper does not use original data from surveys or interviews. It does not contain statistical analysis. It is qualitative synthesis and only rational recommendations. It doesn't measure the level of knowledge of young people today.*

Keywords: Social Media, Cyber Security Knowledge, Digital Knowledge, Youth, Myanmar, Narrative Review, Artificial Intelligence

I. INTRODUCTION

Social media and online services are now placing for communication, learning, looking for jobs and exchanging information. [1] DataReportal talks about the use of the Internet and social media in Myanmar. However, these numbers don't tell the whole story about young people's cybersecurity knowledge. Nor do they prove that young people are the most vulnerable. This paper, however, is specifically concerned with young people. They are very active in the digital environment and have educational questions about it.

International news reported that criminals have used AI tools for impersonation and financial fraud [2]. The creative abilities of AI could easily lead to fake communications being mistaken for genuine ones. ASPI's report on Myanmar, the Ruser report, concerns the systematic fraud operations in Myanmar's conflict economy [3]. But the existence of these operations does not tell us how many young Burmese are being targeted. Nor does it prove that AI was used in the cases they were involved in. The research problem is how to link the three dimensions of international trends, national reports and local youth experiences. These three dimensions are not interchangeable.

Although the selected literature offers insights into emerging threats, education and local contexts, it does not assess the national scale of cybersecurity

knowledge of AI among Myanmar youth. This is a limitation of the evidence on which this paper is based. This is not to say that there aren't other relevant studies.

The objectives of this paper are: 1) to present the reported threats regarding youth cybersecurity, 2) to discuss the recognition and response to suspicious online activities, and 3) to share a conceptual framework and practical suggestions. The structure of the paper is as follows.

Section II presents the literature review. Section III presents the research approach. Sections IV and V present developments and possible implications. Section VI presents the framework. Section VII presents recommendations. Section VIII presents the conclusion.

II. LITERATURE REVIEW

A. AI and emerging cyber threats

Marella, Veluru and Erukude analyze the cybersecurity threats associated with AI [4]. Includes mixed media, automated malware, malicious attacks, social engineering, etc. Their classification is useful for this paper, but it does not measure how widespread these threats are among Myanmar youth. It additionally emphasizes the difference between having AI capabilities and having proof that those capabilities are being used.

INTERPOL has said that criminals have access to tools that can clone a person's voice or face and are using them to impersonate others [2]. So, education must include the danger of mixed media. But not all fraud online is generated by AI. Visual error detection does not always detect mixed content. Therefore, an educational response should incorporate the how-to of checking the authenticity of a message, an image, or a sound.

B. Ransomware and other forms of threats

The StopRansomware guide describes the encryption, disruption, and data-extortion functions of ransomware and lists several initial access pathways [5]. Phishing is one way it does this, but it also uses

stolen credentials and vulnerabilities." So, ransomware should not be dismissed as one "user error." Prevention should include system maintenance, access control, recovery plans, and understanding suspicious requests.

In the literature on the AI threat [4] it is stated that artificial intelligence tools can assist with attack vectors. However, that does not mean AI-enabled ransomware is common among Myanmar's young people. Nor should ransomware be seen as a new emerging category. It is important for youth education to know about unsafe downloads, identity protection, risk of file loss and where to find help.

TABLE I. THREAT CATEGORIES, DESCRIPTIONS, AND PRACTICAL EXAMPLES.

Threat Category	Key Description	Practical Example in Context (e.g.)	Relevance to Paper
AI-Assisted Phishing & Deception	Use of AI tools to generate natural, grammatically flawless deceptive messages.	E.g., social media messages offering fictitious scholarships or job offers that request verification codes or passwords. Globally, fraud-related INTERPOL Notices and Diffusions rose 54% between 2024 and 2025, with financial fraud losses estimated at USD 442 billion in 2025 (INTERPOL, 2026).	Shows that grammar alone is no longer a reliable cue for identifying scams.
Synthetic Media & Impersonation	Generating deepfake audio or video to impersonate individuals.	E.g., replicating the voice or image of a family member or acquaintance to request emergency funds. INTERPOL estimates that such AI-enhanced fraud is roughly 4.5 times more profitable than traditional methods (INTERPOL, 2026).	Highlights the need for independent verification, even when a request appears to come from a known contact.
Ransomware & System Exploitation	Encrypting data to extort funds or disrupt operations.	E.g., unauthorized entry via vulnerable portals or unsafe downloads, leading to data exfiltration and extortion. The guide identifies phishing, stolen credentials, and vulnerability exploitation as the leading initial-access routes but reports no incidence figures specific to Myanmar or youth populations (CISA/FBI, 2023).	Emphasizes that ransomware involves system vulnerabilities, not solely user error.
Organized Scam Syndicates	Structured criminal networks operating large-scale online fraud.	E.g., industrial-scale scam operations linked to conflict economies. ASPI documents that dedicated scam compounds along the Thailand–Myanmar border grew from 11 to 30 since 2021, expanding at roughly 13.5 acres per month over four years (ASPI, 2025).	Shows that fraud operations are institutionalized rather than isolated individual mistakes.

