

---

## THE IMPACT OF DIGITAL LITERACY ON PHISHING PREVENTION BEHAVIOUR: A LITERATURE REVIEW

**Nastiti Aura Istiqomah**

Universitas Airlangga, Surabaya, Indonesia

Email: nastiti.aura.istiqomah-2023@fisip.unair.ac.id

**Naza Aprilia Lorenza**

Universitas Airlangga, Surabaya, Indonesia

Email: naza.aprilia.lorenza-2023@fisip.unair.ac.id

**Fitri Mutia**

Universitas Airlangga, Surabaya, Indonesia

Email: fitri.mutia@fisip.unair.ac.id

---

Received: 04/03/2025

Revised: 21/10/2025

Accepted: 01/12/2025

---

**Abstract:** The advancement of technology has brought about ease and efficiency, but along with these benefits, a multitude of complexities and risks have also arisen. Among these complexities, threats to cyber security are of utmost concern. This paper zeros in on phishing as one of the most widespread forms of digital data theft. The aim of the paper is to explore the role of digital literacy in predicting phishing behavioral responses. The research methodologies employed in this study is systematised literature review (SLR) which incorporates the methodology of collecting, analysing and synthesising previous works in the field to develop research findings. This particular review focuses on 18 articles published between the years 2014 and 2024, the review indicates that digital literacy substantially influences individuals' capacity to prevent phising incidents. The various ramifications of phishing include monetary losses, social and security ramifications, damage to privacy and media information as well as psychological harm to the affected individuals. Phishing cybercrimes has been the primary reason for the digital literacy outreach initiatives to help the public improve their skills and understand the importance of protecting their data. Efforts to strengthen prevention may include integrating digital literacy into education curricula, conducting continuous employee training, and adopting AI-based detection systems.

---

Corresponding Author:

Nastiti Aura Istiqomah

Universitas Airlangga, Surabaya, Indonesia; nastiti.aura.istiqomah-2023@fisip.unair.ac.id



©2025 by the authors. Pustakaloka: Jurnal Kajian Informasi & Perpustakaan is licensed under a Creative Commons Attribution-NonCommercial\_ShareAlike 4.0 International License. <https://creativecommons.org/licenses/by-nc-sa/4.0/>

---

*Strengthening digital literacy in the outreach programs is essential to reducing the risk of phishing cybercrimes.*

**Keywords:** digital literacy; phishing prevention; cybersecurity

**Abstrak:** Perkembangan teknologi selain menawarkan kemudahan juga menghadirkan risiko dan tantangan. Ancaman keamanan siber adalah ancaman utama yang menjadi perhatian. Pada penelitian ini, memfokuskan pada kejahatan siber phishing yang merupakan kejahatan pencurian data yang kian marak. Tujuan penelitian ini adalah untuk menganalisis dampak literasi digital terhadap perilaku pencegahan phishing. Penelitian ini menggunakan metode Systematic Literature Review (SLR) yang digunakan untuk mengumpulkan, menganalisis, dan mengorganisasi artikel dari penelitian sebelumnya, yang kemudian diolah menjadi kesimpulan penelitian. Dari 18 artikel yang relevan dengan rentang tahun 2014-2024, menunjukkan bahwa literasi digital punya peran dalam pencegahan serangan phishing. Dampak phishing yang ditemukan meliputi kerugian finansial, dampak sosial, dampak privasi keamanan, dampak media informasi, hingga kerusakan mental pada korban. Dari artikel, upaya penyuluhan literasi digital dilakukan untuk meningkatkan kesadaran masyarakat terhadap kejahatan siber, menunjukkan peningkatan pemahaman dan keterampilan masyarakat dalam melindungi data pribadi. Upaya pencegahan ini dapat didukung melalui penambahan kurikulum literasi digital di bidang pendidikan, pelatihan rutin bagi karyawan, serta penggunaan AI untuk pencegahan phishing. Temuan ini menggarisbawahi pentingnya penguatan literasi digital sebagai strategi pencegahan kejahatan siber phishing.

**Kata kunci:** literasi digital; pencegahan *phishing*; keamanan siber

*How to Cite:*

Istiqomah, N. A., Lorenza, N. A., & Mutia, F. (2025). The Impact of Digital Literacy on Phishing Prevention Behaviour: A Literature Review. *Pustakaloka*, 17(2), 102-125. <https://doi.org/10.21154/pustakaloka.v17i2.10495>.

## **PENDAHULUAN**

According to data from the Badan Pusat Statistik, based on the results of the Susenas Survey, 66.48% of Indonesia's population had internet access in 2022.<sup>1</sup> The internet provides ease of access to various available digital applications and platforms; one can communicate in seconds, shop from anywhere, follow the latest news, and access education and healthcare online. Therefore, the internet has become an integral part of daily life. A study shows that the presence of the internet is shifting the paradigm of human life from

---

<sup>1</sup> Badan Pusat Statistik, *Statistik Telekomunikasi Indonesia 2022*, ed. oleh Teknologi Informasi dan Pariwisata Direktorat Statistik Keuangan (Badan Pusat Statistik, 2022), <https://www.bps.go.id/publication/2023/08/31/131385d0253c6aae7c7a59fa/statistik-telekomunikasi-indonesia-2022.html>.

physical reality to a new reality, namely the digital world.<sup>2</sup> The digital world offers convenience and efficiency, but it also presents a number of new risks and challenges, especially cybercrime. As technology advances rapidly, cybercrime has become a serious focus in Indonesia because it has reached alarming levels.<sup>3</sup>

According to a report from the Badan Siber dan Sandi Negara (BSSN), cybercrime in Indonesia increased by 30% compared to the previous year, with phishing being one of the most frequent cybercrimes.<sup>4</sup> Generally, phishers operate by sending messages to victims as if they are from official institutions or by sending messages containing links to obtain free data, shopping vouchers, and so on; however, these links actually direct victims to certain websites that make it easier for phishers to steal data, such as email accounts, phone numbers, bank account numbers, and even very important personal information.<sup>5</sup> For those who are not vigilant, they are likely to be persuaded and immediately click on the provided link without thinking twice.

According to Rompi & Muaja (2021), 67% of cybercrimes originate from phishing.<sup>6</sup> Limited digital literacy appears to be one of the underlying reasons behind such vulnerabilities.<sup>7</sup> Digital literacy extends beyond technical use of devices; it encompasses the cognitive skills to interpret, evaluate, and apply digital information critically and responsibly.<sup>8</sup> Through these cognitive abilities, society can build its critical thinking skills to evaluate the credibility of information, identify hidden motives in digital information, and be skeptical of temptations. Without this ability, even a technically proficient person can easily fall prey to phishing scams. Therefore, good digital literacy is very important to avoid the threat of phishing. In line with research by M. Syafii et al. (2024),

---

<sup>2</sup> Sindy Ariyaningsih dkk., "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi di Indonesia," *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1–11, <https://doi.org/10.56457/jjih.v1i1.38>.

<sup>3</sup> A. L. Sariani, "Efektivitas Penegakan Hukum terhadap Kejahatan Siber di Indonesia," *Al-Dalil* 2 (2023), <https://doi.org/10.58707/aldalil.v2i2.777>.

<sup>4</sup> Badan Siber dan Sandi Negara, *Laporan Tahunan Kejahatan Siber di Indonesia* (Badan Siber dan Sandi Negara, 2025).

