Risk Literacy, Scam Prevention and Public Education: Building a Resilient Society against Financial and Digital Fraud

Rudresh Kumar[1], Samarth Dubey[2], Sheetanshu Raghav[3], Sonam Tomar[4], Tanu[5] (PG Student)
Dr.Tarun Babu Shrivasatava[6],(Faculty of Commerce, Supervisor)
DPBS College, Anupshahr, Bulandshahr, UP, India[1,2,3,4,5,6]

How to Cite this Article:

Kumar, R., Dubey, S., Raghav, S., Tomar, S. & Tanu, (2026). Risk Literacy, Scam Prevention and Public Education: Building a Resilient Society against Financial and Digital Fraud. International Journal of Creative and Open Research in Engineering and Management, <i>02</i>(6). https://doi.org/10.55041/ijcope.v2i6.345

https://doi.org/ 10.55041/ijcope.v2i6.345

Abstract

The rapid expansion of digital technologies, online banking, electronic commerce, and social networking platforms has transformed the way people communicate; conduct financial transactions, and access public services. While these technological developments have generated significant economic and social benefits, they have simultaneously created new opportunities for fraudsters to exploit individuals through increasingly sophisticated scams. Cyber-enabled financial fraud, phishing, identity theft, investment fraud, romance scams, fake job offers, and social engineering attacks have become major global concerns, affecting people across all age groups and socioeconomic backgrounds. In this context, risk literacy has emerged as an essential life skill that enables individuals to identify, evaluate, and respond appropriately to various forms of financial and digital risks. Individuals possessing adequate risk literacy are more capable of recognizing deceptive tactics, assessing the credibility of information, making informed decisions, and protecting themselves from fraudulent schemes.

Public education serves as one of the most effective preventive mechanisms against scams because informed citizens are less vulnerable to manipulation and misinformation. Educational institutions, governments, financial institutions, media organizations, and civil society can collectively strengthen public awareness through structured financial education, cyber security campaigns, digital literacy initiatives, and community-based outreach programs. Rather than relying solely on law enforcement after fraud has occurred, preventive education empowers individuals to detect warning signs before becoming victims.

This paper presents a conceptual analysis of the relationship between risk literacy, scam prevention, and public education by reviewing recent literature, policy initiatives, and emerging challenges. The study argues that integrating risk literacy into educational curricula and lifelong learning programs is essential for building a digitally secure and financially resilient society. The paper concludes that public education should be regarded not merely as an awareness campaign but as a long-term national strategy for reducing fraud, enhancing consumer confidence, and promoting responsible digital citizenship.

Keywords: Risk Literacy, Scam Prevention, Public Education, Financial Literacy, Digital Literacy, Cyber Fraud, Consumer Protection, Online Scams.

1. Introduction

The twenty-first century has witnessed unprecedented growth in digital technologies that have fundamentally altered the nature of commerce, communication, governance, and everyday life. Internet banking, mobile payment systems, e-commerce platforms, social networking applications, and artificial intelligence have simplified numerous aspects of modern living. However, alongside these advancements, cybercriminals have continuously adapted their methods to exploit technological innovations and human vulnerabilities. Fraud has evolved from conventional financial deception into highly sophisticated digital scams capable of targeting millions of individuals simultaneously.

Modern scams rarely depend solely on technological weaknesses. Instead, they frequently exploit psychological biases such as fear, urgency, trust, greed, curiosity, and emotional attachment. Fraudsters manipulate victims through phishing emails, fake investment opportunities, impersonation of government officials, romance scams, lottery fraud, fake employment offers, cryptocurrency fraud, and fraudulent customer support services. These scams often appear legitimate because criminals employ professional websites, artificial intelligence-generated content, deepfake technologies, and convincing social engineering techniques.

One of the most effective strategies to combat these evolving threats is the development of **risk literacy**. Risk literacy refers to an individual's capacity to understand uncertainty, interpret risk-related information, evaluate probabilities, distinguish reliable information from deception, and make informed decisions under uncertain circumstances. Risk-literate individuals are less likely to become victims of scams because they critically evaluate suspicious offers instead of reacting impulsively.

Public education complements risk literacy by disseminating knowledge at the societal level. Awareness campaigns, financial education programs, cyber security workshops, school curricula, media literacy initiatives, and community engagement activities collectively strengthen citizens' ability to identify fraudulent activities before financial or personal damage occurs. Unlike reactive law enforcement approaches, preventive education reduces victimization by addressing the root causes of vulnerability.

