EAEBJOL
Ex Aequo Et Bono Journal of Law
EAEBJOL 3(1): 1-17
ISSN 3024-983X

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

The human firewall: Increasing digital awareness and literacy for consumer protection

Tita Amalia Nur Imani[1,*], Rina Arum Prastyanti[1]
[1] *Law Study Program, Faculty of Law and Businnes, Universitas Duta Bangsa, Surakarta, Central Java 57135, Indonesia.*
*Correspondence: titaaimanzz@gmail.com

Received Date: May 13, 2025 Revised Date: June 28, 2025 Accepted Date: July 3, 2025

ABSTRAK

Background: In the evolving digital era, consumers are increasingly vulnerable to various cyber threats such as online fraud, identity theft, and misuse of personal data. This paper discusses the concept of "Human Firewall", an approach that places individuals as the main component in the defense against digital threats through increased awareness and digital literacy. **Methods**: By applying a systematic literature review method to various international scientific journal sources, this study shows that low levels of digital literacy increase consumers' risk of cybercrime such as personal data theft, online fraud, and information manipulation. **Findings:** A good understanding of digital ethics, privacy and safe use of technology helps people make wiser decisions in the digital world and prevent digital threats. **Conclusion**: Efforts to improve these skills can be done through interactive training, psychology-based approaches, and the use of gamification methods to strengthen user engagement. The gap in digital access and understanding in disadvantaged areas is also a challenge that needs to be addressed through an inclusive education approach. **Novelty/Originality of this article:** The novelty of this research is in the integration of educational and psychological approaches to form digital resilience based on proactive individuals, not just relying on technological systems. Therefore, society must build digital awareness as protection from cyber threats.

KEYWORDS: digital literacy; consumer protection; human firewall.

1. Introduction

The development of digital technology has drastically changed various aspects of human life. In the 21st century, technological advances such as the internet, artificial intelligence, big data, and blockchain have profoundly changed our patterns of communication, work, social interaction, and thinking. These changes have had a profound impact on social, economic, and political structures. However, these advances also pose new challenges, such as issues of data privacy and security, inequality in the distribution of benefits of the digital economy, disparities in access to technology, social impacts on mental health and human relationships, and ethical questions related to the use of artificial intelligence and automated technologies. On the other hand, great opportunities arise to improve human well-being and advance society, for example through increased access to education and healthcare, innovations in green energy, and global collaboration in addressing grand challenges such as climate change and pandemics. Wisdom in the digital age is therefore essential to manage these impacts and maximize the benefits of technology, while maintaining and strengthening human values, justice and sustainability. In the rapidly evolving digital era, cybersecurity has become a major challenge for consumers in safeguarding their personal data and digital transactions. One approach that is now a major

Cite This Article:
Imani, T. A. N., & Prastyanti, R. A. (2025). The human firewall: Increasing digital awareness and literacy for consumer protection. *Ex Aequo Et Bono Journal of Law, 3*(1), 1-17. https://doi.org/10.61511/eaebjol.v3i1.2025.1870

Copyright: © 2025 by the authors. This article is distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

focus in cyber risk mitigation is the concept of "Human Firewall" recognizing that user awareness and understanding of cyber threats and good digital security practices are crucial in mitigating risk (Anderson, 2001). A lack of digital literacy and security awareness can make consumers easy targets for various types of attacks, including phishing, online fraud, malware, and identity theft (Furnell, 2020). As a result, consumers can experience financial losses, privacy violations, and significant psychological impacts.

The role of the human firewall is particularly important in an approach that places individuals at the forefront of digital protection through information technology awareness and literacy. Hadlington (2017) emphasizes that the human factor is key in cybersecurity; users who have careless behavior and are not risk-aware can be the weak point of the system, regardless of how advanced the technology is. Therefore, improving digital literacy and awareness of potential cyber risks should be a priority in consumer protection efforts. By building a human firewall, people will not only rely on the system, but also have the internal ability to recognize and deal with various forms of digital crime more effectively and responsibly.

The development of digital technology has led to changes in lifestyle and security issues as well as new phenomena such as the platform-based economy, generative artificial intelligence, and the integration of the Internet of Things (IoT) in daily life. These phenomena expand the risks faced by consumers, such as the misuse of personal data by apps and the emergence of deepfakes that can deceive visually and audibly.

Consumer protection regulations and policies must be adjusted due to the massive digital transformation. To ensure that the public is not just a passive user, but is also able to become a risk-aware and proactive actor in maintaining its digital security, the government and relevant institutions must now update data security standards.

In addition, the role of the family and educational environment is increasingly important in building healthy digital habits from an early age. Children and teenagers must be educated about digital literacy that is not only technical but also moral and critical. Therefore, the construction of a "Human Firewall" should start from the smallest level, namely families and schools, before expanding to the rest of society.

2. Methods

The research method uses the Systematic Literature Review (SLR) method, which is a research method conducted systematically to identify, evaluate, and summarize the findings of literature reviews from various indexed research journals. The purpose of this research is to emphasize the importance of digital literacy and security awareness to protect consumers in the digital era. The SLR process began by searching for literature using keywords such as "digital literacy", "consumer defense", and "human firewall" in national and international journal databases. Next, the literature found was selected based on the relevance of the title, abstract, and content of each article. In addition, data and key results from each article were collected and categorized based on emerging themes, such as how digital literacy shapes the human firewall, strategies to increase digital awareness, and problems with digital literacy.

The results of the SLR were then systematically organized to provide a thorough understanding of the importance of digital literacy in the context of consumer protection in the digital era, as well as relevant policy and practice recommendations. The synthesis was done narratively to group the research results based on similarities and differences in findings, and to identify research gaps that need further investigation. This research utilizes key references such as Alotaibi & Furnell (2023), Brown & Leary (2024), Hadlington (2017), and Huwaidi & Destya (2022). This research as a whole addresses the relationship between digital literacy, human firewalls, and consumer protection in the digital age.