<sup>5</sup> Rizky Fauziah, "Literasi Digital Kekinian Agar Komunikasi Lebih Bermakna," *Journal of Science and Social Research* 4, no. 2 (2021): 218, <https://doi.org/10.54314/jssr.v4i2.646>.

<sup>6</sup> Tonny Rompi dan Harly Stanly Muaja, "Tindak Kejahatan Siber di Sektor Jasa Keuangan dan Perbankan," *Lex Privatum* 9, no. 4 (2021): 183–92.

<sup>7</sup> Andi Asyhary J Arsyad dkk., "Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Literasi Digital: Studi Kasus di SMK Darussalam Makassar," *Jurnal Pengabdian Literasi Digital Indonesia* 3 (2024): 60–71, <https://doi.org/10.57119/abdimas.v3i2.122>.

<sup>8</sup> Rila Setyaningsih dkk., "Model of Strengthening Digital Literacy Through Utilization of E-Learning," *Journal of ASPIKOM* 3, no. 6 (2019): 1200, <https://doi.org/10.24329/aspikom.v3i6.333>.

awareness of the importance of digital literacy and cybersecurity is becoming an essential part of daily life.<sup>9</sup>

However, there are still many individuals with low digital literacy levels, making them vulnerable to phishing threats.<sup>10</sup> To address this, various educational efforts in digital literacy need to be implemented continuously. This increase in digital literacy aims to equip the public with the ability to recognize, avoid, and combat potential cyber crimes such as phishing, which is prevalent in Indonesia. As stated by Arigo et al. 2022, mastering the skills of digital literacy is valuable for community engagements on the internet so that the positive functions of the internet can be utilized for the benefits of smart and productive society. Therefore, this study aims to analyze the impact of digital literacy on phishing prevention behavior as one form of cybercrime threat prevalent among Indonesian society.<sup>11</sup>

The research is intended to contribute to the understanding of the importance of educating digital literacy to improve the public's digital skills, so that the public will be more educated and digitally responsive to the potential phishing threats on the internet. If society has a high level of digital literacy, it will impact their ability to prevent phishing cases in today's technological era. Society must be smart in handling and protecting personal data and sensitive information so that it is not easily exploited by irresponsible parties.

## **RESEACRH METHODS**

This review follows the Kitchenham framework, adapted from Pitrianti et al. (2023), as guide in systematically identifying, selecting, and synthesizing relevant studies.<sup>12</sup> This method allows researchers to collect, analyze, and organize articles from previous studies to obtain data. Next, this data is processed and used to draw conclusions about the research results. Here are the steps in conducting an SLR:

---

<sup>9</sup> M. Syafiih dkk., "Pendampingan Literasi Digital untuk Mengurangi Risiko Kejahatan Siber Membentuk Masyarakat yang Lebih Aman," *JILPI: Jurnal Ilmiah Pengabdian dan Inovasi* 2, no. 4 (2024): 1027–36, <https://doi.org/10.57248/jilpi.v2i4.456>.

<sup>10</sup> Arsyad dkk., "Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Literasi Digital: Studi Kasus di SMK Darussalam Makassar."

<sup>11</sup> Muhammad Arigo dkk., "Akibat Hukum Bagi Pelaku Tindak Pidana Penipuan Online Melalui Modus Arisan Online di Media Sosial Elektronik," *Jurnal Rectum* 4, no. 2 (2022): 182–90, <https://doi.org/10.46930/jurnalrectum.v4i2.1733>.

<sup>12</sup> Siti Pitrianti dkk., "Literasi Digital pada Masyarakat Desa," *Prosiding Seminar Nasional Teknologi dan Sistem Informasi* 3, no. 1 (2023): 43–49, <https://doi.org/10.33005/sitasi.v3i1.655>.

### 1) Planning

The researchers determined the main keywords related to the study, namely "digital literacy" and "phishing". These keywords will be used for searching articles on DOAJ, Google Scholar, Research Gate, Science Direct, and Scopus. In their search, the researchers used Boolean Logic as follows:

Table 1. Research Strategy

No	Database	Keyword
1.	DOAJ	digital literacy AND phishing
2.	Google Scholar	<ul style="list-style-type: none"><li>"digital literacy OR literasi digital" AND "phishing"</li><li>dampak phishing AND pentingnya literasi digital</li></ul>
3.	Research Gate	digital literacy AND phishing AND impact AND prevention behavior
4.	Science Direct	digital literacy AND phishing AND impact AND prevention behavior
5.	Scopus	digital literacy AND phishing AND impact AND prevention behavior

Source: Authors' data processing, 2025

Articles published in national and international scientific journals throughout the last ten years (2014–2024) are the only ones covered. The thoroughly investigated study also explores the connection between prevention of phishing attacks and digital literacy as a component of cybersecurity.

### 2) Implementation

Following the methodology of Shina et al. (2023).<sup>13</sup>, the research of this article uses the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flowchart to show the steps involved in screening and choosing included studies.

<sup>13</sup> Abhinav Sinha dkk., "Meta-Analysis on Plasmodium Falciparum Sulfadoxine-Pyrimethamine Resistance-Conferring Mutations in India Identifies Hot Spots for Genetic Surveillance," *International Journal of Antimicrobial Agents* 63, no. 3 (2024): 107071, <https://doi.org/10.1016/j.ijantimicag.2023.107071>.

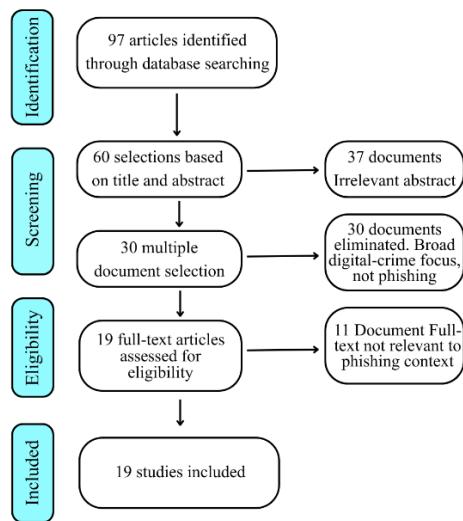


Figure 1. Data selection process with the PRISMA model

Source: Author's Data Processing (Shina et al., 2023)

At this stage, the researcher searches for relevant articles, identifies, and analyzes them. The search was conducted by entering search keywords into each target database. The results obtained were 97 relevant articles indexed in the last 10 years, from January 2014 to December 2024. Next, manual actions were taken by reviewing each relevant article by analyzing the abstract, introduction, and conclusion. The result obtained is 18 articles. To obtain articles that are relevant and aligned with the research focus, inclusion and exclusion criteria were applied and are explained in the following table.

Table 2. Inclusion and Exclusion Criteria

No.	Criteria	Inclusion	Exclusion
1.	Title and Abstract	The title and abstract are relevant to the context of phishing	Articles are not included if their title or abstract is not relevant to phishing.
2.	Research Focus	Research on cybercrime focusing on phishing and digital literacy	The article is excluded if the research does not specifically address phishing and digital literacy.
3.	Type of Publication	Scientific journal articles with full text are available and relevant to the context of phishing.	The article is excluded if its full-text document is not relevant to the phishing content.

Source: Authors' data processing, 2025

The included articles clearly describe the abstract and content of research findings on phishing and digital literacy. The articles are from scientific journals with full-text access. Conversely, articles will be excluded if they are not relevant and do not focus on phishing and digital literacy. This process allows authors to select appropriate and high-quality studies.