The importance of this issue has increased considerably following the rapid digitization of financial services during recent years. The expansion of digital payment systems and online financial transactions has improved accessibility but has also widened opportunities for cybercriminals. Individuals with limited digital literacy, elderly citizens, rural populations, and first-time internet users remain particularly vulnerable because they may lack sufficient understanding of online security practices.

International organizations, including the **Organization for Economic Co-operation and Development (OECD)**, the **World Bank**, and the **International Telecommunication Union (ITU)**, have consistently emphasized the importance of financial education, digital literacy, and consumer awareness as essential components of economic resilience and cyber security. Many governments have therefore adopted national strategies aimed at strengthening public awareness and consumer protection through coordinated educational initiatives.

The present study examines the conceptual relationship between risk literacy, scam prevention, and public education. It argues that sustainable fraud prevention requires not only technological safeguards and legal enforcement but also informed citizens capable of recognizing and responding effectively to emerging risks. Developing risk literacy should therefore become an integral component of national education systems and lifelong learning programs.

2. Literature Review

Research on risk literacy has expanded significantly over the past two decades as scholars increasingly recognize that individuals often make decisions under conditions of uncertainty. Early studies primarily examined statistical reasoning and probability estimation; however, contemporary research views risk literacy as a multidimensional competency encompassing critical thinking, financial knowledge, digital awareness, media literacy, and behavioral decision-making.

Gigerenzer (2014) argued that individuals who understand probabilities and statistical information are better equipped to make rational decisions in health, finance, and public policy. According to his framework, risk literacy enables people to distinguish genuine risks from manipulated information, thereby reducing susceptibility to deception.

The **OECD (2023)** emphasized that financial literacy and digital financial literacy are indispensable for consumer protection in increasingly digital financial markets. Its research indicates that individuals possessing stronger financial knowledge demonstrate greater confidence in identifying fraudulent financial products and online investment scams.

Similarly, the **World Bank (2022)** highlighted that digital financial inclusion should be accompanied by comprehensive consumer education. While digital banking expands financial access, inadequate awareness regarding cyber security significantly increases the likelihood of fraud among new users.

Studies on cybercrime consistently identify **social engineering** as one of the most successful strategies employed by scammers. Rather than exploiting software vulnerabilities alone, criminals manipulate human psychology through persuasion, authority, fear, urgency, or emotional attachment. **Hadnagy (2018)** explained that cybercriminals deliberately exploit cognitive biases and emotional responses because human behavior often represents the weakest link in cyber security.

Recent research has also explored the relationship between media literacy and scam prevention. **Livingstone (2020)** observed that misinformation, fake news, manipulated digital content, and fraudulent online advertisements have blurred the distinction between authentic and deceptive information. Individuals capable of critically evaluating digital information are less likely to trust fraudulent communications.

Financial education has emerged as another important dimension of risk literacy. According to **Lusardi and Mitchell (2023)**, financially literate individuals are better able to assess investment risks, recognize unrealistic promises of guaranteed returns, and avoid fraudulent financial schemes. Their studies demonstrate that financial literacy contributes directly to household financial resilience.

Educational researchers have increasingly advocated integrating cyber security awareness into school curricula. **UNESCO (2023)** emphasized that digital citizenship education should extend beyond technical skills to include ethical online behavior, privacy protection, information verification, and cyber safety. Such education enables students to become responsible participants in digital society while reducing their vulnerability to online fraud.

Several empirical studies indicate that public awareness campaigns significantly improve scam recognition. Community workshops, mass media campaigns, interactive digital learning modules, and financial awareness programs have shown measurable improvements in participants' ability to identify phishing messages, fraudulent websites, and deceptive investment offers.

Despite these advances, researchers acknowledge several limitations. Public awareness campaigns often reach urban and educated populations more effectively than marginalized communities. Elderly individuals, persons with limited digital access, and populations with lower educational attainment continue to experience disproportionately higher levels of victimization. Furthermore, the rapid evolution of artificial intelligence, deep fake technologies, and automated fraud techniques requires continuous updating of educational materials.

