Int. j. adv. multidisc. res. stud. 2026; 6(3):2058-2061

Received: 07-05-2026
Accepted: 17-06-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Emerging Cyber Threats and Digital Safety: A Review of Cybercrime, Disinformation, and Financial Fraud

[1] Dr. Mukta Sathisha, [2] Sowmya KN

[1, 2] Assistant Professor, Division of Languages, School of Life Sciences, JSS Academy of Higher Education and Research, Mysuru, India

DOI: https://doi.org/10.62225/2583049X.2026.6.3.6530
Corresponding Author: **Dr. Mukta Sathisha**

Abstract

Cybercrime has become a major worldwide issue that impacts people, businesses, and governments in equal measure. This review article looks at current problems with digital financial fraud, misinformation, disinformation, cybercrime, and cybersecurity in the digital age. The report draws attention to the growing worries about identity theft, financial fraud, internet scams, fake news, and technology weaknesses that impact people all around the world. The significance of digital financial literacy as a crucial skill needed to enable safe engagement in an increasingly digital economy is also examined. Evidence from EU members, Africa and Asia emphasizes the necessity of inclusive policy frameworks, technology safeguards, and behavioural interventions to confront new cyber threats. Improving cybersecurity necessitates a multifaceted strategy that includes public awareness, digital literacy, technology protection, regulatory changes, and international cooperation. Building a secure and resilient digital society still requires raising citizens' understanding of cybersecurity and digital finance.

Keywords: Cyber Threats, Digital Safety, OECD

1. Introduction

The endless space known as the web is referred to as ‘cyber-space’ and the set of regulations designed to safeguard the internet is known as cyber-security. The term ‘cybercrime’ represents a group of organized crimes that target both cyberspace and cybersecurity. Because threats to cyber security now need to be treated more seriously, cyber security has become a global problem [1].

Fake news, misinformation, and disinformation are now considered as emerging risks in the digital world [2] The inadvertent dissemination of incorrect information on the internet is known as online misinformation. Because of its general risk and the threat, it poses to maintaining democratic integrity, standard journalism, and an educated public, especially during times of crisis, it has drawn increasing public and scholarly attention and concern [3].

People are obtaining news via websites, news portals, social media, and other digital news platforms instead of traditional mass media. People encounter misleading material on the Internet if they rely solely on it for all of their information. Any information that lacks a legitimate and trustworthy source or that is likely to mislead the public is referred to as false or fake news [4].

The objective and content type are the primary distinctions between misinformation, disinformation, and fake news. Fake news is a general phrase for manufactured articles that pass for genuine journalism, misinformation is deceptive data that is accidentally transmitted, and disinformation is a purposeful deception intended to deceive. Spreading false information or slanderous propaganda with dangerous repercussions is known as fake news. In the twenty-first century, fake news is taking over social media journalism [5].

Individual financial security is seriously jeopardized by these issues, especially for varied and digitally heterogeneous communities. Disinformation and fake news are widely acknowledged as significant global concerns that affect citizen safety, public wellness, information environments, democratic processes, and public confidence. Disinformation impedes access to factual data, erodes trust in public institutions and the media, and threatens social harmony, according to international organizations like UNESCO. Misinformation and disinformation competencies are now specifically addressed in UNESCO's

media and information literacy frameworks as crucial skills for digital citizens. These international frameworks were transformed into educational resources and valuable tools, such as fact-checking procedures and disinformation typologies, for discriminating between genuine and fraudulent content.

2. Rapid digital financial growth coupled with increased incidents of digital scams

India's expansion of digital financial ecosystems — particularly UPI and mobile payments has reaped economic and inclusion benefits made possible by government initiatives, owning of smart phones and internet outreach in the rural areas [6].

Though the use of digital payments has eased financial transactions for consumers, it has also let to an increase in online frauds, which has become a challenge for individuals and financial institutions. Findings of studies on online digital fraud indicate that the main causes of fraud are low awareness, cybersecurity flaws, financial illiteracy, and technological complexity. While non-victims draw attention to cybersecurity vulnerabilities and sluggish investigations, victims note financial illiteracy and technological complexity [4].

Such nationwide trends highlight digital financial literacy as one of the most important digital competencies which must complement financial inclusiveness with technology [5].

While the Indian government and law enforcement organizations have taken significant actions to prevent online criminal activity, there are still a lot of vulnerabilities, which indicates that more comprehensive and long-term measures are essential. Only 60% of cybercrime officers interviewed felt that Indian Cyber Crime Coordination Centre (I4C) and the 1930 National Cybercrime Helpline, established by the Ministry of Home Affairs was very effective in combating cyber-crime, while only 45% believed that the IT Act 2000 was very effective. 60% believed that the National Security Policy was effective while only 54% believed that the personal data protection bill was effective [6].