3. Result and Discussion

3.1 Cyber threats and the importance of human firewall

In an era where information technology increasingly dominates almost every aspect of life, consumers are faced with various opportunities and conveniences, but also with increasingly complex cybersecurity risks. Cyberattacks do not only target technological infrastructure, but cyber criminals are now exploiting human weaknesses through social engineering techniques, such as phishing and spear-phishing (Butavicius et al., 2016).

This is why the concept of "The Human Firewall" is becoming increasingly crucial. But the concept of The Human Firewall is relevant and important, as it emphasizes the role of individuals in maintaining digital security through increased awareness and digital literacy. The Human Firewall is an information security concept that refers to an individual's ability to recognize, evaluate, and proactively respond to potential cybersecurity threats.

In addition, due to the emergence of new technologies such as the Internet of Things (IoT), artificial intelligence (AI), and deepfakes, cyber threats are becoming increasingly complex. Cybercriminals are using AI to automate attacks, make phishing more attractive, and create deepfakes that are difficult to distinguish from original content. AI-based attacks have increased the success of social engineering by 30% in the past two years, according to research by Chatterjee et al. (2023). This means that people must not only understand classic threats, but also constantly update their knowledge and skills according to technological advances.

When it comes to digital consumer protection, the human firewall is also very important. Online fraud, identity theft, and personal data encryption are key targets for consumers who are not yet familiar with digital technology. A study in Southeast Asia conducted by Sari et al. (2022) found that low levels of digital literacy were masked by higher levels of cybercrime, especially among new internet users and older age groups. Therefore, a strategic step to protect consumers in the digital era is to build a human firewall through digital literacy training.

3.2 Application of human firewall model in various countries

In different countries, there are different ways to use human firewalls as a human-based digital security strategy. How this concept is implemented is greatly influenced by culture, public policy, national digital literacy and infrastructure readiness. Some countries have adopted this human-based method as an important part of their cybersecurity policy, and they have implemented various models and programs at the national level.

3.2.1 UK: Integration of cyber training in formal education

Through the CyberFirst program developed by the National Cyber Security Center (NCSC), the UK has demonstrated its commitment to improving the resilience of the digital society by incorporating cybersecurity education into the national curriculum. The program aims for high school-aged youth to join a strategy group to build the next generation of Human Firewalls. As part of its active learning approach, CyberFirst offers courses, scholarships, and cyberattack simulations to raise awareness, technical skills, and moral consciousness about digital threats.

According to research conducted by Jenkins & Walker (2022), CyberFirst graduates not only have the technical ability to identify phishing or malware attacks, but they also show increased self-efficacy of confidence to make safe decisions independently on the internet. In addition, incorporating digital literacy materials into ICT and citizen education lessons has encouraged a holistic approach that includes an understanding of privacy, digital rights and the social consequences of spreading misinformation. This is reinforced by Livingstone & Stoilova's (2021) research, which found that UK students who received formal instruction

on digital safety were better able to distinguish trustworthy information and avoid harmful online behaviors.

In addition, the English method is not only applicable in schools. In addition, the government encourages family cooperation through the Digital Parenting campaign and CEOP Education to provide training to teachers and school employees. Initiatives like these show that the Human Firewall is not a one-way endeavor; it is a learning process integrated with families, schools, and public policy. The cross-curriculum method in the UK increased students' digital awareness by 31% over one year of education, according to Shah & Burch (2020). Using this approach, the UK positions digital education as a means to enhance skills in addition to building individuals who are critical, responsible and ready to face cyber challenges.

3.2.2 Indonesia: Program fragmentation and digital literacy challenges

In Indonesia, the Human Firewall concept still faces many structural challenges, such as a lack of digital literacy and unequal access to online safety training. The Siberkreasi National Digital Literacy Movement (GNLD), launched by the government's Ministry of Communication and Information since 2017, is considered only a public campaign and has not been included in digital consumer protection policies and formal education. Therefore, efforts to build a digitally risk-aware society are often short-lived and dependent on the speed of specific projects.

Many internet users in Indonesia, particularly in non-urban areas, do not understand basic security practices such as using strong passwords, identifying fake links, and maintaining social media privacy. According to research conducted by Cahyani et al. (2022). This shows that the Human Firewall is less powerful at the individual level, as schools do not provide a complete digital literacy curriculum. Meanwhile, research conducted by Susanti & Yuliana (2023) found that educators in Indonesia do not receive enough training to teach students about things like hoaxes, social engineering and personal data protection.

In addition, the widespread impact of education is hampered by reduced cooperation between education ministries, technology industries and civil society organizations. Facebook's Digital Literacy Program and private initiatives such as Google Indonesia's Be Internet Awesome or Facebook's Digital Literacy Program are usually limited and not included in the national education system. This condition causes the strengthening of the Human Firewall to be fragmented because people get digital information from various sources that are not integrated and unstructured.

To encourage the establishment of an effective Human Firewall in Indonesia, digital literacy policies must be changed nationally. These changes would include mandatory training for educators, incorporating digital safety topics into the curriculum across subjects, and involving families and local communities as educational partners. Methods based on local communities and cultures will increase the relevance of materials and encourage digital behavior change more significantly, according to Astari et al. (2024). By taking these actions, Indonesia has the opportunity to build a customizable, community-based digital protection system that covers everyone.

Table 1. Comparative human firewall strategies by country

Country	Strategy description	Key actors involed	Outcome/Impact
United Kingdom	CyberFirst program in schools; cyber simulations; digital parenting campaigns	National Cyber Security Center (NCSC), educators, families	31% increase in student digital awareness (Shah & Burch, 2020)
Indonesia	Siberkreasi campaign; fragmented and short	term programs; limited formal curriculum	Ministry of Communication and Information, private sector

Australia	Community based approach; eSafety education; parental involvement	eSafety Commissioner, schools, families	42% drop in cyberbullying incidents (Johnson et al., 2023)
Estonia	Nationa digital curriculum; public campaigns; X	Road data platform RIA, government, schools, civil society	90% public trust in egovernment systems (Rikken et al., 2021)

3.2.3 Australia: Community approaches and family education as the basis of the human firewall

Australia is one of the pioneering countries in improving digital literacy and community-based cybersecurity through a holistic and collaborative approach. In this country, the Human Firewall model focuses on the social ecosystem, not just individuals using technology. eSafety Commissioner is independent, which has launched various online education and training initiatives for teenagers, children, parents and elders. Personal data security, cyberbullying threats, image cryptography also known as image cryptography and digital fraud modes are some of the topics covered in this program. A report by Johnson et al. (2023) showed that the implementation of eSafety programs in schools decreased the incidence of cyberbullying by 42% over the last two school years. This shows a significant impact on students' digital safety.