C. Digital literacy and cybersecurity education

Piki, Markou, and Stavrou developed a model of cybersecurity literacy [6]. It integrates four dimensions: academic, professional, conceptual, and experiential. Their work supports the need for not only knowledge but also practical skills. The application of this dimension to AI fraud is an extension of what we have here and is not a result of their original study.

In this paper, "digital literacy" refers to the ability to evaluate digital information and use online tools effectively. "Cybersecurity awareness" is being aware of dangers and knowing the defensive solutions. "Protective behavior" means taking measures such as accepting a request, restricting account access, or asking for support. The three ideas are similar, yet different. Knowing a platform is not equal to having

security abilities. Knowing the danger is one thing, but being able to act on it if you need to is another thing.

D. Knowledge, attitudes and protective actions

Bhagat and Pravin presented an addition to the Knowledge-Attitude-Behavior model [7]. They evaluated the relationship between training, past experiences and awareness with adaptive responses. This approach is beneficial but should not be seen as evidence that training (or previous experience) by itself will make for safer conduct.

Mahlangu, Chipfumbu Kangara and Masunda created a citizen-centric model based on Protection Motivation Theory [8]. Their investigation identified links among knowledge, attitudes, intentions, and behavior.

The findings have not been replicated among Burmese

youngsters.

But they argue that knowledge of the danger and conviction that the solution on offer will be effective are significant.

E. Myanmar's unique evidence

Their [9] research from Yangon investigates cybercrime awareness and legal issues. It is historical background material, but geographical coverage and sample size is restricted. Hence, it should not be used as a measure of Myanmar youth's present understanding or awareness of contemporary AI risks.

The 2025 Cybersecurity Law in Mon State was analyzed by Min Oo and Ma Mak Kul via a case study of young people [10]. They said they had been under surveillance, restricted access to information and fear of arrest. Although the results may not be generalizable to the whole nation, they have implications for instructional design in terms of how to locate credible information.

III. REVIEW APPROACH

A. Design and dimensions

The paper is a narrative review of secondary sources, and a conceptual discussion. The publications and reports are the only evidence cited in the text. It does not contain original survey, interview data or statistical analysis. The results of the cited studies are not replicated in this paper. The materials were selected for relevance to emerging threats, cybersecurity education or the Myanmar context. This is intended to give a general idea of the discussion and not a systematic selection process. It does not include a systematic database search, formal verification process or independent peer review process. Note that this review is not a complete or validated review of all cases.

In this paper, the term "youth" refers to the academic focus of the paper rather than a sample population with the same age range. Each study included its own population (e.g., social media users, students). Different sources defined age ranges differently. So, no common age range was established. Further studies should clearly define the target age range and recruitment criteria.

B. Analytical organization

The review is divided into three phases. The first part considers what the sources say about the threats and the context. The second stage looks at factors that might make it difficult to identify or react to those threats. The third stage is the compilation of educational and institutional responses. This is not a coded data set or a tested model, but a set of content and ideas.

Three differences are noted. The first is the difference between international evidence and Myanmar-specific evidence. Second is the difference in Myanmar between reports of fraud and evidence about victims. The third is the distinction between general findings and direct findings about youth. The differences are so great that you cannot substitute one word for the other.

C. Limitations

The sources cited vary in purpose, date, geographical scope and validity. The roles of academic journals, proposed models, operational evaluations and policy reports vary. Technical details may be omitted from public reports. This review does not purport to assess current knowledge, compare age groups or recommend interventions. The framework and recommendations are intended only as suggestions for further evaluation.

IV. REPORTED DEVELOPMENTS AND THEIR RELEVANCE

A. AI-assisted deception

AI-powered impersonation and social engineering have been described by international sources [2], [4]. These capabilities are important for education, because a smooth message or familiar voice can make a false claim more believable. This should be understood when considering Myanmar youth but it does not mean that all youth have experienced it. It is also not an estimate of levels of national exposure or awareness.