The rise of cybercrime in India has made it necessary to establish a single enforcement system that can handle the intricate, international character of cybercrimes [7].

Google's DigiKavach program has worked with Indian stakeholders to detect and reduce the risks of online fraud using digital efforts [8].

The Sanchar Saathi App is known for its call and complaint centre to report digital fraud, trace stolen phones and assist users in case they buy a phone with a fake IMEI, or fall victim to a SIM swap. The government advertised it as a digital emergency service, in December 2024. It can be voluntarily downloaded by users, though preinstallation of the app is not mandatory by mobile phone manufacturers [12].

Scammers use fake KYC updates, payment alerts, and urgent messages to trick users into sharing sensitive information. Mobile phone manufacturers and app developers are faced with the crucial task of protecting mobile apps from numerous risks as fraudsters constantly change their strategies. These initiatives must emphasize the importance of media literacy and cyber security education in national cyber resilience plans. Adopting cutting-edge technology like blockchain, artificial intelligence, and quantum-resistant cryptography while upholding core security principles is one way to combat phishing and digital fraud. A more secure mobile app ecosystem can be created by putting security first throughout the app development lifecycle, putting multi-layered defence tactics into practice, and cultivating a user base that is security conscious. By protecting private data and guaranteeing the integrity of mobile applications in an increasingly interconnected environment, the ultimate objective is to establish and preserve user confidence [13].

Over 900 million people in India use digital media, but misinformation is widespread, weakening public trust and triggering contentious debates. In order to confirm media credibility and check false information, fact-checking organizations like Alt News and Boom have become essential [9].

These organizations provide a larger environment where academic studies on misinformation literacy are pertinent and effective.

Thawornwichian W presents the OECD Truth Quest Survey methodology and significant findings and adds to the corpus of literature on misinformation and fake news [15]. Online false and misleading content puts people's health and society at serious danger, but there is still a dearth of cross-national comparable data. This study analyses if certain content categories are easier to determine as deceitful and untrue than others, and whether the theme has any bearing on this identification. It offers information on the effects of AI labelling as well as evidence regarding whether AI-generated content is simpler to recognize than human-generated content. The OECD highlights that individual empowerment via literacy and resilience building—rather than depending entirely on technology or policy—is essential to combat disinformation. The importance and effectiveness of educational measures to promote information integrity are further demonstrated by recent OECD research, which also demonstrate that media literacy interventions may significantly reduce the intent to spread deceptive material online. Global efforts to counter misinformation and online scams include collaborative intergovernmental actions. The accuracy and flow of information from a number of sources are crucial to a successful as well as inclusive digital economy and society. The present scenario of research suggests that in order to assess and manage systemic risks, governance capability must be strengthened, and availability of data must be broadened [16].

Developing digital policies and evaluating the effects of governance reforms on the information domain are difficult without an empirical foundation. Some of the strategies to combat online misinformation and fake news include 34 states signing the Global Declaration on Information Integrity Online in 2023. This urges signatories to refrain from participating in state-led disinformation efforts, denounce them, and refrain from restricting free speech in the name of combating misinformation. Recent transnational initiative such as the International Conference on the Global Partnership Against Online Scams held in Bangkok on December 17–18, 2025, brought together more than 300 participants from over sixty nations to address the rapidly expanding transnational scam centres. Thailand contributed to the start of an international campaign to stop the proliferation of internet scams, which involve criminal organizations primarily based in Southeast Asia that are thought to defraud victims worldwide of billions of dollars each year. These initiatives demonstrate how media and

digital literacy, together with cyber security awareness, are increasingly viewed by countries and global institutions as fundamental components of systemic responses to online scams.

Scams are widespread around the world, and their effects negatively impact both national security and private privacy. In Bangladesh, financial scams are becoming more common as many financial firms continue to use political influence to embezzle public funds. Though countries like Singapore has made significant progress in addressing different scam types through its community initiatives, while Bangladesh has not yet developed a strict regulatory framework for such crime [1, 17] Globally, countries should effectively address the dynamic and always changing nature of online frauds by promoting international alliances and placing a strong emphasis on data-driven legislation. Countries like Nigeria has witnessed an increase in cyber-crimes in recent times The internet has contributed to the advancement of fraudulent practices among youth in Nigeria, who view online fraud as a widely recognized avenue for financial support. The rise of the online crime subculture has been exacerbated by the governmental leadership's corruption [1] One of the main reasons why young people are involved in online fraud is the importance and value placed on accumulating money.