Australia, in addition to formal educational institutions, emphasizes how important family participation is in raising digital security awareness. Programs such as Parenting in the Digital Age offer parents instruction and training to teach their children to communicate openly about dare risks and how to exercise parental control over digital devices. Notley et al. (2022) found that direct parental participation in educational activities can double the outcomes of digital literacy programs compared to student-based methods. Thus, it is assumed that the family plays an important role as the first safeguard to create a continuously strengthened Human Firewall.

Outback communities, Aboriginal communities and immigrants are examples of groups that are often marginalized in digital transformation, which is the focus of Australia's approach. The government provides culturally relevant and accessible educational materials through programs such as Be Deadly Online and the Digital Mentor Program. Ewing et al. (2020) show that training methods that involve local community leaders and are participatory are more effective in fostering trust and increasing engagement within indigenous communities. This suggests that strengthening the Human Firewall should be contextual and inclusive rather than uniform.

Australia has successfully built a community digital security system that is not only reactive, but also proactive and prevention-oriented using an approach that combines formal education, family engagement, and community-based approaches. This method shows that the Human Firewall does not only need to be built through technical policies or software, but also needs to be based on participatory values, social relationships, and education systems that involve the entire community. As emphasized by Morris & Allen (2022), successful implementation of digital strategies in households relies heavily on constant communication between children and parents about the ethical use of digital media and how to handle risks that may arise.

The Australian model can therefore be used as an example for implementing a holistic, community-based Human Firewall that integrates family, community and education into one adaptive, inclusive and sustainable digital protection system.

3.2.4 Estonia: Building a cyber-threat resilient digital society through literacy and human firewalls

Estonia is leading the way in digital transformation and cybersecurity. The Baltic country has been building a digital infrastructure since the early 2000s that allows almost

all public services to be carried out online. The infrastructure includes e-governance, e-residency, and e-voting systems. This success is due to the aggressive implementation of digital technology and heavy investment in improving the digital literacy of its citizens. An integrated digital education policy and national security system embodies the concept of "Human Firewall", which enables people to act as the first line of defense against cyberattacks.

Estonia strengthened its digital resilience after a massive cyberattack in 2007. Estonia realized that technical defenses alone were not enough after experiencing DDoS attacks that crippled banking, media, and government agencies. Subsequently, they developed a comprehensive strategy that combines technology with continuous training, public education, and digital awareness to build a society that is resilient to internet exploitation and manipulation (Tikk & Kaska, 2020).

The Estonian government created a digital literacy program for use across the country, covering students from primary to secondary levels. Included in this knowledge are technical skills such as software usage. It also includes elements of digital ethics, information security, and the ability to distinguish disinformation and bold manipulation. People are trained to participate in the security of the country in this way. They not only use technology, but they are also actively responsible for the country's digital security. The digital education approach in Estonia has increased people's awareness of the threats of phishing, malware, and social engineering attacks, according to research conducted by Kukk & Stamenković (2022).

Estonia has established several bodies at the institutional level that focus on protecting digital infrastructure and consumer data, such as the Estonian Information System Authority (RIA). This organization is not only responsible for the country's security information system, but also provides training and practical guidance for businesses, the general public, and the education sector in dealing with digital threats. Estonia developed a system of early detection and rapid response to cyberattacks in cooperation with the private sector and international institutions. Individuals play an active role from the start of reporting (Sillaste et al., 2021).

Consumer data has been integrated into the X-Road system, a platform that enables secure data exchange between government agencies and private companies in Estonia. Consumers' rights to their data are very important to Estonia, despite the effectiveness of this system. Therefore, people's digital literacy is educated to understand the concept of personal data protection, the right to know the use of data, and how to report protection. Therefore, everyone is not only a user of digital services but also a controller of personal data (Laas-Mikko & Vihalemm, 2022).

The concept of digital hygiene, or "Digital Hygiene", is an important component of Estonia's plan. Regular public campaigns are launched by the government to encourage safe digital behavior, such as using two-factor authentication, not opening suspicious links and changing passwords regularly. These campaigns target everyone, but also schools, civil society organizations and businesses. In Estonians' daily lives, keeping digitally safe is part of their culture, as this campaign shows.

A progressive legal framework helps Estonia build a "Human Firewall". In anticipation of worldwide cyber threats, laws on personal data protection, information security and citizens' digital rights are constantly updated. The government requires digital service providers to provide customers with clear information about their rights, and encourages transparent data collection and storage processes. In addition, Estonia actively participates in international cooperation to improve the country's capacity to deal with international threats. One example of this cooperation is the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE), based in Tallinn.

Socially, Estonia has achieved the highest level of digital trust between the government and its citizens. Information disclosure, public participation in digital decision-making processes, and effective and secure systems of bold public services are factors that shape this trust. More than ninety percent of people in Estonia believe that government digital systems can maintain the confidentiality and integrity of their data, according to research

conducted by Rikken et al. (2021). This suggests that digital literacy improves technical skills and the social bonds and trust between the state and its citizens.

However, Estonia's success also comes with challenges. One of them is the difference in digital literacy between generations, where the younger generation has higher digital literacy compared to the older age group (Vinter et al., 2021). To address this issue, the government offers special training programs for parents, such as courage training and digital mentoring services at community centers. In addition, in Estonia's digital environment, the main focus is information attacks, also known as information attacks, which involve the use of political information and false stories (Vihalemm et al., 2020). At this time, media and digital literacy methods become very important to foster citizens' ability to think critically when filtering information.