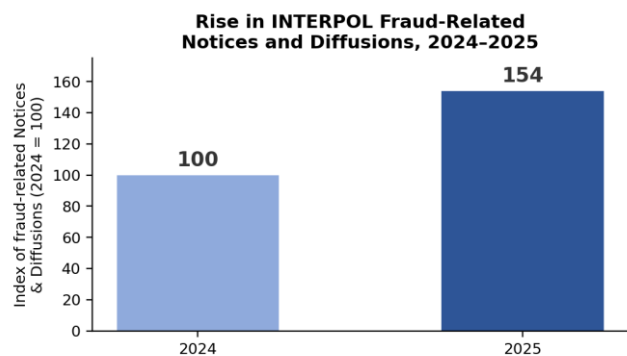


Fig. 1. Rise in INTERPOL fraud-related Notices and Diffusions, 2024–2025, indexed to 100 in 2024 (INTERPOL, 2026).

B. Social media and trust

The user can access a social media account that has been stolen or is fake. For example, an account might say they are a scholarship provider and ask you to click a link to get to it. You may be asked for a code to verify that you are you. This is not a real incident in Myanmar, but a hypothetical example for educational

purposes. Lessons learned point to the best approach, which is to look at the source and intent of the request, rather than the name of the sender or the format of the message.

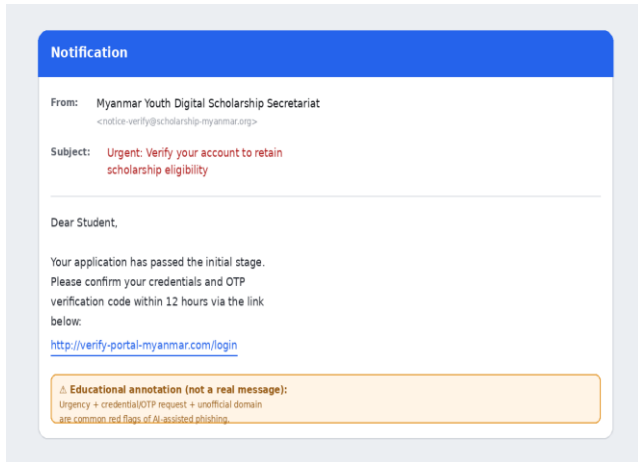


Fig. 2. Hypothetical example of a deceptive social media notification used for educational verification exercises.

There are opportunities for communication via platforms, but this analysis does not quantify the degree to which time spent online is associated with victimisation. It can depend on your account settings, the support available, what the attacker does, your situation. Some background material The National Social Media Report [1]. Advertising reach and user profiles should not be used as a proxy for individual exposure for adolescents.

C. Systematic fraudulent activities

ASPI has previously explored the linkages between fraud systems, criminal networks and the war economy in Myanmar [3]. It is about the institutional and physical infrastructure that enables fraud. It moves

the discussion away from individual blunders. The location of the company, the location of the victim, and the age of the victim are independent issues, but. This report does not show that Myanmar youth are the main target, or that all institutions are using AI.

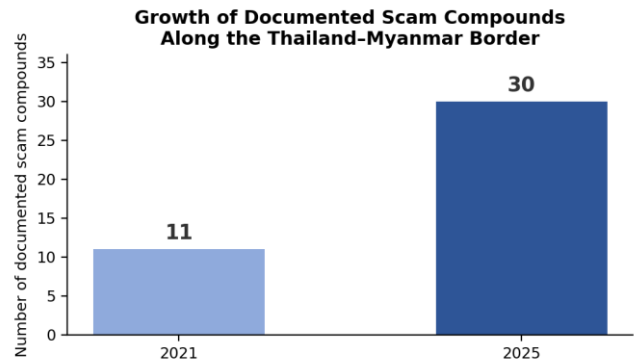


Fig. 3. Growth in the number of documented scam compounds along the Thailand–Myanmar border, 2021–2025 (ASPI, 2025).

D. Local awareness and information gathering

The Yangon Awareness Research [9] and the Mon State Digital Rights Study [10] ask different questions. The first contains historical data on the awareness of chosen internet users. The second one describes specific experiences and concerns within the legal and political context. The results they got cannot be generalized into one measure for the nation. Instead, they raise questions of educational access and dependable support that should be addressed locally, not a wholesale deficit among young people.