The sociodemographic, non-cognitive, and cognitive elements linked to fraud victimization were investigated using a systematic review, with an emphasis on how these elements change according on the type of fraud and age group. Three scientific databases—PsycINFO, Scopus, and PubMed—were thoroughly searched in accordance with PRISMA principles. The findings indicated a fragmented landscape, suggesting that fraud victims cannot be treated as a homogeneous group [18].

In addition to improving convenience and inclusivity, the European Union's (EU) quick digitalization of financial services has raised vulnerability to advanced online financial scams. A popular strategy for educating customers and lowering fraud victims is digital financial literacy. Findings of a study done on online scams in the European Union show that behavioural insights, technology protection, and non-discriminatory policy considerations are all necessary for the successful deployment of digital financial literacy interventions [19].

International organizations working on media literacy like Debunk.org, a Lithuanian-born project brings together volunteers and media outlets to monitor more than 2,500 websites in 26 languages in order to detect and evaluate disinformation efforts [20].

Online fraud and cybercrime are now seen by international frameworks as being entwined with disinformation, fake news and misinformation. The transnational scope of online scams and the necessity of integrated strategies that incorporate preventive education, law enforcement, and cyber resilience are highlighted in international conversations, such as those taking place in Southeast Asia. Trusted News Initiative (TNI), founded by BBC, is an active collaboration of media organizations and digital platforms across the globe, partnered by AP, AFP, BBC, CBC/Radio-Canada, European Broadcasting Union (EBU), Financial Times, Information Futures Lab, Google/YouTube, The Hindu, The Nation Media Group, Meta, Microsoft, Thomson Reuters, Reuters Institute for the Study of Journalism, Twitter, The Washington Post, Kompas (Indonesia), Dawn (Pakistan), Indian Express, NDTV (India), ABC (Australia), SBS (Australia), and NHK (Japan) [21]. Members of TNI engage to address issues of misinformation and to foster audience trust. It is the first forum of its kind in the world created to combat misinformation in real time since it incorporates social media platforms and media organizations.

3. Conclusion

By improving communication, information access and the swift expansion of cyberspace has profoundly changed the system of financial transactions. But this technological progress has also made people more vulnerable to online fraud, disinformation, and dangers to digital security. The research examined in this article shows that cyber risks have grown to be a significant worldwide issue that affects people, businesses, and countries equally. Fake news, phishing attacks, financial scams, identity theft, and digital fraud are becoming more common, which emphasizes the critical need for more robust cybersecurity defences and more public awareness. The intricate and ever-changing nature of cyber dangers cannot be adequately addressed by technology solutions like Sanchar Saathi and DigiKavach alone. Media literacy, cybersecurity awareness, and digital financial literacy have become critical skills for safe engagement in the digital world. The significance of cooperative strategies including governments, tech firms, academic institutions, and civil society organizations is further highlighted by international initiatives to fight disinformation and online fraud. Experiences from several nations show that a collaborative perspective on behavioural insights, technology protections, regulatory changes, and public education are necessary for successful interventions. It requires continuous financial support for cybersecurity infrastructure, digital literacy initiatives, and international collaboration to create a safe and reliable digital ecosystem. In an increasingly interconnected world, lowering vulnerabilities and guaranteeing the safe and ethical use of digital technologies depend on strengthening users' awareness and resilience against cyber-attacks.

4. References

1. Ibikunle F, Odunayo E. Approach to Cyber Security Issues in Nigeria: Challenges and Solution. International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE) [Internet]. [Cited 2026 Apr 13], Jun 20, 2013; 1(1):100-110. Available from: https://www.ijcrsee.com/index.php/ijcrsee/article/view/65/558
2. Petratos PN. Misinformation, disinformation, and fake news: Cyber risks to business. Bus Horiz, Nov 1, 2021; 64(6):763-774. Doi: 10.1016/J.BUSHOR.2021.07.012
3. Vadapalli SK, Doyal S, Vanheusden FJ, Binder JF, Kuss DJ. Exploring the impact of online misinformation on ideological polarisation and institutional distrust: An integrative review and strategic framework for counteraction. SN Social Sciences, Feb 23, 2026; 6(3):87. Doi: 10.1007/S43545-026-01349-0
4. Pandey B, Kumar G, Algavi LO, Kumar M, Sharma V. Exposure of fake news to the indian social media users. RUDN Journal of Studies in Literature and Journalism. 2023; 28(2):381-396. Doi: 10.22363/2312-9220-2023-28-2-381-396