The literature therefore demonstrates broad consensus that technological solutions alone cannot eliminate scams. Sustainable fraud prevention requires an integrated approach combining legal regulation, cyber security infrastructure, financial literacy, digital education, media literacy, and public awareness. Risk literacy serves as the connecting framework that enables individuals to apply knowledge effectively when confronted with uncertain or deceptive situations.

---

3. Objectives of the Study

The present study seeks to achieve the following objectives:

1. To examine the concept and dimensions of risk literacy in the context of financial and digital security.
2. To analyses the growing nature and characteristics of modern scams affecting individuals and society.
3. To evaluate the role of public education in enhancing scam awareness and prevention.
4. To assess the contribution of financial literacy, digital literacy, and media literacy in reducing fraud vulnerability.
5. To identify major challenges in promoting risk literacy among diverse population groups.
6. To suggest policy recommendations for strengthening public education and developing a risk-aware society.

---

4. Research Methodology

This study is based on a **descriptive and analytical research design** using secondary sources of information. Relevant literature was collected from peer-reviewed journal articles, books, and government publications, reports of international organizations, cyber security reports, policy documents, and research papers relating to risk literacy, financial literacy, scam prevention, consumer protection, digital education, and cybercrime.

The collected information was critically reviewed and organized through thematic analysis. Major themes—including risk literacy, behavioral vulnerability, financial fraud, public awareness, digital education, and policy interventions—were identified and analyzed to understand their interrelationships. The study does not involve primary data collection; rather, it synthesizes existing knowledge to develop a comprehensive conceptual understanding of how risk literacy and public education contribute to scam prevention in contemporary digital society.

Given the rapid evolution of digital fraud, emphasis has been placed on recent academic literature and policy documents published during the past decade, while also incorporating seminal works that have significantly influenced the development of risk literacy research.

5. Risk Literacy: Concept, Dimensions and Importance

Risk is an inseparable component of modern life. Individuals encounter risks while making financial investments, sharing personal information online, using digital payment systems, purchasing products through e-commerce platforms, or responding to unsolicited communications. The ability to recognize, evaluate, and manage these uncertainties is referred to as **risk literacy**. Unlike general literacy, which focuses primarily on reading and writing skills, risk literacy equips individuals with the knowledge and judgment required to make informed decisions in uncertain situations.

Risk literacy encompasses multiple dimensions. The first is **financial literacy**, which enables individuals to understand concepts such as interest rates, investment returns, inflation, credit, insurance, and financial fraud. People with sound financial knowledge are generally better able to evaluate investment opportunities and avoid schemes that promise unrealistic profits.

The second dimension is **digital literacy**, which involves the ability to use digital technologies safely and responsibly. Digital literacy includes understanding online privacy, password security, two-factor authentication, secure browsing, and responsible use of social media. As financial and governmental services increasingly move online, digital literacy has become essential for protecting personal information and financial assets.

Another important dimension is **media and information literacy**. The digital environment exposes users to an enormous volume of information, much of which may be misleading or intentionally deceptive. Media literacy enables individuals to verify information sources, distinguish credible content from misinformation, and critically evaluate online messages before acting upon them. This skill is particularly important because many scams rely on false information presented through convincing websites, advertisements, emails, or social media posts.

Risk literacy also includes **behavioural awareness**. Research in behavioural economics has demonstrated that decision-making is often influenced by emotions rather than rational analysis. Fraudsters deliberately exploit psychological tendencies such as fear, urgency, greed, sympathy, curiosity, and trust. A risk-literate individual recognizes these emotional triggers and takes time to verify information before making decisions.

From a societal perspective, risk literacy contributes to economic stability and public confidence. Individuals who understand financial and digital risks are less likely to become victims of fraud, resulting in lower financial losses, reduced legal disputes, and greater trust in digital financial systems. Consequently, promoting risk literacy benefits not only individuals but also governments, financial institutions, and the broader economy.

---

6. Understanding Modern Scams and Their Emerging Forms

Technological innovation has transformed traditional fraud into sophisticated digital scams capable of reaching millions of potential victims across geographical boundaries. Modern scams often combine technological expertise with psychological manipulation, making them increasingly difficult to identify.

One of the most widespread forms is **phishing**, in which criminals impersonate trusted organizations such as banks, government agencies, or online service providers. Victims receive emails, text messages, or phone calls requesting confidential information, passwords, or one-time passwords (OTPs). These communications often appear authentic, making unsuspecting users vulnerable to identity theft and financial loss.