TABLE II. COMPARISON OF CYBER THREATS: INTERNATIONAL CONTEXT VS. LOCAL MYANMAR CONTEXT.

Threat Dimension	International Context & Evidence	Local Myanmar Context & Specific Findings
AI Deception Prevalence	High adoption of voice/face cloning and automated phishing; global financial fraud losses reached an estimated USD 442 billion in 2025, with a 54% rise in fraud-related Notices and Diffusions from 2024 to 2025 (INTERPOL, 2026).	E.g., lack of empirical national-scale data specifically measuring AI deepfake victimization among Myanmar youth.
Fraud Infrastructure	Transnational cybercrime syndicates leveraging advanced AI tooling; INTERPOL supported more than 1,500 transnational fraud cases involving USD 1.1 billion in traced assets since 2024 (INTERPOL, 2026).	E.g., large-scale scam syndicates tied to conflict economies operating in Myanmar; ASPI documents growth from 11 to 30 dedicated scam compounds along the Thailand–Myanmar border since 2021 (ASPI, 2025).
Legal & Social Environment	Standardized cybersecurity regulations and data-privacy frameworks.	E.g., youth in Mon State report surveillance concerns and restricted information access under the 2025 Cybersecurity Law (Minn Oo & Mamadkul, 2026).
Digital Exposure & Connectivity	Expanding global internet and social media adoption widens the population reachable by phishing and impersonation attempts.	E.g., Myanmar recorded 39.8 million internet users (72.5% penetration) and 21.0 million social media user identities (38.2% of the population) as of late 2025 (DataReportal, 2026), though this reach figure is not a measure of youth cybersecurity knowledge.

V. POSSIBLE SUPPORTING FACTORS AND DISCUSSION

A. Verification skills and confidence

One possible problem is the difference between knowing you have a suspicious request and knowing what to do about it. The learner may be able to identify pressure or urgency but may not be sure how to check an account, reject a request or seek help. The educational approaches in claim that information, attitudes and perceived skills are combined to examine the link. It is an outstanding issue if these relationship dynamics are experimentally played out in a group of young Burmese people.

B. Attractive content and social pressure

You can't tell stuff created by AI by the syntax, or by the way it looks. But familiarity, urgency and promises of advantages may all influence responsiveness to a request. Education alone does not make learners become deepfake detection experts. There are enough decision points to be getting on. Independent verification is a useful talent, the study contends. But it doesn't indicate any single practice decreases exploitation in Myanmar.

C. Access to support and local conditions

Educational materials work best when they are customized to the language, connection and institutional environment of the learners. The Mon State research [10] also examined the ease of individuals in sharing about internet experiences. When creating a program, these criteria should be considered. But this evaluation cannot measure the knowledge gap created by a legislation. Suitable routes of distribution and assistance will need to be identified via local engagement.

D. Responsibilities that go beyond the individual.

Being informed is not enough to react to organizational breaches and fraud infrastructure. Schools and service providers may affect account recovery, security settings and assistance choices. The system-level strategies described in this study support the educational emphasis. This separation of responsibility ensures that the victim is not blamed for any successful assault that may have resulted from his ignorance or ineptitude.

These factors combined establish a paradigm that highlights the relationship between education and context. That is not to imply that they follow a special goal that would necessarily lead to under-awareness or disadvantage in AI development. Young individuals may already be using useful preventative behaviors. The next exam will identify strengths and unmet requirements.

VI. PROPOSED CONCEPTUAL FRAMEWORK

The paradigm links three domains: exposure to false claims, capacity to assess and act on such claims, and protective measures. All three domains are local environments. Knowledge, practical skills, attitudes and action are not a single construct but interrelated educational considerations. The framework is motivated by [6]–[8] and the Myanmar context is discussed in [3], [9], and [10].

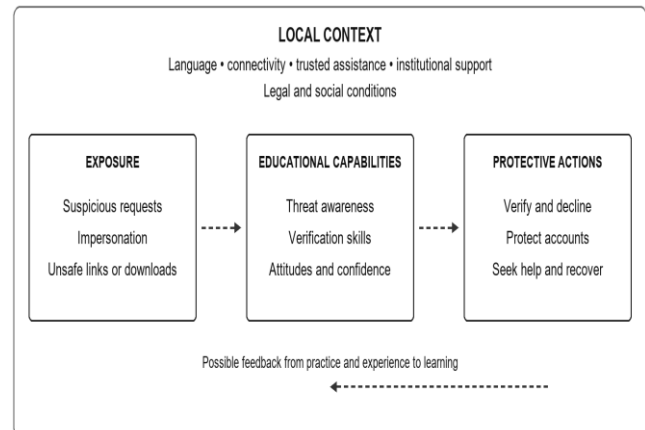


Fig. 4. Proposed framework for youth cybersecurity education in Myanmar. Dotted arrows indicate possible relationships only. They do not show causal effects. They have not been tested.

