Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th February 2026. Vol. 5. No. 2; e-ISSN: 2808-4519

Cybersecurity Awareness: A Literature Review on Internet Users' Awareness and Safe Behavior

Ananda Amalia Putri [1*], Anisa [2], Yuni Azizah [3], A. Hamdani [4]

[1,2,3,4]*Information Technology, Ibrahim University, Indonesia*
nandamaliaptr@gmail.com[1], anisa.aufa87@gmail.com[2], yuniazizah255@gmail.com[3], dan.kidz88@gmail.com[4]

Abstract

The rapid development of information technology has facilitated various aspects of human life, from communication and education to financial transactions. However, this progress has also been accompanied by the growing threat of cybercrime, such as data theft, hacking, and digital fraud. One of the most influential factors contributing to this growing threat is the low level of cybersecurity awareness among internet users. This article aims to review the various literature related to cybersecurity awareness and user safety behavior in the online world. The method used is to review literature from various scientific sources from 2022 to 2025 that discuss cybersecurity awareness, behavior, and education. The results of the study show that while security technology continues to evolve, human awareness remains the weakest point in cyber defense. Therefore, improving education and digital culture is a key strategy in developing safe behavior among internet users.

Keywords: Cybersecurity, Cyber Awareness, Security Behavior, Digital Culture

1. Introduction

Advances in digital technology have had a significant impact on human life. In today's digital age, almost all human activities are connected to the internet, whether for personal, business, or government purposes. However, behind these various facilities, a new threat has emerged, also known as cybercrime. Common forms of cyberattacks include *phishing, malware, ransomware, identity* theft, and misuse of personal data. Article 9.

Cybersecurity awareness is essential to prevent such attacks. Highly conscious users will be more careful in managing personal data and learning about cyber threats. Tony Tan et al.'s (2024) research on students in Batam City revealed a low level of cybersecurity awareness, with many ignoring software updates, using weak passwords, and yet sharing their personal data publicly without caution. [9]

Awareness-raising strategies are also being implemented through education, such as developing an online cybersecurity education platform. Colby's (2024) research shows that digital education and socialization can help increase public knowledge of the importance of protecting personal information from cyber threats. In addition, socialization that takes place in various communities up to the government level is highly recommended to promote cybersecurity behavior. [7]

2. Theoretical Foundations

2.1. Definition of Cybersecurity

Cybersecurity *is defined* as an effort to protect computer systems, networks, and data from attacks, illegal access, and damage caused by irresponsible parties. The main goal of cybersecurity is to maintain confidentiality, integrity, and data availability, known as the CIA trio. According to Jansen and von Solm (2022), cybersecurity is not only a technical responsibility, but also human behavior. Users play a vital role in keeping information secure, with the majority of attacks exploiting human errors such as opening malicious links or providing personal data to unknown parties. [9][6]

2.2. Definition of Cybersecurity

Cybersecurity awareness refers to an individual's understanding of potential digital threats and their ability to take preventive measures to protect themselves from cyber risks. Ramadan's (2022) research shows that social media users' level of knowledge of cyber threats significantly affects their ability to recognize and anticipate existing digital risks. [5]

Al-Qarni et al. (2024) explain that cyber awareness involves three important aspects: knowledge of cyber threats and risks, vigilance towards suspicious activities, and proactive behavior in maintaining the security of personal data. Qolbi's (2024) study on cybersecurity education platforms emphasizes the importance of vigilance and proactive behavior as the key to preventing security incidents in the digital world.

2.3. Safe behavior for Internet users

Safe behavior in the context of cybersecurity includes habits such as using strong and unique passwords. This is especially important since many cyberattacks exploit weak passwords. A study by Tan et al. (2024) found that college students who used strong passwords tended to have a lower risk of personal data theft and cyberattacks. [9]

In addition, not sharing personal information randomly is also considered safe behavior that must be maintained. Ramazani's (2022) research confirms that awareness of the risks of sharing personal data freely on social media significantly impacts users' security from identity theft and other cyberattacks. [5]

Avoiding opening links or attachments from anonymous sources is usually important to prevent malware and phishing. Colby (2024) emphasized in his research that vigilance in evaluating digital information sources is very effective in reducing security incidents caused by cyber manipulation. [7]

Another important behavior is to make regular software updates to fix security vulnerabilities. The Indonesian Ministry of Youth and Youth Report (2023) states that regular updates to systems are one of the key strategies to enhance network security from cyber threats.