3) Report

Articles that meet the criteria based on the previous stage are analyzed and discussed through a synthesis scheme. The synthesis analysis process includes the importance of digital literacy and phishing prevention behavior.

## RESEARCH AND DISCUSSION

In today's digital environment, digital literacy stands as a core competency for confronting cybersecurity challenges, particularly phishing threats. According to research by Hariadi et al. (2024), digital literacy enables individuals to obtain accurate information, interact effectively, and maintain personal security from security risks such as hacking and identity theft.<sup>14</sup> Another study also states that understanding how to filter, evaluate, and use information wisely is very important because the information received can have a positive impact on everyone as a whole.<sup>15</sup> This is also supported by various articles that serve as references for this research, with 18 relevant articles found. Here is the table containing the results from the data findings obtained by the researcher:

**Table 3. Previous Research Data**

No	Title	Author	Year	Results
1.	Introducing Cybersecurity Awareness in a Digital Literacy Context	Mark Frydenberg and Birgy Lorenz	2020	Raising awareness of cybersecurity requires digital literacy skills, which include the capacity to distinguish phishing software and hardware from DDoS attacks and human factors. This awareness helps students understand serious impacts such as financial losses, service disruptions, reputational damage, and data theft, as well as how to address them.

<sup>14</sup> Muhaemin Hariadi dkk., "4 Pilar Literasi Digital yang Perlu Diketahui Masyarakat Desa Tugu Utara," *Jurnal Pengabdian Masyarakat Cendekia* 3 (2024): 240–47, <https://doi.org/10.62180/mxcxqv50>.

<sup>15</sup> Abd Rahim dan Mutiara Indah, "Pentingnya Pendidikan Literasi Digital di Kalangan Remaja," *Jurnal Pengabdian Masyarakat* 2, no. 2 (2024): 52.

2.	Digital Safety Assistance as a Precaution Against Digital Fraud in Sidomukti Mayang Village	Ulya Anisatur Rosyidah and Taufiq Timur Warisaji	2022	Phishing has become one of the various types of digital fraud experienced by the residents of Sidomukti Village, resulting in financial losses for the residents. Therefore, digital literacy assistance is provided to raise public awareness of digital scams.
3.	Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness	Musaddag Elrayah and Saima Jamil	2023	The increase in cybersecurity awareness, such as phishing, strengthens the relationship between digital literacy, online privacy, and cyber awareness. Awareness programs enhance users' decision-making abilities through knowledge about threats, the importance of strong passwords, and effective security measures. Social norms also influence safety behavior and user decisions.
4.	The Urgency of Digital Literacy in Social Media to Prevent Fraud in Islamic Banking	Susi Apriya, Wahyu Akbar, and Akhmad Jaki	2023	Unverified information on social media can be exploited by perpetrators for data manipulation and fraud. Therefore, digital literacy needs to be promoted to prevent phishing in Islamic banking. Although some social media platforms already provide fraud prevention content, further development is needed to attract public interest.
5.	Socialization of Healthy Internet on Social Media and Awareness of Phishing at SMPN 23 South Tangerang	Sofyan Mufti Prasetyo, Jefryanus Lemur, Andrea Firmansyah, Athaya Putri, Dafrosa Desi Udu, Doni Maulana, Lusius Dian Margareta, Yuantino Muhammad Syafiq, Widian Dwi Putra, and	2023	The community service activities at SMPN 23 South Tangerang successfully increased students' knowledge about healthy internet use on social media and awareness of phishing. The lack of digital literacy among students and the need for knowledge training to help them identify and steer clear of online scams that could jeopardize their security and privacy are the driving forces behind this activity.

---

Nando Bachtiar

6.	Police Strategies in Preventing Phishing Crimes through Social Media in Cyberspace	Rahmat Syah	2023	Phishing attacks can lead to identity theft, breaches of sensitive data, and financial losses that affect trust and stability in the online world. therefore, it is very important to raise user awareness about the dangers of phishing by teaching strategies regarding Education on how to recognize signs of an attack and self-protection measures.
7.	Digital Literacy for Personal Data Protection	Dwi Fajar Saputra	2023	Digital literacy encompasses instruction on spotting security threats, creating secure passwords, controlling application permissions, and avoiding phishing scams. Enhancing digital literacy can improve risk awareness and security practice implementation, as well as boost personal data protection.
8.	Analysis of Online Fraud Communication Networks through Social Media Whatsapp Messenger	Wahyuddin, Lutfiah F. Ersa, Gusti Aningsih, Taufik Hidayat, and Alam Febri Sonni	2024	Phishing via WhatsApp Messenger frequently takes advantage of links, visual iconography, and familiar connections to win over victims and steal their personal data. Avoiding online scams requires digital literacy because it makes it harder for people to be influenced to visit dangerous websites.
9.	Analysis of Online Phishing Crimes in Society	Kelas 4A4 and Octo Iskandar	2024	Phishing victims not only experience identity theft but also financial losses and mental damage. The lack of digital literacy is one of the main causes, as many people do not yet understand how phishing works and how to protect themselves from it.
10.	Education on Cyber Crime Trends at SMA Negeri 2 Baubau	Mashendra, Safrin Salam, Amrun Kahar, Eko S La Ode Muhammad	2024	Through digital literacy education outreach, high school students have shown an increased understanding of various cybercrimes, including phishing, hacking, online scams,

		Karim, Muhammad Sutri Masyah, Abdul Rahim, and Yayayn Serah	identity theft, malware attacks, and so on. With initial data showing that 28 or 93% of students did not know or recognize the types of cybercrimes in the online world.
11.	Increasing Teen Awareness of Phishing through Digital Literacy: A Case Study at SMK Darussalam Makassar	Andi Asyhary J. Arsyad, Usman Tamrin, Janisa Pascawati Lande, and Najirah Umar	2024 Digital literacy significantly contributes to preparing teenagers to face phishing threats. Digital literacy for teenagers is very important because teenagers often become targets of phishing and other cybercrimes. In addition, the importance of law enforcement against phishing perpetrators to reduce cybercrime rates.
12.	Training on Enhancing Digital Literacy, Safe Internet Use for the Rumah Harapan Karawang Foundation	Maolana Nopiansah, Silvia N. P. Erito, Dede Nurrahman, and Tri Haryati	2024 Digital literacy training helps most of the orphans at Yayasan Rumah Harapan Karawang recognize and avoid phishing. Participants learned useful skills during the course, including how to manage strong passwords, spot phishing scams, and comprehend privacy settings across many platforms.
13.	Teenagers' Behavior in Using the Internet to Recognize and Avoid Phishing at Muhammadiyah High School Pacitan	Sunardi, Murinto, Krisna Astianingrum, Baiq Nikum Yulisasih, and Salsabilla Azahra Putri	2024 The effectiveness of the community empowerment program in increasing students' knowledge on how to avoid phishing attacks. Seminars on teenage online usage and how to spot and steer clear of phishing were offered as part of the program.
14.	The Economic Impact Of Phishing, Vishing, Online Marketplaces, and Emerging Cybercrimes: Exposing the	Yoganandham Govindharaj	2024 Cybercrime such as phishing significantly impacts the economy, particularly in the online marketplace. The losses incurred by individuals and organizations are usually accompanied by long-term consequences. These attacks can cause customers to lose trust, reduce market share, and disrupt