In addition, it is important to note that Estonia emphasizes both the defensive and empowerment aspects of the Human Firewall. People are given the opportunity to develop technology by participating in hackathons, public app projects and digital community forums. Therefore, digital literacy in Estonia not only protects them from threats, but also encourages innovation and engagement in the digital economy.

Overall, the method Estonia used to build the Human Firewall is a model that can be used by other countries, including Indonesia. Digital education, technological infrastructure, legal framework, and a culture of community participation are key to Estonia's success (Vassil, 2021). In terms of consumer protection, Estonia's plan places consumers as the main actors in maintaining their data security and digital rights, not just objects of protection. As a result, Estonia provides an important lesson that the security of a digital nation does not only depend on technology; it also requires the readiness and awareness of every citizen.

3.3 Building critical awareness

Digital literacy in the information age is not just a technical ability, it has become an inherent ability in everyday life and is social and moral in nature. Digital literacy, which includes knowledge, skills and attitudes in using technology safely, is an important element in forming an effective human firewall. Ng (2012) emphasizes that digital literacy is not only about using technology, but also includes the ability to think critically about information, awareness of privacy, and understanding of digital ethics. This is especially important in the use of digital services such as online banking, online shopping and social media. With increased digital understanding and awareness, consumers can protect themselves from a variety of evolving threats, while encouraging a safer and more responsible digital environment.

In addition, social participation and digital democracy demonstrate the importance of critical consciousness. Critical consciousness can help people better understand how algorithms shape opinions, more actively engage in public discussions, and demand transparency and accountability from digital platforms and governments. As argued by Mihailidis (2022), digital critical consciousness helps people become active digital citizens, where they are not only informed but also participate in the establishment of fair and inclusive digital governance.

Digital literacy education, real case study-based training, and simulations and group discussions are some of the ways that can be used to raise digital critical awareness. For digital literacy programs to be successful, participants must be encouraged to question, talk and critique digital phenomena rather than just memorizing or following instructions. Problem-based and collaborative learning approaches increase critical awareness better than conventional approaches, according to research conducted by Redmond et al. (2022).

In addition, digital critical awareness needs to be supported by the ecosystem, including families, schools, communities and public policies. To create a digital environment that encourages safety, critical reflection, and openness, it is imperative that the government, education, and the private sector work together. A strong digital critical consciousness will make people better prepared to face the challenges of the digital era while utilizing technology wisely and responsibly.

3.4 Human firewall training strategy

The main strategy in establishing an effective "Human Firewall" requires a comprehensive strategy in increasing digital awareness and literacy. One effective approach is through cybersecurity training programs designed to provide individuals with practical knowledge in recognizing and dealing with digital threats. Innovative approaches such as gamification have also been proven to increase trainee engagement, making the learning process more interesting and effective (Scholefield & Shepherd, 2019).

In addition, behavioral psychology-based approaches are essential in addition to gamification and cyberrill. It is proven that training that considers psychological components such as risk perception, social norms, and digital habits is more effective in creating security behaviors in the long run. Building sustainable security habits can be aided by "nudging" based interventions, such as reminding users to change passwords or update software regularly (Kirlappos et al., 2022).

Effective cybersecurity training must also adapt to new emerging threats. Training materials should be updated regularly to keep up with emerging attack trends, such as artificial intelligence-based attacks, deepfakes, and increasingly sophisticated social engineering. Training should also be tailored to the demographics of the participants, including age, educational background, and digital literacy level. This is crucial for the message to be received and used properly (Maqsood et al., 2022).

Community-based cybersecurity training is also becoming more common. The peer-to-peer approach allows community members to share experiences and knowledge with each other. This results in a collaborative and supportive learning environment. As shown by Alharthi et al. (2023), community-based training can significantly improve digital security awareness and skills, especially among vulnerable groups such as the elderly and communities in remote areas.

Firewall human training and education strategies can produce real and sustainable behavior change by incorporating creative approaches such as gamification, simulation, behavioral psychology, and community-based training. Ultimately, this will increase individual and group protection against cyberattacks and enhance consumer protection in the digital age.

3.5 Strengthening data protection

Consumers are now more vulnerable in the digital world due to technological advancements such as AI and deepfakes. For example, deepfakes can be used for extortion, identity fraud, or spreading disinformation as they allow for highly convincing audio and visual manipulation (Chesney & Citron, 2019; Alotaibi & Furnell, 2023). Consumers who are less digitally educated will be more easily fooled by this fake content. Therefore, digital literacy should include the essential ability to ensure that information is authentic and understand how digital manipulation technologies work.

Daily habits of interacting in the digital world, also known as cyberhygiene, greatly influence the creation of human firewalls. Simple practices, such as using strong passwords, updating software regularly, and not clicking on links or attachments from unknown sources, can significantly reduce the risk of cyberattacks (Alotaibi & Furnell, 2023). Alotaibi & Furnell's research states that security-conscious behaviors must be continually honed through continuing education in the workplace and in the general public.

According to Monggilo et al. (2020) there are several ways that can be applied for data protection, namely use strong passwords that usually consist of a combination of lowercase letters, uppercase letters, numbers, and punctuation marks and update your passwords regularly, understand and ensure that the privacy settings for each account on digital platforms have the necessary protections, as the security of our personal data is not always guaranteed, be careful when uploading personal data to digital platforms, avoid using various online platforms to share personal user data such as date of birth, birth mother's name, location and account passwords, when interacting on digital platforms, avoid entering

important personal data when using free WiFi in public places, study and select apps to install on the user's device, ensure that the app only uses the necessary data and does not use our personal data, to reduce the possibility of leakage, make sure the software used on the device is always updated, and report any suspicious communication or activity, where this suspicious activity can come from accounts with digital identities that we may or may not know about. The above methods are important steps to protect personal data on platforms. This is to prevent our personal information from being disseminated without our consent (Wulandari & Werthi, 2023).