According to Putrey and Nogroho (2023), safe behavior is not only influenced by knowledge, but also by habits, digital experiences, and the influence of the user's social environment. [6]

2.4. Factors Affecting Cyber Awareness

Some of the key factors that affect the level of user awareness include:

1. Education and digital culture: The higher the level of reading and writing, the more users are aware of digital risks.
2. Personal experience: Users who have been exposed to cyberattacks tend to be more cautious.
3. Training and socialization: Educational activities from institutions or governments have a significant impact.
4. Organization culture: In the workplace, safety policies can shape safe employee behavior.

3. Research Methods

The method used in this study is to review the literature by collecting and analyzing various relevant scientific sources on cybersecurity awareness and the safe behavior of internet users. Tan's (2024) research applies a similar approach by reviewing the literature to determine the current state of cybersecurity awareness and behavioral indicators in users. [9]

Literature standards include publications from international journals, national journals, official reports, and academic publications that discuss cybersecurity awareness, behavior, or training. Kusumaningrom's (2022) study used similarly rigorous criteria in his literature study to measure students' level of cybersecurity awareness through models such as the Critical Security Behavior Scale and HAIS-Q. [3]

The analysis was conducted descriptively by comparing the results of different studies to find common patterns, challenges, and solutions to increase cybersecurity awareness. The research on the Cybersecurity Capabilities Gap in Indonesia (2024) applies a descriptive analysis of the literature to identify digital threat patterns and literacy recommendations. [4]

The analysis was conducted using a descriptive-comparative approach, comparing the results of different studies to find general patterns, challenges, and proposed solutions to increase cybersecurity awareness. In this way, a literature review not only summarizes the content of each article, but also attempts to identify a common thread that can serve as a basis for recommendations for developing digital culture strategies and personal data protection in Indonesia.

4. Discussion

4.1. Factors Affecting Cyber Awareness

Globally, the level of cybersecurity awareness remains relatively low. Based on the *Cybersecurity Awareness Index* (2024) report, only 38% of users regularly update passwords regularly. In Indonesia, a survey from Cominfo (2023) showed that 60% of people still use the same password for several accounts at the same time.

This demonstrates the need for continuous education so that users understand the risks and impacts of unsafe acts in cyberspace.

4.2. Challenges in Increasing Cyber Awareness

Some of the main obstacles found in the literature include:

1. The decline of digital culture among the general public.
2. Lack of training or public campaigns on cybersecurity.
3. There is a perception that security is the responsibility of the technician, not the user.
4. Difficulty changing digital behavior that has become a habit.

As Al-Qarni et al. (2024) explained, changing behavior requires time, motivation, and a sustainable educational approach.

4.3. Effective Strategy and Education

Some of the main obstacles found in the literature include:

1. Integrate cybersecurity topics into the education curriculum from an early age.
2. Public campaigns via social media and educational institutions.
3. Simulation and training in real cases (e.g., anti-phishing training).
4. Collaboration between government, academia and the private sector in building a culture of digital security.