Investment scams have also expanded rapidly in the digital era. Fraudsters promise unusually high returns through crypto currency investments, foreign exchange trading, fake stock markets, or fraudulent online investment platforms. Such schemes frequently exploit limited financial knowledge and the desire for quick profits.

Another growing concern is **romance scams**, where criminals establish emotional relationships through social networking platforms or dating applications before requesting financial assistance. Victims often suffer both financial losses and psychological distress because the deception involves emotional manipulation over an extended period.

Job and employment scams target unemployed individuals and recent graduates by advertising attractive employment opportunities requiring advance registration fees, training charges, or document verification payments. Similarly, **lottery and prize scams** falsely inform victims that they have won substantial rewards but must first pay taxes or processing charges to receive their winnings.

The rapid adoption of artificial intelligence has introduced new challenges through **deepfake scams**. Fraudsters now use AI-generated audio and video recordings to impersonate family members, employers, or public officials. These highly realistic digital manipulations significantly increase the credibility of fraudulent communications and complicate traditional methods of verification.

Cybercriminals also exploit **social engineering**, which relies more on manipulating human behavior than on attacking technological systems. By creating a false sense of urgency or authority, scammers encourage victims to disclose confidential information without carefully verifying the authenticity of requests.

These developments indicate that technological advancement alone cannot eliminate fraud. Instead, citizens must possess sufficient knowledge and critical thinking skills to identify warning signs before responding to suspicious communications.

---

7. The Role of Public Education in Scam Prevention

Public education represents one of the most effective and sustainable approaches to preventing scams. While law enforcement agencies investigate fraud after it occurs, education reduces victimization by empowering individuals to recognize fraudulent activities before financial or personal damage takes place.

Educational institutions play a foundational role in developing risk awareness from an early age. Schools and universities can integrate financial literacy, digital citizenship, cyber security awareness, and critical thinking into their curricula. Students who understand online privacy, password security, misinformation, and responsible digital behaviour are better prepared to navigate increasingly complex digital environments throughout their lives.

Community education programs are equally important, particularly for adults and senior citizens who may have limited exposure to rapidly changing digital technologies. Workshops conducted by banks, local governments, non-governmental organizations, and consumer protection agencies can improve awareness regarding emerging fraud techniques and safe financial practices.

Mass media serves as another influential educational platform. Television, radio, newspapers, and digital media campaigns can rapidly disseminate information about newly emerging scams and practical preventive measures. Public service announcements explaining common fraud tactics, warning signs, and reporting procedures significantly enhance community preparedness.

Financial institutions also bear substantial responsibility for consumer education. Banks, insurance companies, payment service providers, and **fintech** organizations increasingly provide cyber security guidance through mobile applications, websites, SMS alerts, and awareness campaigns. These initiatives encourage customers to verify suspicious communications, protect confidential credentials, and immediately report unauthorized transactions.

Social media platforms have become both a source of scams and an important channel for awareness. Governments and consumer organizations increasingly utilize social media to distribute verified information, clarify misinformation, and educate citizens regarding emerging fraud trends. Interactive videos, infographics, webinars, and short educational messages can effectively reach younger audiences who rely heavily on digital communication.

An effective public education strategy should extend beyond occasional awareness campaigns. It requires continuous learning opportunities that evolve alongside technological developments and emerging cyber threats. Lifelong education ensures that citizens remain informed about new forms of fraud and changing digital risks throughout their lives.

---

8. Government and International Initiatives for Risk Literacy and Scam Prevention

Governments across the world have increasingly recognized that consumer protection requires both regulatory enforcement and public education. Consequently, many countries have developed national strategies aimed at strengthening financial literacy, cybersecurity awareness, and digital inclusion.

The **Organization for Economic Co-operation and Development (OECD)** has consistently promoted financial literacy as a key component of consumer protection and economic resilience. Through its International Network on Financial Education (INFE), the organization encourages member countries to develop national financial education strategies that improve citizens' ability to make informed financial decisions and recognize fraudulent schemes.

The **World Bank** supports financial capability programs that integrate digital financial education with consumer protection measures. Its initiatives emphasize that expanding digital financial services should be accompanied by adequate public awareness regarding cyber security, online fraud, and responsible financial behaviour.