---

---

	Cybercrime Economy and Social Costs in the Modern Era of Digital Fraud- An Assessment			business operations.
15.	Digital Literacy and Social Media Ethics Program for Students	Asep Hidayat, Rodhiyat Fajar Salim, Ilyas, and Fugiyar Suherman	2024	The low level of digital literacy makes students unaware of online risks such as phishing threats, and the lack of understanding of basic security and ethics in social media can increase vulnerability to cyber attacks, including the spread of misinformation and unhealthy interactions. Therefore, digital literacy is essential.
16.	Digital Data Security Education for Students of SMPN 32 Padang	Renny Permata Saputri, Monica Fransisca, and Yuliawati Yunus	2024	The lack of digital literacy among students makes them increasingly vulnerable to personal data exploitation through phishing. The addition of a digital literacy curriculum in the field of education is necessary to build understanding and awareness among students from an early age to prepare for digital challenges.
17.	Strategy for Increasing Public Awareness of Data and Information in the Digital Era	Rizki Agam Syahputra, Noer Octaviana Maliza, Kasmawati, and Cut Widya Aulia Putri	2024	Phishing threats can cause financial and personal harm. Therefore, it is very important to enhance digital literacy and public awareness about the urgency of protecting personal information, and it has proven effective as a resource for the community.
18.	Education on Protecting Personal Data While Using the Internet to Avoid Phishing Dangers in Pajang Village	Bekti Nugrahadi, Raditya Yoga Pratama, Agung Widiyanto Fajar Sutrisno, and Rosyadah Hafidz	2024	In facing technological advancements, high digital literacy is needed to enhance understanding and skills accurately, wisely, and safely. Phishing is one of the threats that can pose risks in the fields of business, government agencies, and users due to the misuse of sensitive data, loss of money and productivity, as well as social and

---

personal discomfort.

---

Source: Authors' data processing, 2025

The reviewed studies collectively reveal that phishing incurs multiple forms of impact, including:

A. Economic Impact and Financial Loss

Six articles demonstrate how phishing attacks cause financial loss and have an impact on the economy. For example, according to research by Rosyidah and Warisaji (2022), a lot of people in Sidomukti Mayang village experienced material and immaterial losses as a result of falling victim to digital fraud, including phishing.<sup>16</sup> Research by Syahputra et al. (2024) also demonstrates how the threat of phishing can negatively impact people's finances and personal lives.<sup>17</sup> Additionally, the research presented by Govindharaj (2024) explains that phishing has a significant impact on the economy, particularly in the marketplace.<sup>18</sup>

Phishing frequently targeted individuals or businesses, leading to direct financial losses via bank account theft, fraudulent transactions, and the theft of private financial data. E-commerce platforms are also susceptible to financial losses as a result of fraudsters abusing them to carry out illicit transactions that lead to chargebacks. This is consistent with Carter's (2025) research, which claims that online fraud has a systemic impact on the economy that affects growth and stability by impeding digital financial inclusion and causing financial market losses.<sup>19</sup> Syah (2023) highlights that phishing attacks have detrimental impacts because it results in financial losses, and the revelation of personal information.<sup>20</sup>

Nugrahadi et al. (2024) make a similar point, claiming that phishing attacks are a significant risk to internet use because they can lead to social

---

<sup>16</sup> Ulya Anisatur Rosyidah dan Taufiq Timur Warisaji, "Pendampingan Digital Safety sebagai Precaution Penipuan Digital di Desa Sidomukti Mayang," *Abdimastek* 1, no. 2 (2022): 83–89.

<sup>17</sup> Rizki Agam Syahputra dkk., "Strategi Peningkatan Kesadaran Data dan Informasi Masyarakat di Era Digital," *Jurnal Pengabdian kepada Masyarakat Nusantara (JPkMN)* 5, no. 3 (2024): 3164–71, <https://doi.org/10.55338/jpkmn.v5i3.3543>.

<sup>18</sup> Yoganandham Govindharaj, "The Economic Impact of Phishing, Vishing, Online Marketplaces, and Emerging Cybercrimes: Exposing the Cybercrime Economy and Social Costs in the Modern Era of Digital Fraud - An Assessment," *GIS Science Journal* 11, no. 9 (2024): 215.

<sup>19</sup> W. Carter, "The Economic Impact of Online Fraud: A Review," *Preprints*, advance online publication, 2025, <https://doi.org/10.20944/preprints202507.0436.v1>.

<sup>20</sup> Rahmat Syah, "Strategi Kepolisian dalam Pencegahan Kejahatan Phising Melalui Media Sosial di Ruang Siber," *Jurnal Impresi Indonesia* 2, no. 9 (2023): 864–70, <https://doi.org/10.58344/jii.v2i9.3594>.

and personal discomfort, as well as the exploitation of private information and financial and productivity losses.<sup>21</sup> Developing awareness of cybersecurity requires an understanding of the implications of digital literacy. Problems with awareness can affect the impact of Distributed Denial of Service (DDoS) attacks, hardware, software, and human components of cybersecurity such as phishing. As a result, this also impacts financial losses since it may lower a company's or institution's revenue.<sup>22</sup> In similar lines, Cobos & Cakir's (2024) research demonstrates that the economic impacts of cyberattacks go well beyond financial losses, including indirect charges and substantial long-term reaction costs. Therefore, understanding the economic impact of cybercrime is crucial to ensuring the cybersecurity space remains protected from major threats.<sup>23</sup>

#### B. Social Impact

According to seven relevant articles, phishing's social impact relates to harm to one's reputation and a drop in public trust. For example, research by Frydenberg & Lorenz (2020) show that cyber attacks like phishing have the ability to steal data, interrupt services, and harm a company's brand.<sup>24</sup> Similarly, phishing undermines merchants' trust, damages consumer confidence and brand image, lowers user engagement and market share, and may even hurt a company's ability to compete.<sup>25</sup> According to another study, phishing can result in the exploitation of private information, financial losses, decreased productivity, and social and personal impact, making it potentially dangerous for businesses, government agencies, and users.<sup>26</sup> In similar lines, Gopalan & Devi's (2025) research shows that cyber security incidents can undermine customer confidence in digital banking in India in addition to causing financial and reputational harm. As a result, raising

---

<sup>21</sup> Bekti Nugrahadi dkk., "Edukasi Menjaga Data Pribadi dalam Menggunakan Internet untuk Menghindari Bahaya Phishing di Kelurahan Pajang," *Jurnal Pengabdian Masyarakat Bangsa* 2, no. 10 (2024): 4549–53, <https://doi.org/10.59837/jpmba.v2i10.1756>.

<sup>22</sup> Mark Frydenberg dan Birgy Lorenz, *Introducing Cybersecurity Awareness in a Digital Literacy Context*, 18 (2020): 33–45.

<sup>23</sup> Estefania Vergara Cobos dan Selcen Cakir, *A Review of the Economic Costs of Cyber Incidents* (World Bank Group, 2024).

<sup>24</sup> Frydenberg dan Lorenz, *Introducing Cybersecurity Awareness in a Digital Literacy Context*.

<sup>25</sup> Govindharaj, "The Economic Impact of Phishing, Vishing, Online Marketplaces, and Emerging Cybercrimes: Exposing the Cybercrime Economy and Social Costs in the Modern Era of Digital Fraud - An Assessment."