5. Dr. Durgesh Tripathi, Priyanka Sachdeva. Is Fake News and Veracity Intermingled? Perilous Effect of Social Media Fake News on Indian Societies. International Journal of Communication Development, Jun 30, 2019, 68-78. Doi: 10.65301/IJCD.2019.9.3.4.12
6. Jain A. Digital payments in India: Trends, growth analysis and future prospects. ~ 444 ~ International Journal of Research in Finance and Management. 2025; 8(2):444-449. Doi: 10.33545/26175754.2025.v8.i2e.571
7. Amit Kumar Singh, Krishna Kumar Agarwal. An Overview of Digital Payment Frauds: Causes, Consequences, and Countermeasures. Journal of Informatics Education and Research, Feb 25, 2025; 5(1). Doi: 10.52783/JIER.V5I1.2230
8. Desy Wulan Ayuning Gumilar, Khresna Bayu Sangka, Salman Alfarisy Totalia. Digital Financial Literacy and Digital Financial Inclusion in the Era of Digital Disruption: Systematic Literature Review. Formosa Journal of Multidisciplinary Research, May 30, 2024; 3(5):1563-1576. Doi: 10.55927/FJMR.V3I5.9213
9. Joshi D. Navigating Cybercrime in India's Digital Era: Current Trends and Challenges. Int J Sci Res Sci Technol [Internet]. [Cited 2026 Apr 13]. 2024; 11(10). Available from: www.ijsrst.com
10. Goyal HR. Strengthening Cyber Policing in India: A Critical Study of the Role and Reform of the Indian Cyber Crime Coordination Centre (I4c). J Neonatal Surg, Jul 14, 2025; 14(32S):10430-10437. Doi: 10.63682/JNS.V14I32S.9955
11. Keeping India Safer Online with Google - Safety Centre [Internet]. [Cited 2026 Apr 13]. Available from: https://safety.google/intl/en_in/safety/engineering-center/engineering-center-india/
12. Dr. A Shaji George. View of Sanchar Saathi Digital Security versus Civil Liberty in India's Smartphone Era. Partners Universal International Research Journal [Internet]. [Cited 2026 Jun 21], Dec 26, 2025; 4(4):1-22. Available from: https://puirj.com/index.php/research/article/view/231/183
13. Muthineni SR. Enhancing Mobile App Security: Protecting Against Common Threats. International Journal of Computer Engineering and Technology, Jan 6, 2025; 16(1):186-198. Doi: 10.34218/IJCET_16_01_017
14. Nishant Sagar, Dr. Manoj Kumar Srivastava. The Role of Fact-Checking Initiatives in Indian Media: Strengthening Credibility in the Digital Age. Innovative Research Thoughts, Dec 28, 2025; 11(4):194-198. Doi: 10.36676/IRT.V11.I4.1740
15. Thawornwichian W. The OECD Truth Quest Survey: Methodology and findings. OECD Digital Economy Papers. OECD Digital Economy Papers, Jun 28, 2024; 369. Doi: 10.1787/92A94C0F-EN
16. Gillwald A, Berger G, Orembo E. Mapping the Information Integrity Debate and Informing the Agenda of the G20 Integrity of Information and Trust in the Digital Economy [Internet]. [Cited 2026 Apr 14], Sep 2024. Available from: https://www.g20.utoronto.ca/2024/P3_-_G20_DEWG_Brasil_2024_-_Mapping_the_Information_Integrity_Debate.pdf
17. Rahman KF, Jiow HJ, Lee B. Preventing Crimes of Online Scams Across Countries: A Comparative Study Between Bangladesh and Singapore. Social Science Review, Nov 3, 2025; 42(1):45-62. Doi: 10.3329/SSR.V42I1.85321
18. Dadà CB, Colautti L, Rosi A, Cavallini E, Antonietti A, Iannello P. Uncovering vulnerability to fraud and scams among adult victims in online and offline contexts: A systematic review. Comput Human Behav, Nov 1, 2025; 172:108734. Doi: 10.1016/J.CHB.2025.108734
19. Maina CW, Bashokoh MI, Koponicsné Györke D. A Bibliometric Analysis of Digital Financial Literacy and its Role in Reducing Online Financial Fraud in the European Union. International Journal of Financial Studies, Jan 8, 2026; 14(1):18. Doi: 10.3390/IJFS14010018
20. Jovanović M. Digital media literacy programs: Overview, good practices and potential problems [Internet]. [Cited 2026 Apr 14], 2024. Available from: https://www.debunk.org/digital-media-literacy-programs-overview-good-practices-and-potential-problems
21. Trusted News Initiative - Beyond Fake News [Internet]. [Cited 2026 Jun 22]. Available from: https://www.bbc.co.uk/beyondfakenews/trusted-news-initiative/