Exposure covers suspicious messages, phishing, unsafe links and downloads. Education skills include the ability to identify the risk, the ability to independently review the claim, the ability to identify available protection and the confidence to use it. Protective measures include verification, careful management of accounts, refusal of inappropriate requests, seeking assistance and recovering the account in case of an incident.

Local context includes language, connectivity, institutional support, trusted help, and the legal and social environment. These factors are to be taken into account for local assessment not for measurement. The framework also acknowledges feedback. Thus, incident experience does not necessarily lead to safer behavior. However, practical experience can inform subsequent learning. This figure is not a validated measurement instrument. It is a tool for compilation and should be used before the practical testing.

VII. SUPPORT AND SUGGESTIONS

This paper's contribution is linking selected Myanmar-specific evidence to the international threat literature. It keeps their different dimensions. It provides a framework for identifying educational questions, designing and evaluating responses. There's no new national knowledge base from this. It also does not claim that the framework is the first.

A. Practical education

Teachers are able to use short, clear scenarios (e.g., scholarship offer, job message, account alert, impersonating a close contact). Exercises should focus on the learner explaining what they would do to verify a request on their own and when they would ask for help. The objective is to have a decision-making process that is not based on blind trust in the content or that it came from an AI.

Should detect phishing, account theft, synthetic media impersonation, and ransomware. Not necessarily true AI is able to be used in materials. Learners need opportunities to practice safe responses and to discuss uncertainties. “We shouldn’t judge educational effectiveness by subsequent attendance or self-reported satisfaction, but by actual assessments.”

TABLE III. CONCEPTUAL FRAMEWORK DOMAINS, EDUCATIONAL SCENARIOS, AND PROTECTIVE ACTIONS.

Framework Domain	Practical Scenario Example (e.g.)	Recommended Protective Action
Exposure	E.g., receiving unsolicited messages on Telegram or Facebook with links claiming account suspension or a contest win.	Refrain from clicking links immediately; critically evaluate the legitimacy of the request.
Educational Capabilities	E.g., recognizing pressure tactics, artificial urgency, or unusual requests for credential verification.	Perform independent verification through a trusted, out-of-band communication channel.
Protective Actions	E.g., experiencing an account breach or an accidental link click.	Immediately reset account credentials, enable Two-Factor Authentication (2FA), and report to a trusted institutional channel.

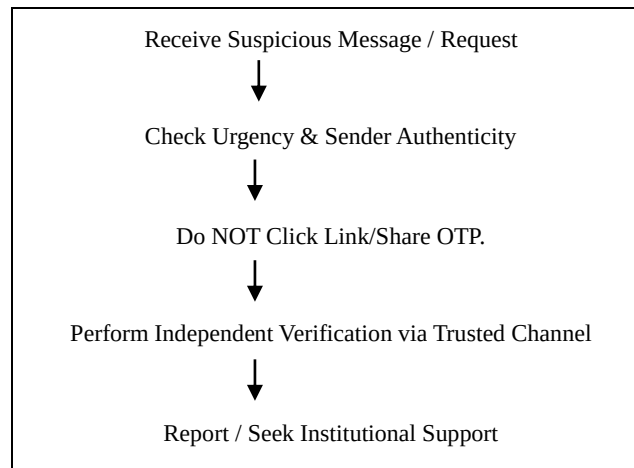


Fig. 5. Proposed decision-making workflow for youth independent message verification and protective action.

Fig. 6.

B. Institutional Security and Assistance

Schools should think about ways to transparently report suspicious messages and offer account recovery assistance. All relevant preventive measures are software maintenance for the systems they manage, proper access control, stronger authentication and recoverable backups [5]. Educational materials should state explicitly what the learner can do alone and when he/she needs help from the institution. It should not be inferred from these recommendations that the authors have identified any vulnerabilities in their own organizations.

C. Easily transportable and convenient delivery

Program designers can engage with youth and educators about language, connections, examples and priority support channels. Printed, or low bandwidth, materials can be useful in contexts of limited access.