<sup>26</sup> Nugrahadi dkk., "Edukasi Menjaga Data Pribadi dalam Menggunakan Internet untuk Menghindari Bahaya Phishing di Kelurahan Pajang."

cybersecurity literacy and awareness is essential to reducing risks and fostering trust, which will promote the long-term expansion of online banking services in India.<sup>27</sup>

Phishing crimes are becoming increasingly dangerous, especially in the banking sector, due to psychological factors, weak privacy protection, and a lack of user awareness. Efforts to raise public awareness are necessary, similar to the study by Apriya et al. (2023), as done through social media for fraud prevention education, especially in Islamic banking.<sup>28</sup> A creative approach is expected to increase public interest and build a positive image of banking. Social media is often used for communication and team collaboration, but users are vulnerable to phishing attacks due to negligence. These attacks can lead to identity theft, data breaches, and financial losses, which have the potential to undermine stability and trust in the digital realm.<sup>29</sup> According to a related study by Tian et al. (2023), phishing attacks can harm an organization's reputation in addition to causing financial losses and privacy violations. Public faith financial losses and and privacy violations. Public faith in digital institutions, which mostly depend on reliability and corporate image, may be indirectly undermined by this reputational harm. The study also shows that employees in the financial industry are more susceptible to reciprocity-based phishing attacks because they are more likely to accept requests that seem like genuine business transactions due to a transactional work culture and a strong desire to uphold their professional reputation and social credit.<sup>30</sup>

Therefore, cybersecurity awareness is very important because it influences individual behavior within the social context and norms of the community. According to research by Elrayah & Jamil (2023), awareness of cyber threats, such as phishing, can enhance digital literacy, online privacy

---

<sup>27</sup> P. Sathya Devi Gopalan, "The Impact of Cyber Security Awareness on Customers' Trust and Adoption of Internet Banking in Palakkad District, Kerala," *IJIRT: International Journal of Innovative Research in Technology* 11, no. 12 (2025): 6418-26.

<sup>28</sup> Susi Apriya dkk., "The Urgency of Digital Literacy in Social Media to Prevent Fraud in Islamic Banking," *SERAMBI: Jurnal Ekonomi Manajemen Dan Bisnis Islam* 5, no. 3 (2023): 135-54, <https://doi.org/10.36407/serambi.v5i3.1118>.

<sup>29</sup> Syah, "Strategi Kepolisian dalam Pencegahan Kejahatan Phising Melalui Media Sosial di Ruang Siber."

<sup>30</sup> Annie Chuan Tian dkk., "Phishing Susceptibility Across Industries: The Differential Impact of Influence Techniques," *Computers & Security* 135 (2023): 103487, <https://doi.org/10.1016/j.cose.2023.103487>.

concern, and security awareness.<sup>31</sup> The impact of social norms also influences safety behavior and decision-making. Because by educating people about cyberthreats, the value of strong passwords, how to spot phishing, and practical security measures, cybersecurity awareness programs can assist users in making better decisions. A society with a high level of cybersecurity awareness is undoubtedly well-versed in digital literacy, which will impact its social environment in terms of beliefs, understanding, and behavior.<sup>32</sup> This is supported by research by Phan et al. (2025), which indicates that a greater understanding of cybersecurity on an individual basis will promote good attitudes and safe digital conduct. Furthermore, vulnerabilities that usually take advantage of user's low level of digital literacy are known to decrease with improved security knowledge.<sup>33</sup>

### C. Impact on Mental Health

Mental harm caused by depression is one of the major impacts that phishing victims face.<sup>34</sup> Due to the theft of their personal information, this condition is brought on by severe tension and anxiety. In a field research of 480 employees at a corporation, it was discovered that employees who successfully reported the phishing threat had lower stress levels than employees who fell victim to phishing by clicking on phishing links.<sup>35</sup> This study demonstrates how phishing causes psychological reactions that have an impact on mental health. In more severe situations, particularly when extremely private information is misused, victims may experience PTSD (Post-Traumatic Stress Disorder), which manifests as persistent feelings of

---

<sup>31</sup> Musaddag Elrayah dan Saima Jamil, "Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness," *International Journal of Cyber Criminology* 17, no. 2 (2023): 166–87, <https://doi.org/10.5281/zenodo.4766711>.

<sup>32</sup> Krisna Astianingrum dkk., "Perilaku Remaja Dalam Menggunakan Internet Untuk Mengenali dan Mengindari Phishing pada SMA Muhammadiyah Pacitan," *Jurnal Ahsana Penelitian dan Pengabdian Kepada Masyarakat* 2, no. 3 (2024): 70–78, <https://doi.org/10.59395/ahsana.v2i3.367>.

<sup>33</sup> Bao Trung Phan dkk., "The Impact of Digital Literacy on Personal Information Security: Evidence from Vietnam," *Proceedings of the International Conference on Emerging Challenges: Sustainable Strategies in the Data-Driven Economy (ICECH 2024)*, Atlantis Press International BV, 2025, <https://doi.org/10.2991/978-94-6463-694-9>.

<sup>34</sup> Octo Iskandar, "Analisis Kejahatan Online Phishing pada Masyarakat," *Leuser: Jurnal Hukum Nusantara* 1, no. 2 (2024): 32–36.

<sup>35</sup> M. Schops dkk., "Simulated Stress: A Case Study of a Simulated Phishing Campaign on Employees' Perception, Stress and Self-Efficacy," *USENIX Conference Proceedings*, 2024.

threat, trouble sleeping, and reliving those upsetting moments.<sup>36</sup> As a result, the impact on mental health may be more profound and persistent than just financial losses.

#### D. Impact on Privacy and Security

According to Prasetyo et al. (2023), healthy internet socialization at SMPN 23 South Tangerang aims to protect students' personal and financial information.<sup>37</sup> This activity is caused by the low level of digital literacy among students, while phishing threats require education so that students can recognize and avoid online scams that can damage their privacy and security. Research by Nugroho et al. (2023), which offers digital security education linked to phishing links and covers everything from characteristics to actions to take when encountering a phishing link, further supports the significance of education among students.<sup>38</sup> It is anticipated that students will be able to actively contribute to safeguarding the security of their personal data through this outreach. Therefore, raising public awareness of phishing requires digital literacy.

Furthermore, Saputra (2023), in his research, explains that digital literacy is knowing how to identify security risks, making secure passwords, controlling application permissions, and avoiding phishing.<sup>39</sup> Improving security procedures and increasing risk awareness are both impacted by increased digital literacy. A study that demonstrates a good correlation between digital literacy and the public's ability to identify cyberthreats like phishing supports this. According to a study by Fadya (2025), people with strong digital literacy abilities are typically better at spotting phishing emails by looking for irregularities in the sender's address, grammatical mistakes, and irrational data requests.<sup>40</sup> To stop data theft, these actions are essential.

---

<sup>36</sup> F. P. E. P. Putra dkk., "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study," *Brilliance: Research of Artificial Intelligence* 4, no. 1 (2024), <https://doi.org/10.47709/brilliance.v4i1.4357>.

<sup>37</sup> S. M. Prasetyo dkk., "Sosialisasi Internet Sehat pada Sosial Media dan Waspada terhadap Phishing di SMPN 23 Tangerang Selatan," *APPA: Jurnal Pengabdian kepada Masyarakat* 1, no. 4 (2023): 248–51.

<sup>38</sup> Nugrahadi dkk., "Edukasi Menjaga Data Pribadi dalam Menggunakan Internet untuk Menghindari Bahaya Phishing di Kelurahan Pajang."