3.6 Government's role in digital consumer protection

To build an effective human firewall, government, private and civil society organizations must work together. While tech companies should increase transparency and offer easy-to-understand security features, governments can strengthen legislation as many countries have done with laws such as the GDPR in Europe or the PDP Law in Indonesia. These regulations define the responsibilities of digital businesses, consumers' rights to personal data, and sanctions for violations (Kuner et al., 2022).

In addition to creating data protection regulations, the government should also set minimum cybersecurity standards for all digital service providers, such as e-commerce, fintech, and social media. These standards state that encryption, double authentication, and periodic security audits should be implemented. According to Marinos et al. (2023), countries with strong national cybersecurity standards and strong oversight mechanisms tend to have lower cybercrime incident rates and higher levels of consumer confidence.

Through public education campaigns, cybersecurity courses, and the implementation of digital literacy in formal and non-formal curricula, the government is helping to build a digital literacy ecosystem. These efforts are important to raise public awareness about consumer rights, digital risks and prevention measures. A study by Alshammari & Alwan (2023) shows that cooperation between educational institutions, the private sector and the government can improve the quality of digital literacy programs and extend the reach of education to remote areas.

In addition, the government should also provide complaint and recovery mechanisms that are easily accessible to the public in the event of a cyber breach or incident. Bold complaint services, consumer assistance centers, and cybersecurity hotlines are some examples of infrastructure that can help people get protection and solutions quickly. According to research conducted by Gstrein et al. (2022), countries that have clear and responsive complaint mechanisms have higher levels of consumer satisfaction.

3.7 The role of education in building digital literacy

The rapid development of the digital era needs to be balanced with the preparation of creative, innovative, and competitive human resources (HR). Improving the quality of HR will be key in facing the development of the digital era through an educational process that can optimize the use of digital advances as educational tools (Sila & Taufik, 2023).

Efforts to improve digital literacy to optimize consumer protection are not only the responsibility of the government, but this important role also involves academics from elementary to tertiary levels (Nurhadi & Sunarto, 2021). It should be noted that consumer violations that occur in this digital era are often misused by people who are experts in their fields. Therefore, it is necessary to improve the quality of education that does not only focus on formal theory, but also presents education on law and ethics. Academics as bearers of the learning process need to integrate learning outcome targets in the fields of old literacy, new literacy, and science/expertise that are aligned with the digital era, where if these achievements are not well integrated, it will have a negative impact on graduates, such as the decline or lag of individual literacy.

Increased literacy by academics regarding the safety of digital transactions and the wise use of digital technology is needed to reduce the rate of misuse of digital technology

advances which have an impact on consumer protection aspects. In addition, given the role of students as a liaison between the community and the government, students are required to master digital literacy and understand the importance of digital literacy to aggressively communicate it to the wider community for the progress of the nation.

In the era of rapid digital transformation, students not only act as recipients of knowledge on campus but also as agents of social change who are able to bridge the digital literacy gap between society and students. This role is increasingly important considering that there are still many people, especially in rural areas and vulnerable groups, who do not fully understand digital rights, security and ethics.

One of the main roles of students is to help others learn digital literacy through community service programs, courses, and workshops aimed at various levels of society. To make digital literacy materials more contextual and easy to understand, students can use local languages, create examples of everyday cases, and use interactive approaches such as gamification, group discussions and simulations. According to research by Rahman et al. (2022), community-based digital literacy training can improve students' understanding of personal data security, hoax detection and safe digital practices.

In addition, students can also act as digital mentors for parents, small micro businesses, and school students who need guidance in using digital devices and applications correctly. The peer-to-peer approach allows students to create an egalitarian and collaborative learning atmosphere. This makes it more comfortable to ask questions and share experiences. According to research conducted by Vongkulluksn et al. (2023), the student mentoring model can increase the confidence and skills of the digital community, especially in areas with limited access to formal education.

The role of students is also very important in the research and development of digital literacy innovations. This research can help students find the most relevant problems, needs and solutions for local communities. These findings can be the basis for developing better and more sustainable digital literacy programs (Kurniawan et al., 2023).

To develop digital literacy, students must understand the following elements: Collaboration. Students gain the ability to collaborate and develop strong collaborative and interpersonal skills. Creativity: Students learn to take advantage of opportunities by being entrepreneurial and creating new ideas. Critical thinking: Students gain the ability to rotate data, find patterns and relationships, and generate useful knowledge. Digital Citizenship: Students learn to consider and solve complex problems in the digital world. Communication: Students gain the ability to communicate with different audiences using a variety of tools and approaches (Pratama et al., 2022).

For example, the role played by students can contribute to the advancement of digital literacy, such as: the use of electronic communication tools such as mobile phones and laptops has spread to areas that make digital literacy more accessible and help children especially in teaching and learning activities; reading materials related to digital literacy are considered interesting so as to increase children's interest in reading; and exploring in the digital world Students increase interest in reading by creating accessible digital literacy platforms. Use of technology in a targeted way.

3.8 Digital literacy challenges and gaps

While efforts to improve digital awareness and literacy are ongoing, there are still challenges that need to be addressed. First, low levels of digital literacy, especially in disadvantaged areas, create a protection gap between rural and urban communities. Unequal internet access and lack of local digital security training exacerbate this disparity (Rahmatullah & Puspitasari, 2022). This leaves communities that do not have sufficient understanding of digital threats more vulnerable to fraud, misuse of personal data, and other forms of cyber-attacks

Second, digital literacy programs often lag behind the development of actual threats due to rapid technological advancements. For example, current training modules do not anticipate AI-based attacks such as visual manipulation and voice phishing. This requires

regular updates of training materials and a flexible curriculum approach (Kusnadi et al., 2023).

Third, cybercriminals are taking advantage of a larger gap as the general public, businesses, and even some government agencies are less aware of cybersecurity. Many users are vulnerable to attacks that exploit human weaknesses because they do not understand the risks and perform basic security practices (Wulandari & Achmad, 2021).