Participants are not required to disclose passwords, private messages, or identifiable victim accounts. Don’t assume that a local channel is relevant – check locally if it is suitable.

D. Future assessment

Future research could include interviews, educational pilot studies or situation-based assessments for the validation of the relevance of the framework. One may want to estimate knowledge in a particular population. A survey may be appropriate. Where the study involves minors, appropriate consent processes, age range, collection method, measures and safeguards should be specified. No such activities have been performed in this paper.

VIII. CONCLUSION

This narrative review explores emerging cyber risks and drivers of youth responses, along with

educational and institutional interventions that may be relevant in Myanmar. International reports concentrate on AI-assisted deception. Selected Myanmar sources provide background information on awareness, systematic deception and access to information. Existing data do not determine current national youth awareness, prevalence, or linkages of these factors. The proposed framework situates validation skills, knowledge, attitudes and confidence in a wider context of support and opportunity for action. Practical education, institutional security and accessible support are proposed as complementary areas for development. The future will see the assessment of the effectiveness and applicability of the framework for some youth groups.

REFERENCES

- [1] S. Kemp, "Digital 2026: Myanmar," DataReportal, Nov. 8, 2025. Accessed: Sep. 13, 2026. [Online]. Available: <https://datareportal.com/reports/digital-2026-myanmar>
- [2] INTERPOL, *Global Financial Fraud Threat Assessment*, 2nd ed., Mar. 2026. [Online]. Available: <https://www.interpol.int/content/download/24291/file/INTERPOL+Global+Financial+Fraud+Threat+Assessment+2026.pdf>
- [3] N. Ruser, "Scamland Myanmar: How conflict and crime syndicates built a global fraud industry," Australian Strategic Policy Institute, Canberra, ACT, Australia, Sep. 8, 2025. [Online]. Available: <https://www.aspi.org.au/report/scamland-myanmar-how-conflict-and-crime-syndicates-built-a-global-fraud-industry/>
- [4] S. T. Erukude, V. C. Marella, and S. R. Veluru, "AI-driven cybersecurity threats: A survey of emerging risks and defensive strategies," arXiv:2601.03304, Jan. 2026, doi: [10.48550/arXiv.2601.03304](https://doi.org/10.48550/arXiv.2601.03304).
- [5] Cybersecurity and Infrastructure Security Agency, Multi-State Information Sharing and Analysis Center, National Security Agency, and Federal Bureau of Investigation, "#StopRansomware guide," ver. 3.0, Oct. 2023. [Online]. Available: <https://www.ic3.gov/CSA/2023/231019.pdf>
- [6] A. Piki, M. Markou, and E. Stavrou, "Towards a unified model of cybersecurity literacy: Blending pedagogical, professional, conceptual and empirical insights," in *Proc. 2024 AIS SIGED European Conf. Information Systems Education Research*, 2024, Paper 7. [Online]. Available: <https://aisel.aisnet.org/eciser2024/7/>
- [7] S. Bhagat and D. P. Pravin, "Cybersecurity awareness and adaptive behavior: Does prior exposure lead to adaptive behavior?" in *Proc. 29th Americas Conf. Information Systems (AMCIS)*, 2023, Information Security and Privacy (SIG SEC), Paper 23. [Online]. Available: https://aisel.aisnet.org/amcis2023/sig_sec/sig_sec/23/
- [8] G. Mahlangu, C. Chipfumbu Kangara, and F. Masunda, "Citizen-centric cybersecurity model for promoting good cybersecurity behaviour," *Journal of Cyber Security Technology*, vol. 7, no. 3, pp. 154–180, 2023, doi: [10.1080/23742917.2023.2217535](https://doi.org/10.1080/23742917.2023.2217535).
- [9] Y. Sein, "A study on cybercrimes awareness of internet users in Yangon," M.Dev.S. thesis, Dept. Economics, Yangon Univ. Economics, Yangon, Myanmar, Dec. 2020. [Online]. Available: <https://meral.edu.mm/records/8643>
- [10] M. M. Minn Oo and J. Mamadkul, "Assessing impacts on digital rights and freedom among youths under Myanmar's Cybersecurity Law 2025: A case study of youths in Mon State," *Journal of Contemporary Social Sciences and Humanities*, vol. 13, no. 1, pp. 70–86, 2026, doi: [10.59796/jcsh.v13i1.70-86](https://doi.org/10.59796/jcsh.v13i1.70-86).