<sup>39</sup> Dwi Fajar Saputra, "Literasi Digital untuk Perlindungan Data Pribadi," *Jurnal Ilmu Kepolisian* 17, no. 3 (2023): 1–8.

<sup>40</sup> A. R. Fadya, "Peran Literasi Digital dalam Meningkatkan Kesadaran Keamanan Siber di Kalangan Pengguna Internet" (Universitas Widyaatama, 2025).

### E. Impact on Information Media

According to research by Hidayat et al. (2024) , the low level of student literacy, such as understanding security and ethics on social media, increases vulnerability to cybercrime and makes them unaware of online risks like phishing, leading to the spread of misinformation and unhealthy interactions.<sup>41</sup> Similar research by Saputri et al. (2024) also explains that the lack of digital literacy in cybersecurity among college students makes them vulnerable to data exploitation cases.<sup>42</sup> Consequently, phishing prevention requires digital literacy. This is supported by research, the research demonstrates that individuals with high levels of digital literacy will recognize cyberthreats like phishing and will comprehend the need of safeguarding personal information.

In the context of social media, the study conducted by Wahyuddin et al. (2024) also highlights phishing carried out on WhatsApp Messenger.<sup>43</sup> The phishers carried out their actions by sending links in the form of invitations and messages that appeared to come from official institutions. The victim is directed to a website that has been altered by the phisher when they click on the link. In addition to losing their own data, the victim unintentionally propagated the malicious link and aided in the wider spread of false information by automatically sharing the link with their acquaintances. Many WhatsApp users are susceptible to phony messages due to their lack of digital literacy and knowledge of digital security systems.<sup>44</sup>

Phishers use social media sites like Facebook, Twitter, LinkedIn, and even Instagram to disseminate links by imitating official entities in addition to sending messages over WhatsApp.<sup>45</sup> This certainly affects the credibility of information media as a source of information that often lacks information resilience. Education, mindset, and social interactions are influenced by

---

<sup>41</sup> Asep Hidayat dkk., "Program Literasi Digital dan Etika Media Sosial Bagi Pelajar," *Jurnal Pendidikan Teknologi dan Bisnis* 6, no. 1 (2024): 63–70, <https://doi.org/10.36555/jptb.v6i1.2288>.

<sup>42</sup> Renny Permata Saputri dkk., "Edukasi Keamanan Data Digital pada Siswa SMPN 32 Padang," *Jurnal Pengabdian dan Inovasi Pendidikan Masyarakat* 1, no. 2 (2024): 99–107.

<sup>43</sup> Lutfiah Firdausiah Ersa Wahyuddin dkk., "Analisis Jaringan Komunikasi Penipuan Online melalui Media Sosial WhatsApp Messenger," *Jurnal Netnografi Komunikasi* 2, no. 2 (2024): 33–50, <https://doi.org/10.59408/jnk.v2i2.27>.

<sup>44</sup> A. Trianurahmah dkk., "Analisis Ancaman Phishing melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspadai Maraknya Kejahatan Phishing dengan Modus Berbasis Link," *Orbit: Jurnal Ilmu Multidisiplin Nusantara* 1, no. 2 (2024), <https://doi.org/10.63217/orbit.v1i2.81>.

<sup>45</sup> Ardiansyah I. Rustam dan A. Saudi, "Dampak Hukum Siber terhadap Privasi Data Pribadi di Indonesia," *Jurnal Hukum dan Kewarganegaraan* 6, no. 12 (2024).

digital literacy, making it an important skill for society to avoid misinformation, which can have widespread impacts.

Seeing the impacts caused as explained above, that digital literacy is important in preventing cybercrime, including phishing. Mashendra et al. (2024) in their research conducted an outreach program on digital literacy.<sup>46</sup> Data shows that 93% of 30 students do not know about cybercrime, and this activity was conducted alongside cybercrime education counseling. In line with the research conducted by Arsyad, et al. (2024), 80% of 227 respondents agreed that digital

literacy can influence the reduction of phishing crime impacts.<sup>47</sup> With digital literacy, it enhances personal abilities to combat threats and protect accounts on the internet. This training has many benefits and positive effects.<sup>48</sup>

In addition to providing instructions, training, and socialization about the importance of digital literacy and how to maintain the security of personal digital data to prevent phishing, there are several ways to avoid phishing, including:

1. Providing a digital literacy learning curriculum in the field of education.

In the digital era, the younger generation must be educated about cyber threats and how to handle them. Besides basic literacy in reading and writing, students should also understand digital literacy skills. This is also supported by research by Luic et al. (2022), which shows that the participants do have a basic understanding of digital literacy, but there is still a lot of ignorance that makes them vulnerable to cyber attacks.<sup>49</sup>

The students agreed to add digital literacy subjects to the school curriculum to enhance their knowledge.

2. Providing regular training on digital security to employees in an organization or company.

---

<sup>46</sup> M. Mashendra dkk., "Edukasi Trend Kejahatan Cyber pada SMA Negeri 2 Baubau," *Journal of Community Development* 5 (2024): 333–39, <https://doi.org/10.47134/comdev.v5i2.291>.

<sup>47</sup> Arsyad dkk., "Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Literasi Digital: Studi Kasus di SMK Darussalam Makassar."

<sup>48</sup> Maolana Nopiansah dkk., "Pelatihan Peningkatan Literasi Digital dan Pemanfaatan Internet yang Aman bagi Yayasan Rumah Harapan Karawang," *PRAWARA: Jurnal Abdimas* 3, no. 3 (2024): 89–94, <https://doi.org/10.63297/abdimas.v3i3.103>.

<sup>49</sup> Ljerka Luic dkk., *Economic and Social Development (Book of Proceedings)*, 78th International Scientific Conference on Economic and Social Development, dalam *Economic and Social Development* (2022), <http://www.esd-conference.com>.

Employees need further and more in-depth training on cybercrime, such as how to handle suspicious incoming emails and messages and what appropriate steps can be taken when a phishing attack occurs. This training is certainly aimed at making employees more proactive in maintaining the security of the company's information. As stated by Wibowo & Hidayat (2024), it is recommended that organizations provide stronger training and conduct it regularly using supporting software to enhance employee performance in addressing and reducing the risk of cybercrime.<sup>50</sup>

3. Using the assistance of Artificial Intelligence (AI) technology in identification for phishing prevention

Using Artificial Intelligence (AI) technology to help detect phishing and thus prevent phishing crimes from occurring. In a study, it was concluded that AI-based email classification systems are essential for addressing the increasingly complex threats of spam and phishing. With advanced AI techniques, spam and phishing can be effectively filtered, but technical and ethical challenges must still be considered. With the right approach, this system can protect internet users from cyber threats, and its development is an important step in maintaining the security of digital communication.<sup>51</sup>

## CLOSING

The synthesis of reviewed studies suggests that digital literacy meaningfully shapes individuals' awareness and behavioral responses toward phishing prevention. Digital literacy influences the increase of individual awareness to recognize, avoid, and prevent phishing attacks. Considering that there will be 5 major impacts from phishing crimes based on the results of this study, including 6 articles discussing the economic impact and financial loss, 7 articles addressing the social impact, and impacts on mental health, privacy and security, and information media. Thus, strengthening digital literacy becomes a

---

<sup>50</sup> Budi Wibowo dan Taufik Hidayat, "Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ," *Jurnal Pengabdian Masyarakat Sultan Indonesia* 2, no. 1 (2024): 1–9, <https://doi.org/10.58291/abdisultan.v2i1.294>.