4.4. The Role of Government and Educational Institutions

In addition to the Digital Culture Program at Kuminfo, a number of other initiatives are playing a role in raising awareness of cybersecurity. BSSN, in collaboration with the State Technical Institute of Cyber Science and Cryptography, has developed KLIKS, a web-based educational application based on the UNESCO framework and has proven to be effective in improving the understanding of information security. At the community level, experienced UPN lecturers in Jakarta have done their part to protect personal data in the village of Pankalan Jati, Debuk, which provided hands-on instruction on the use of passwords and regulations. Meanwhile, Batam International University conducted a cyber awareness survey for students and encouraged the integration of digital security education into the curriculum

The government plays an important role in formulating policies and regulations that support national digital security. On the other hand, educational institutions act as a forum to shape the digital behavior of the younger generation. The Ministry of Communication and Informatics has launched the "Indonesian Digital Culture" program that aims to raise public awareness of cyber threats. This type of program should be expanded to include all levels of society and be tailored to meet local needs, so that digital culture is not only a national agenda but also relevant to the needs of communities on the Regional level.

5. The end

Cybersecurity awareness is the key to creating a secure digital environment. Although security technology continues to evolve, the human factor remains the most vulnerable element of the cyber system.

The results of the review show that the level of awareness among internet users remains low, especially in basic practices such as password management and vigilance against online fraud. Therefore, increasing digital culture and continuing education should be a priority.

Suggestions

1. The government and educational institutions need to expand cybersecurity-based digital culture programs.
2. Internet users should get used to implementing safe behaviors, such as using strong passwords and being aware of cyber threats.
3. The following research is expected to examine the effectiveness of cyber awareness training programs empirically in various sectors of society.

References

[1] R. N. Rohma, "Efforts to Build Cybersecurity Awareness among E-Commerce Consumers in Indonesia", *Syndicia Nyaga: Journal of Trade Development and Studies*, Vol. 6, No. 1, pp. 1–11, 2022.
[2] D.V. Saputra, "Digital Culture for the Protection of Personal Data", *Journal of Police Science*, Vol. 17, No. 3, pp. 1–8, December 2023.
[3] Kusumaninderum, H. Wijayanthu, and B. D. Rahraja, "Measuring the Level of Cybersecurity Awareness among Students When Studying from Home Using Multi-Criteria Decision Analysis (MCDA)", *Sen Scientific Journal (JIS),* Vol. 20, No. 1, pp. 69–76, January 2022.
[4] S. A. Elena and A. F. Nograha, "The Gap in Indonesia's Cybersecurity Capabilities in Reducing Cyber Attacks in Digital Public Services in 2020–2025", *Trivikrama: Interdisciplinary Journal of Social Sciences*, Vol. 8, No. 6, pp. 1–15, 2025.
[5] M.R. Ramazani and A.R. Pratama, "Cybersecurity Awareness Analysis among Social Media Users in Indonesia", *UII Journal of Informatics*, Vol. 3, No. 2, pp. 1–14, 2020.
[6] T. J. Laksana and S. Mulyani, "The Underlying Factors of Cybercrime Against Humanity," *Brewers: Journal of Law and Human Rights*, Vol. 11, No. 2, pp. 136–160, March 2024.
[7] N. Kolby and H. Capita, "A Web-Based Cybersecurity Education Platform Based on UNESCO's Global Framework for Digital Culture", *INTEKNA Journal*, Vol. 24, No. 2, pp. 148–155, November 2024.

[8] M. B. Aji and Supakdi, "Cybersecurity Awareness and Protection of Personal Data of Residents of Pankalan Jati Village, Depok City", *Journal of Syntax Admiration*, Vol. 5, No. 8, pp. 2928–2936, August 2024.
[9] T. Tan, H. Sama, T. Wibo, J. Wijaya, and O. E. Abwaji, "Cybersecurity Awareness among University Students in Batam City", *JATI: Journal of Technology and Information*, Vol. 14, No. 2, pp. 163–168, September 2024.
[10] M. Prakusu Aji, "Crypto Dynamics and Cybersecurity Policy in Indonesia as a Sociocultural Change in the Cyber Age", *Journal of Science*, Vol. 12, No. 3, pp. 2307–2315, 2023.
[11] M. Prakusu Aji, "Cybersecurity Systems and Data Sovereignty in Indonesia from a Political Economy Perspective (A Case Study for the Protection of Personal Data)", *Journal of the Legal Politician* , Vol. 13, No. 2, pp. 222–238, 2023.