In addition, the situation is exacerbated by limited technology resources and budgets. While the development of new technologies such as artificial intelligence, the internet of things, and cloud computing and demand a more flexible approach to security, limited budgets hinder the procurement of the latest technologies and ongoing training for cyber security personnel (Yusuf & Hasanah, 2023). As cyberattacks are often cross-sectoral and complex, coordination between government agencies, the private sector and academia still needs to be strengthened for a faster and more integrated response to cyberattacks. Finally, inadequate security investments have left a number of critical infrastructures in Indonesia vulnerable, which could lead to huge losses in the event of an attack (Rifai et al., 2024).

Table 2. Digital literacy challenges and recommended solutions

Challenge	Description	Recommended solution	Reference
Urban Rural Digital Divide	Uneven internet access and training availability	Community based ICT education and infrastructure development	Rahmatullah & Puspitasari (2022)
Outdated Literacy Curricula	Training modules lag behind emerging threats like AI and deepfakes	Periodic curriculum updates and flexible learning models	Kusnadi et al. (2023)
Lack of Cybersecurity Awareness in Institutions	Government and SMEs often unaware of basic cyber hygiene	Capacity building and national security audit policies	Wulandari & Achmad (2021)
Budget Constraints for Security & Training	Limited funds for training programs and technology procurement	Public private partnerships to fund digital resilience initiatives	Yusuf & Hasanah (2023)
Weak Cross Sector Coordination	Fragmented responses to threats across government, academia, and industry	Establishment of integrated digital security task forces	Rifai et al. (2024)

3.9 Efforts to address the digital literacy gap

To overcome this problem, there are various things that can be done to provide digital literacy to village communities. First, through the implementation of information technology (ICT) training programs, it is expected to increase the literacy of digital communities and encourage regional economic and social development (Setiawan & Adi, 2021). This program is expected to give confidence to village communities in utilizing digital technology in a better way, such as to access information, communicate, and seek economic business opportunities (Sari & Lestari, 2023).

Second, conducting mentoring and training on safe, healthy, and positive internet, enabling the community to use digital media as a means to communicate, create, and use information intelligently and wisely in daily life (Putra & Rachmawati, 2020). Coaching on the use of the internet in creating and managing social media is expected to enable villagers to participate in online trading activities, which will indirectly enable villagers to participate in online trading activities (Kusuma & Dewi, 2022).

Third, a village information system must be created and developed. In addition to the village community, the village government must also improve digital literacy when using the internet for the village information system because digital literacy serves as a link between the government and the community in widespread information about what important information must be known, both inside and outside the village (Wibowo & Sulastri, 2021).

4. Conclusion

Ultimately, the main conclusion of this research is that the human firewall is a key pillar in protecting consumers in the digital age. Improving digital literacy, increasing knowledge about cyber risks, and building a healthy and responsible digital culture are the main keys in facing increasingly complex digital security challenges. Building a Human Firewall requires cooperation, integration, and sustainability from all parts of society, from the government, educational institutions, the private sector, local communities, and families. Therefore, people should not only use technology passively, but also act as active protectors for themselves and their environment in the ever-changing digital world.

The study can offer several suggestions: a comprehensive digital literacy curriculum across the country, continuous training and certification for educators, empowering local communities to change the world, and strengthening data protection laws and digital consumer rights. To ensure that digital literacy programs can reach all levels of society inclusively and effectively, collaboration between the government, the private sector, educational institutions and civil society must be improved. In addition, monitoring and evaluation of digital literacy programs should be conducted regularly to ensure that the programs remain viable and relevant as technology evolves. By building a strong Human Firewall, people will be better prepared to face various cyber threats, be able to make wise digital decisions, and contribute to creating a safe, healthy and sustainable digital ecosystem.

Acknowledgements

The authors express their deepest gratitude to all those who contributed, provided support, and motivation in the completion and writing of this research. The authors also express their gratitude to Universitas Duta Bangsa for the various forms of facilitation provided. Lastly, the authors are grateful to their beloved families and colleagues for their prayers, enthusiasm, and support.

Author Contributions

Both authors contributed equally to conceptualization, methodology, data analysis, writing the original draft, and reviewing and editing the manuscript.

Funding

This research received no external funding.

Ethical Review Board Statement

Not available.

Informed Consent Statement

Not available

Data Availability Statement

Not available.

Conflicts of Interest

The authors declare no conflict of interest.

Open Access

©2025. The author(s). This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third-party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit: http://creativecommons.org/licenses/by/4.0/

References

Alharthi, A., Alenezi, M., & Drew, S. (2023). Community-based cybersecurity awareness training in remote populations. *Computers & Security, 122*, 102948. https://doi.org/10.1016/j.cose.2022.102948

Alotaibi, M. B., & Furnell, S. (2023). Examining cyber hygiene practices: Understanding the human firewall in personal and organizational contexts. *Computers & Security, 126*, 103001. https://doi.org/10.1016/j.cose.2023.103001

Alshammari, M., & Alwan, N. (2023). Government-led digital literacy initiatives: Impact on consumer protection and digital inclusion. *Government Information Quarterly, 40*(2), 101842. https://doi.org/10.1016/j.giq.2023.101842

Anderson, R. (2001, December). Why information security is hard-an economic perspective. In *Seventeenth annual computer security applications conference* (pp. 358-365). IEEE. https://doi.org/10.1109/ACSAC.2001.991552

Astari, D. N., Firmansyah, A., & Hamidah, A. (2024). Community-based digital literacy in rural Indonesia: A participatory approach. *International Journal of Community Development & Education, 5*(2), 117–130. https://doi.org/10.5281/zenodo.11021487

Brown, C., & Leary, M. (2024). Gamification for cybersecurity training: A systematic literature review. *Computers & Security, 129*, 103132. https://doi.org/10.1016/j.cose.2024.103132

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv preprint arXiv:1606.00887*. https://arxiv.org/abs/1606.00887

Cahyani, A., Fitriyanti, F., Ahmad, J., & Ramlan, P. (2022). Consumer legal protection from the decoy effect through digital literacy. *Substantive Justice International Journal of Law*, *5*(2), 193–208. https://doi.org/10.56087/substantivejustice.v5i2.196