<sup>51</sup> Kgs M Syarif Hidayatullah dan Tata Sutabri, "Pengembangan Sistem Pengklasifikasi E-Mail Berbasis Kecerdasan Buatan untuk Deteksi Spam dan Phishing," *Indonesian Journal of Multidisciplinary* 2, no. 2 (2024): 351–57.

key strategy for individuals to protect their personal data and minimize the impact of phishing crimes.

Drawing from the findings, two key implications emerge: (1) practical implications and (2) directions for future research:

a. Practical Implications.

- 1) For educators: to integrate the digital literacy curriculum at every educational level to build understanding of cybercrime.
- 2) For corporations or organizations: to provide ongoing cybersecurity training for employees and make use of AI tools to help identify and prevent phishing attempts.

**Implications for Future Research** These findings open opportunities for broader and more focused studies. One potential direction is to adopt more in-depth qualitative methods that allow researchers to observe and understand individual experiences directly, giving richer insight into how people navigate cybersecurity risks in real life. Additionally, expanding the research participants beyond students to include professionals who interact frequently with digital systems.

This study is not without limitations. The review only covered articles published within a specific time range and did not include a deeper evaluation of each study's quality. As a result, there may be publication or methodological biases that influence the findings. To strengthen future research, it will be important to broaden the range of data sources and use more rigorous quality assessment methods when selecting studies.

## **REFERENCE**

- Apriya, Susi, Wahyu Akbar, dan Akhmad Jaki. "The Urgency of Digital Literacy in Social Media to Prevent Fraud in Islamic Banking." *SERAMBI: Jurnal Ekonomi Manajemen Dan Bisnis Islam* 5, no. 3 (2023): 135–54. <https://doi.org/10.36407/serambi.v5i3.1118>.
- Ariyaningsih, Sindy, A. Ari Andrianto, Adri Surya Kusuma, dan Rina Arum Prastyanti. "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi di Indonesia." *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1–11. <https://doi.org/10.56457/jjih.v1i1.38>.
- Arsyad, Andi Asyhary J, Usman Tamrin, Janisa Pascawati Lande, dan Najirah Umar. "Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Literasi Digital: Studi Kasus di SMK Darussalam Makassar." *Jurnal*

*Pengabdian Literasi Digital Indonesia* 3 (2024): 60–71.  
<https://doi.org/10.57119/abdimas.v3i2.122>.

Astianingrum, Krisna, Baiq Nikum Yulisasih, dan Salsabilla Azahra Putri. “Perilaku Remaja Dalam Menggunakan Internet Untuk Mengenali dan Mengindari Phishing pada SMA Muhammadiyah Pacitan.” *Jurnal Ahsana Penelitian dan Pengabdian Kepada Masyarakat* 2, no. 3 (2024): 70–78. <https://doi.org/10.59395/ahsana.v2i3.367>.

Badan Pusat Statistik. *Statistik Telekomunikasi Indonesia* 2022. Disunting oleh Teknologi Informasi dan Pariwisata Direktorat Statistik Keuangan. Badan Pusat Statistik, 2022. <https://www.bps.go.id/id/publication/2023/08/31/131385d0253c6aae7c7a59fa/statistik-telekomunikasi-indonesia-2022.html>.

Badan Siber dan Sandi Negara. *Laporan Tahunan Kejahanan Siber di Indonesia*. Badan Siber dan Sandi Negara, 2025.

Carter, W. “The Economic Impact of Online Fraud: A Review.” *Preprints*, advance online publication, 2025. <https://doi.org/10.20944/preprints202507.0436.v1>.

Cobos, Estefania Vergara, dan Selcen Cakir. *A Review of the Economic Costs of Cyber Incidents*. World Bank Group, 2024.

Elrayah, Musaddag, dan Saima Jamil. “Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness.” *International Journal of Cyber Criminology* 17, no. 2 (2023): 166–87. <https://doi.org/10.5281/zenodo.4766711>.

Fadya, A. R. “Peran Literasi Digital dalam Meningkatkan Kesadaran Keamanan Siber di Kalangan Pengguna Internet.” Universitas Widyaatama, 2025.

Fauziah, Rizky. “Literasi Digital Kekinian Agar Komunikasi Lebih Bermakna.” *Journal of Science and Social Research* 4, no. 2 (2021): 218. <https://doi.org/10.54314/jssr.v4i2.646>.

Frydenberg, Mark, dan Birgy Lorenz. *Introducing Cybersecurity Awareness in a Digital Literacy Context*. 18 (2020): 33–45.

Gopalan, P. Sathya Devi. “The Impact of Cyber Security Awareness on Customers’ Trust and Adoption of Internet Banking in Palakkad District, Kerala.” *IJIRT: International Journal of Innovative Research in Technology* 11, no. 12 (2025): 6418–26.

Govindharaj, Yoganandham. “The Economic Impact of Phishing, Vishing, Online Marketplaces, and Emerging Cybercrimes: Exposing the Cybercrime

- Economy and Social Costs in the Modern Era of Digital Fraud - An Assessment." *GIS Science Journal* 11, no. 9 (2024): 215.
- Hariadi, Muhaemin, Ivana Ismia, Putri Aisah Adhetia, dkk. "4 Pilar Literasi Digital yang Perlu Diketahui Masyarakat Desa Tugu Utara." *Jurnal Pengabdian Masyarakat Cendekia* 3 (2024): 240–47. <https://doi.org/10.62180/mxcxqv50>.
- Hidayat, Asep, Rodhiyat Fajar Salim, dan Fugiyar Suherman. "Program Literasi Digital dan Etika Media Sosial Bagi Pelajar." *Jurnal Pendidikan Teknologi dan Bisnis* 6, no. 1 (2024): 63–70. <https://doi.org/10.36555/jptb.v6i1.2288>.
- Hidayatullah, Kgs M Syarif, dan Tata Sutabri. "Pengembangan Sistem Pengklasifikasi E-Mail Berbasis Kecerdasan Buatan untuk Deteksi Spam dan Phishing." *Indonesian Journal of Multidisciplinary* 2, no. 2 (2024): 351–57.
- Iskandar, Octo. "Analisis Kejahatan Online Phishing pada Masyarakat." *Leuser: Jurnal Hukum Nusantara* 1, no. 2 (2024): 32–36.
- Luic, Ljerka, Ivana Martincevic, dan Vesna Sesa. *Economic and Social Development (Book of Proceedings), 78th International Scientific Conference on Economic and Social Development*. Dalam *Economic and Social Development*. 2022. <http://www.esd-conference.com>.
- Mashendra, M., S. Salam, dan A. Kahar. "Edukasi Trend Kejahatan Cyber pada SMA Negeri 2 Baubau." *Journal of Community Development* 5 (2024): 333–39. <https://doi.org/10.47134/comdev.v5i2.291>.
- Muhammad Arigo, Marnasar Tambunan, dan Gomgom T.P Siregar. "Akibat Hukum Bagi Pelaku Tindak Pidana Penipuan Online Melalui Modus Arisan Online di Media Sosial Elektronik." *Jurnal Rectum* 4, no. 2 (2022): 182–90. <https://doi.org/10.46930/jurnalrectum.v4i2.1733>.
- Nopiansah, Maolana, N.P Silvia Erito, Dede Nurrahman, dan Tri Haryati. "Pelatihan Peningkatan Literasi Digital dan Pemanfaatan Internet yang Aman bagi Yayasan Rumah Harapan Karawang." *PRAWARA: Jurnal Abdimas* 3, no. 3 (2024): 89–94. <https://doi.org/10.63297/abdimas.v3i3.103>.
- Nugrahadi, Bekti, Raditya Yoga Pratama, Agung Widiyanto, dan Fajar Sutrisno. "Edukasi Menjaga Data Pribadi dalam Menggunakan Internet untuk Menghindari Bahaya Phishing di Kelurahan Pajang." *Jurnal Pengabdian Masyarakat Bangsa* 2, no. 10 (2024): 4549–53. <https://doi.org/10.59837/jpmba.v2i10.1756>.
- Phan, Bao Trung, Phuong Huyen Do, dan Da Quynh Le. "The Impact of Digital Literacy on Personal Information Security: Evidence from Vietnam." *Proceedings of the International Conference on Emerging Challenges: Sustainable*