The **International Telecommunication Union (ITU)** promotes cyber security awareness through global capacity-building programs, digital skills training, and public education campaigns. These initiatives encourage governments to strengthen national cyber security cultures by educating citizens about safe online practices.

In India, several government initiatives have contributed to scam prevention and financial awareness. The **Reserve Bank of India (RBI)** regularly conducts public awareness campaigns regarding safe banking practices, digital payment security, and fraud prevention. Banks are encouraged to educate customers about phishing, OTP fraud, unauthorized transactions, and secure digital banking practices.

The **National Cyber Crime Reporting Portal** has improved public access to cybercrime reporting while simultaneously raising awareness regarding online fraud. Cyber awareness campaigns organized under the **Indian Cyber Crime Coordination Centre (I4C)** emphasize responsible digital behavior and encourage citizens to report suspicious online activities promptly.

The expansion of digital payment systems under initiatives such as Digital India has further highlighted the need for widespread digital literacy. Public education programs increasingly focus on secure digital transactions, privacy protection, and responsible use of financial technologies to ensure that technological progress is accompanied by consumer safety.

Collectively, these national and international initiatives demonstrate that scam prevention is most effective when education, regulation, technology, and law enforcement operate in an integrated and coordinated manner.

9. Challenges in Promoting Risk Literacy and Scam Prevention

Despite significant advancements in financial education and cyber security awareness, several challenges continue to hinder the effective promotion of risk literacy across societies. The rapid pace of technological innovation often outstrips the ability of educational institutions, governments, and regulatory agencies to update public awareness programs. Consequently, many citizens remain unaware of emerging fraud techniques until they become victims.

One of the primary challenges is the **digital divide**. Although internet connectivity has expanded considerably, disparities in digital access and technological skills persist between urban and rural populations, younger and older generations, and economically advantaged and disadvantaged communities. Individuals with limited exposure to digital technologies frequently lack the confidence and knowledge necessary to identify online scams or protect their personal information.

Another major challenge is **low financial literacy**. Many individuals possess limited understanding of investment principles, digital banking, credit management, and financial risk. Fraudsters exploit this knowledge gap by promoting unrealistic investment opportunities, fake financial products, and misleading loan or insurance schemes. The increasing popularity of crypto currencies and online investment platforms has further complicated financial decision-making for ordinary consumers.

The growing sophistication of cybercriminals also presents a significant obstacle. Artificial intelligence, **deepfake** technology, automated phishing systems, and personalized social engineering attacks have made fraudulent communications increasingly difficult to distinguish from genuine interactions. Criminals now use publicly available personal information obtained from social media to create highly convincing scams that exploit trust and emotional vulnerability.

Psychological factors further complicate scam prevention. Fraudsters deliberately create situations involving urgency, fear, excitement, or sympathy to discourage victims from carefully evaluating information. Even highly educated individuals may become victims when emotional manipulation overrides rational judgment. Therefore, risk literacy must address behavioral aspects of decision-making in addition to technical knowledge.

Another challenge involves the rapid spread of misinformation through digital platforms. False news, manipulated videos, fake advertisements, and fraudulent websites circulate quickly across social media, making it difficult for users to verify information. Without adequate media literacy, individuals may unknowingly share misleading content that facilitates further fraudulent activities.

Finally, public awareness campaigns often suffer from limited continuity and unequal outreach. Awareness programs may receive considerable attention following major fraud incidents but gradually lose visibility over time. Sustained educational efforts targeting schools, workplaces, rural communities, and senior citizens remain essential for long-term behavioral change.

10. Recommendations

Developing a risk-literate society requires coordinated action involving governments, educational institutions, financial organizations, technology companies, civil society, and individual citizens. Based on the findings of this study, the following recommendations are proposed:

First, risk literacy should be integrated into school, college, and university curricula. Students should receive practical education on financial management, digital safety, cyber security, information verification, and responsible online behavior from an early stage of learning.

Second, governments should establish comprehensive national awareness campaigns that provide timely information about emerging scams. Public education initiatives should utilize television, radio, newspapers, community programs, mobile applications, and social media to reach diverse population groups.

Third, financial institutions should expand customer education beyond regulatory compliance. Banks and digital payment providers should regularly organize workshops, distribute educational materials, and provide real-time fraud alerts that help consumers identify suspicious transactions and fraudulent communications.