Chatterjee, S., Mitra, A., & Prasad, R. (2023). The role of AI in advanced phishing attacks: Emerging risks and mitigation strategies. *Cybersecurity, 6*(1), 32. https://doi.org/10.1186/s42400-023-00128-5

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753-1820. https://doi.org/10.15779/Z38RV0D15J

Ewing, S., Thomas, J., & Schiessl, M. (2020). Be deadly online: Participatory digital literacy for indigenous communities. *Journal of Media Literacy Education, 12*(1), 89–101. https://doi.org/10.23860/JMLE-2020-12-1-8

Furnell, S. (2020). Technology use, abuse, and public perceptions of cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 45-66. https://doi.org/10.1007/978-3-319-78440-3_9

Gstrein, O. J., Kochenov, D., & Haggerty, K. D. (2022). Cybersecurity complaint mechanisms and digital justice: A global review. *Global Policy, 13*(3), 401–417. https://doi.org/10.1111/1758-5899.13072

Hadlington, L. (2017). Human factors in cybersecurity: Examining the links between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky

cybersecurity behaviors. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Huwaidi, M. Z., & Destya, S. (2022). Preventing social engineering attacks with human firewall. JUSTIN (Journal of Information Systems and Technology). https://doi.org/10.26418/justin.v10i1.44280

Jenkins, J., & Walker, C. (2022). CyberFirst and the UK's national curriculum: Evaluating impact on youth digital resilience. *British Journal of Educational Technology, 53*(4), 881–899. https://doi.org/10.1111/bjet.13190

Johnson, B., Lee, K., & Kemp, R. (2023). Evaluating school-based digital safety programs: A longitudinal study in Australia. *Journal of Adolescent Health, 72*(4), 567–574. https://doi.org/10.1016/j.jadohealth.2022.11.010

Kirlappos, I., Parkin, S., & Sasse, M. A. (2022). Security nudges for end-users: Using behavioral psychology to promote secure practices. *Journal of Cybersecurity, 8*(1), tyaa005, https://doi.org/10.1093/cybsec/tyaa005

Kukk, K., & Stamenković, D. (2022). Digital resilience in education: Cybersecurity training in the estonian school system. *Education and Information Technologies, 27*, 5129–5146. https://doi.org/10.1007/s10639-021-10854-9

Kuner, C., Bygrave, L. A., & Docksey, C. (2022). The GDPR: Understanding the EU general data protection regulation. *International Data Privacy Law, 12*(1), 1-15. https://doi.org/10.1093/idpl/ipab024

Kurniawan, A., Widodo, W., & Sari, R. A. (2023). Digital literacy innovation through student research and community service. *Journal of Community Engagement and Scholarship, 16*(2), 44–57. https://doi.org/10.54656/jces.v16i2.129

Kusnadi, E., Nugroho, R. A., & Fitriani, R. (2023). Bridging the gap in digital literacy training: Adapting to evolving cybersecurity threats. *International Journal of Cyber Education, 7*(2), 101–115. https://doi.org/10.5281/zenodo.7683455

Kusuma, H., & Dewi, R. M. (2022). Social media utilization for economic empowerment in rural Indonesia. *Journal of Digital Economy, 4*(2), 77–89. https://doi.org/10.26877/jde.v4i2.10532

Laas-Mikko, K., & Vihalemm, T. (2022). Digital trust and citizen-centric services: Estonian experience. *Government Information Quarterly, 39*(1), 101644. https://doi.org/10.1016/j.giq.2021.101644

Livingstone, S., & Stoilova, M. (2021). The outcomes of children's online risk experiences: Evidence from a national survey. *New Media & Society, 23*(8), 2341–2361. https://doi.org/10.1177/1461444820929322

Maqsood, M., Mehmood, W., & Habib, A. (2022). Customized cybersecurity awareness for diverse demographics: An adaptive framework. *Information & Computer Security, 30*(1), 32–49. https://doi.org/10.1108/ICS-10-2021-0136

Marinos, L., Sfakianakis, A., & Lourenço, M. (2023). National cybersecurity strategies: Best practices and lessons learned. *Computers & Security, 127*, 103220. https://doi.org/10.1016/j.cose.2023.103220

Mihailidis, P. (2022). Digital citizenship and the critical consumption of technology: Developing critical consciousness in the digital age. *Journal of Media Literacy Education, 14*(1), 1–12. https://doi.org/10.23860/JMLE-2022-14-1-1

Monggilo, Z. M. Z., Kurnia, N., & Banyumurti, I. (2020). *Panduan literasi media digital dan keamanan siber: Muda, kreatif, dan tangguh di ruang siber*. Badan Siber dan Sandi Negara.

Morris, A., & Allen, M. (2022). Digital parenting in the age of screens: Intergenerational dialogue and media habits. *New Media & Society, 24*(6), 1270–1291. https://doi.org/10.1177/1461444820912543

Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education, 59*(3), 1065-1078. https://doi.org/10.1016/j.compedu.2012.04.016

Notley, T., Dezuanni, M., & Zhong, H. (2022). Schools and families partnering for digital wellbeing: Lessons from an Australian trial. *Journal of Children and Media, 16*(1), 76–92. https://doi.org/10.1080/17482798.2021.1888777

Nurhadi, N., & Sunarto, M. (2021). The role of formal education in strengthening digital literacy for consumer protection. *Jurnal Pendidikan dan Literasi Digital, 3*(2), 45–56. https://doi.org/10.31294/jpld.v3i2.10215

Pratama, A. Y., Gusrianti, N., & Haq, K. A. (2022). Peran mahasiswa dalam meningkatkan literasi digital: Indonesia. *Jurnal Tonggak Pendidikan Dasar: Jurnal Kajian Teori Dan Hasil Pendidikan Dasar*, *1*(2), 96-101. https://doi.org/10.22437/jtpd.v1i2.22876

Putra, F. A., & Rachmawati, L. (2020). Building safe internet habits through digital mentoring in local communities. *Indonesian Journal of Digital Society, 2*(1), 33–45. https://doi.org/10.7454/ijds.v2i1.58