- Strategies in the Data-Driven Economy (ICECH 2024)*, Atlantis Press International BV, 2025. <https://doi.org/10.2991/978-94-6463-694-9>.
- Pitrianti, Siti, Eliyah A. M. Sampetoding, Arini Anestesia Purba, dan Yulita Sirinti Pongtambing. "Literasi Digital pada Masyarakat Desa." *Prosiding Seminar Nasional Teknologi dan Sistem Informasi* 3, no. 1 (2023): 43–49. <https://doi.org/10.33005/sitasi.v3i1.655>.
- Prasetyo, S. M., A. Firmansyah, dan A. Putri. "Sosialisasi Internet Sehat pada Sosial Media dan Waspada terhadap Phishing di SMPN 23 Tangerang Selatan." *APPA: Jurnal Pengabdian kepada Masyarakat* 1, no. 4 (2023): 248–51.
- Putra, F. P. E. P., Ubaidi, A. Zulfikri, G. Arifin, dan R. M. Ilhamsyah. "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study." *Brilliance: Research of Artificial Intelligence* 4, no. 1 (2024). <https://doi.org/10.47709/brilliance.v4i1.4357>.
- Rahim, Abd, dan Mutiara Indah. "Pentingnya Pendidikan Literasi Digital di Kalangan Remaja." *Jurnal Pengabdian Masyarakat* 2, no. 2 (2024): 52.
- Rompi, Tonny, dan Harley Stanly Muaja. "Tindak Kejahatan Siber di Sektor Jasa Keuangan dan Perbankan." *Lex Privatum* 9, no. 4 (2021): 183–92.
- Rosyidah, Ulya Anisatur, dan Taufiq Timur Warisaji. "Pendampingan Digital Safety sebagai Precaution Penipuan Digital di Desa Sidomukti Mayang." *Abdimastek* 1, no. 2 (2022): 83–89.
- Rustam, Ardiansyah I., dan A. Saudi. "Dampak Hukum Siber terhadap Privasi Data Pribadi di Indonesia." *Jurnal Hukum dan Kewarganegaraan* 6, no. 12 (2024).
- Saputra, Dwi Fajar. "Literasi Digital untuk Perlindungan Data Pribadi." *Jurnal Ilmu Kepolisian* 17, no. 3 (2023): 1–8.
- Saputri, Renny Permata, Monica Fransisca, dan Yuliawati Yunus. "Edukasi Keamanan Data Digital pada Siswa SMPN 32 Padang." *Jurnal Pengabdian dan Inovasi Pendidikan Masyarakat* 1, no. 2 (2024): 99–107.
- Sariani, A. L. "Efektivitas Penegakan Hukum terhadap Kejahatan Siber di Indonesia." *Al-Dalil* 2 (2023). <https://doi.org/10.58707/aldalil.v2i2.777>.
- Schops, M., M. Gutfleisch, E. Wolter, dan M. A. Sasse. "Simulated Stress: A Case Study of a Simulated Phishing Campaign on Employees' Perception, Stress and Self-Efficacy." *USENIX Conference Proceedings*, 2024.
- Setyaningsih, Rila, Abdullah Abdullah, Edy Prihantoro, dan Hustinawaty Hustinawaty. "Model of Strengthening Digital Literacy Through Utilization of E-Learning." *Journal of ASPIKOM* 3, no. 6 (2019): 1200. <https://doi.org/10.24329/aspikom.v3i6.333>.

- Sinha, Abhinav, Sonalika Kar, Charu Chauhan, Chander Prakash Yadav, dan Lokesh Kori. "Meta-Analysis on Plasmodium Falciparum Sulfadoxine-Pyrimethamine Resistance-Conferring Mutations in India Identifies Hot Spots for Genetic Surveillance." *International Journal of Antimicrobial Agents* 63, no. 3 (2024): 107071. <https://doi.org/10.1016/j.ijantimicag.2023.107071>.
- Syafiih, M., Nadiyah, Matlubul Khairi, Moh. Furqan, dan Beny Yusman. "Pendampingan Literasi Digital untuk Mengurangi Risiko Kejahatan Siber Membentuk Masyarakat yang Lebih Aman." *JILPI: Jurnal Ilmiah Pengabdian dan Inovasi* 2, no. 4 (2024): 1027–36. <https://doi.org/10.57248/jilpi.v2i4.456>.
- Syah, Rahmat. "Strategi Kepolisian dalam Pencegahan Kejahatan Phising melalui Media Sosial di Ruang Siber." *Jurnal Impresi Indonesia* 2, no. 9 (2023): 864–70. <https://doi.org/10.58344/jii.v2i9.3594>.
- Syahputra, Rizki Agam, Noer Octaviana Maliza, dan Cut Widya Aulia Putri. "Strategi Peningkatan Kesadaran Data dan Informasi Masyarakat di Era Digital." *Jurnal Pengabdian kepada Masyarakat Nusantara (JPkMN)* 5, no. 3 (2024): 3164–71. <https://doi.org/10.55338/jpkmn.v5i3.3543>.
- Tian, Annie Chuan, Matthew L. Jensen, dan Alexandra Durcikova. "Phishing Susceptibility Across Industries: The Differential Impact of Influence Techniques." *Computers & Security* 135 (2023): 103487. <https://doi.org/10.1016/j.cose.2023.103487>.
- Trianurahmah, A., A. Fauzi, E. N. Tyas, M. A. Suryanto, M. Rizky, dan P. Wibisono. "Analisis Ancaman Phishing melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspadai Maraknya Kejahatan Phishing dengan Modus Berbasis Link." *Orbit: Jurnal Ilmu Multidisiplin Nusantara* 1, no. 2 (2024). <https://doi.org/10.63217/orbit.v1i2.81>.
- Wahyuddin, Lutfiah Firdausiah Ersa, Gusti Aningsih, Taufik Hidayat, dan Alem Febri Sonni. "Analisis Jaringan Komunikasi Penipuan Online melalui Media Sosial WhatsApp Messenger." *Jurnal Netnografi Komunikasi* 2, no. 2 (2024): 33–50. <https://doi.org/10.59408/jnk.v2i2.27>.
- Wibowo, Budi, dan Taufik Hidayat. "Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ." *Jurnal Pengabdian Masyarakat Sultan Indonesia* 2, no. 1 (2024): 1–9. <https://doi.org/10.58291/abdisultan.v2i1.294>.