Fourth, special attention should be given to vulnerable populations, including senior citizens, rural communities, women, first-time internet users, and individuals with limited financial knowledge. Educational programs should be designed in local languages and adapted to varying literacy levels to ensure wider accessibility.

Fifth, digital platforms and technology companies should strengthen mechanisms for detecting fraudulent content, fake websites, phishing messages, and impersonation accounts. Artificial intelligence should be used not only by cybercriminals but also by security organizations to identify and prevent fraudulent activities.

Sixth, media literacy programs should encourage citizens to verify information before sharing it through digital platforms. Critical thinking, source verification, and fact-checking should become integral components of public education.

Finally, governments should encourage collaboration among regulatory agencies, financial institutions, educational organizations, law enforcement authorities, cyber security experts, and civil society. An integrated approach combining education, regulation, technological innovation, and effective law enforcement will produce more sustainable outcomes than isolated interventions.

---

11. Conclusion

The expansion of digital technologies has transformed economic and social life while simultaneously creating new opportunities for cyber-enabled fraud. Modern scams have become increasingly sophisticated, combining technological innovation with psychological manipulation to exploit human vulnerabilities. As a result, protecting citizens from financial and digital fraud requires more than advanced cyber security systems or stricter legal regulations. It requires individuals who possess the knowledge, critical thinking abilities, and behavioral awareness necessary to recognize and respond effectively to uncertain situations.

Risk literacy provides the intellectual foundation for informed decision-making by enabling individuals to understand probabilities, evaluate risks, verify information, and resist deceptive persuasion. When combined with financial literacy, digital literacy, and media literacy, it substantially reduces vulnerability to scams and strengthens consumer confidence in digital environments.

Public education represents one of the most cost-effective and sustainable strategies for scam prevention. Educational institutions, governments, financial organizations, media, and community groups all play complementary roles in developing informed and responsible digital citizens. Continuous awareness programs, practical learning experiences, and inclusive educational initiatives can empower individuals across all age groups to recognize emerging fraud techniques before financial losses occur.

The findings of this study suggest that risk literacy should no longer be viewed as a specialized competency reserved for financial professionals or cyber security experts. Instead, it should be recognized as a fundamental life skill essential for participation in modern society. Investing in public education and lifelong learning will not only reduce the incidence of scams but also contribute to financial inclusion, digital trust, consumer protection, and sustainable economic development. As digital transformation continues to reshape global society, strengthening risk literacy will remain a critical priority for governments, educators, policymakers, and citizens alike.

References (APA 7th Edition)

Gigerenzer, G. (2014). *Risk savvy: How to make good decisions*. Viking.

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

International Telecommunication Union. (2023). *Global cyber security index 2023*. ITU.

Lusardi, A., & Mitchell, O. S. (2023). *The importance of financial literacy: Theory and evidence*. Journal of Economic Literature, 61(4), 1225–1263.

Organisation for Economic Co-operation and Development. (2023). *OECD/INFE international survey of adult financial literacy*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2022). *Recommendation on financial literacy*. OECD Publishing.

Reserve Bank of India. (2024). *Annual Report 2023–24*. Reserve Bank of India.

Reserve Bank of India. (2024). *RBI Kehta Hai: Financial awareness and safe digital banking initiatives*. Reserve Bank of India.

United Nations Educational, Scientific and Cultural Organization. (2023). *Global education monitoring report: Technology in education*. UNESCO.

World Bank. (2022). *Digital financial inclusion*. World Bank.

World Economic Forum. (2023). *Global risks report 2023*. World Economic Forum.

National Crime Records Bureau. (2023). *Crime in India 2023*. Ministry of Home Affairs, Government of India.

Indian Cyber Crime Coordination Centre. (2024). *Cyber awareness handbook*. Ministry of Home Affairs, Government of India.

Federal Bureau of Investigation. (2024). *Internet Crime Report 2023*. FBI Internet Crime Complaint Center.

European Union Agency for Cyber security. (2023). *ENISA Threat Landscape 2023*. ENISA.

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

NIST. (2024). *Cyber security Framework (CSF) 2.0*. National Institute of Standards and Technology.

World Health Organization. (2022). *Infodemic management: An overview*. WHO.

United Nations Office on Drugs and Crime. (2023). *Global study on cybercrime*. UNODC.

Consumer Financial Protection Bureau. (2024). *Fraud prevention and consumer protection*. CFPB.