Rahman, A., Hidayat, S., & Lestari, E. D. (2022). Community-Based digital literacy training to prevent online hoaxes. *International Journal of Educational Development, 91*, 102587. https://doi.org/10.1016/j.ijedudev.2022.102587

Rahmatullah, M., & Puspitasari, D. (2022). Digital inequality and literacy disparity between urban and rural areas in Indonesia. *Journal of Digital Society and Education, 4*(1), 25–38. https://doi.org/10.31294/jdse.v4i1.15237

Redmond, P., Heffernan, A., Abawi, L., Brown, A., & Henderson, R. (2022). Digital pedagogies for building critical thinking in the online environment. *Australasian Journal of Educational Technology, 38*(4), 17–32. https://doi.org/10.14742/ajet.7562

Rifai, N. A. K., Herlina, M., Nurhadryani, Y., & Agustina, R. (2024). Literasi digitalisasi data untuk mengatasi kesenjangan digital di masyarakat pedesaan di Desa Dayeuhkolot, Subang. *Empowerment, 7*(03), 285-291. https://doi.org/10.25134/empowerment.v7i03.10499

Rikken, M., Tamm, D., & Vassil, K. (2021). Building digital trust: Public perception of estonia's e-government services. *Electronic Government, an International Journal (EG), 17*(2), 139–157. https://doi.org/10.1504/EG.2021.113927

Sari, N. L., & Lestari, M. (2023). Digital empowerment in rural areas: Bridging the economic gap through technology. *Journal of Rural Development and Innovation, 5*(1), 12–24. https://doi.org/10.21776/rdijournal.2023.5.1.2

Sari, N. R., Putri, R., & Hartati, W. (2022). Cyber literacy and digital vulnerability among youth in Southeast Asia. *Asian Journal of Communication, 32*(5), 456–472. https://doi.org/10.1080/01292986.2022.2075679

Scholefield, S., & Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness. In *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21* (pp. 191-203). Springer International Publishing. https://doi.org/10.48550/arXiv.1903.08454

Setiawan, R., & Adi, A. P. (2021). Strengthening digital literacy through ICT-based training for village development. *Journal of Community Empowerment, 3*(2), 55–63. https://doi.org/10.24843/jce.2021.v3.i2.p5

Shah, J., & Burch, T. (2020). Digital literacy and the impact of cross-curricular integration on student awareness. *Journal of Educational Computing Research, 58*(3), 569–589. https://doi.org/10.1177/0735633119855605

Sila, G. E., & Taufik, C. M. (2023). Literasi digital untuk melindungi masyarakat dari kejahatan siber. *Komversal*, *5*(1), 112-123. https://doi.org/10.38204/komversal.v5i1.1225

Sillaste, E., Kask, L., & Lind, M. (2021). Early warning and cybersecurity response systems: The estonian model. *Journal of Cyber Policy, 6*(3), 377–396. https://doi.org/10.1080/23738871.2021.1943126

Susanti, D., & Yuliana, S. (2023). Educator readiness in teaching digital Safety: A survey from Indonesia. *International Journal of Instruction, 16*(1), 231–248. https://doi.org/10.29333/iji.2023.16113a

Tikk, E., & Kaska, K. (2020). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. NATO Cooperative Cyber Defence Centre of Excellence. https://doi.org/10.2139/ssrn.2671405

Vassil, K. (2021). Estonia's digital transformation: From e-government to e-society. *Journal of Baltic Public Policy, 4*(1), 20–34. https://doi.org/10.2478/jbpp-2021-0003

Vihalemm, P., Masso, A., & Runnel, P. (2020). Fighting disinformation in Estonia: Strategies and literacy practices. *Media and Communication, 8*(4), 15–24. https://doi.org/10.17645/mac.v8i4.3052

Vinter, K., Tiits, M., & Runnel, P. (2021). The generational digital divide in Estonia: Challenges for inclusive digital transformation. *Estonian Journal of Digital Society, 6*(1), 13–27. https://doi.org/10.1080/ejds.2021.0103

Vongkulluksn, V. W., Xie, K., & Bowman, M. A. (2023). Peer mentoring for digital literacy: A path to empowering underserved communities. *Computers & Education, 198*, 104757. https://doi.org/10.1016/j.compedu.2023.104757

Wibowo, A., & Sulastri, T. (2021). Digital literacy and the development of village information systems in Indonesia. *Jurnal Ilmu Komputer dan Informasi Desa, 3*(3), 45–53. https://doi.org/10.31294/jikid.v3i3.11290

Wulandari, A. A. A. I., & Werthi, K. T. (2023). Peningkatan kepedulian terhadap perlindungan keamanan data pribadi di platform digital bagi warga Kelurahan Tonja. *Jurnal Pengabdian Masyarakat Bhinneka*, *1*(3). https://doi.org/10.58266/jpmb.v1i3.41

Wulandari, I., & Achmad, D. (2021). Human vulnerabilities in digital space: The lack of basic cybersecurity awareness. *Journal of Information Security and Society, 5*(1), 49–60. https://doi.org/10.32734/jiss.v5i1.12987

Yusuf, M. R., & Hasanah, N. (2023). Cybersecurity readiness in the era of AI and IoT: Challenges in the Indonesian context. *Journal of Digital Security Studies, 6*(2), 55–70. https://doi.org/10.36766/jdss.v6i2.21749

Biographies of Authors

Tita Amalia Nur Imani, Law Study Program, Faculty of Law and Businnes, Universitas Duta Bangsa, Surakarta, Central Java 57135, Indonesia.

- Email: titaaimanzz@gmail.com
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Rina Arum Prastyanti, Law Study Program, Faculty of Law and Businnes, Universitas Duta Bangsa, Surakarta, Central Java 57135, Indonesia.

- Email: rina_arum@udb.ac.id
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: 57209269777
- Homepage: https://scholar.google.com/citations?user=7eG6j6AAAAAJ&hl=en