Economic Sciences
ISSN: 1505-4683
Vol. 26, No. 1 (2026)

The Role of Online Platforms in Preventing Cyber Fraud

Akriti Mehra[1], Dr. Yamini Atreya[2]

[1]Research Scholar, pursuing PhD.
[2]Assistant Professor, Manav Rachna University

Abstract

The rapid growth of digital technology has changed the way people communicate, shop, and interact through online platforms such as social media, e-commerce websites, digital payment apps, and online dating services. Along with these benefits, there has been a sharp rise in cyber fraud, where criminals use digital tools and psychological tricks to cheat users and steal money or personal information.

Cyber fraud includes activities like phishing, identity theft, online scams, fake shopping websites, and fraudulent investment schemes. These crimes are increasing because of weak security awareness, technological loopholes, and gaps in regulation.

Online platforms, which were earlier seen as neutral service providers, now play an important role in preventing cyber fraud. They use technologies like artificial intelligence, fraud detection systems, encryption, and user verification to identify and stop suspicious activities. They also create policies, monitor content, and cooperate with law enforcement agencies.

This research paper examines the role of online platforms in preventing cyber fraud, along with their responsibilities, challenges, and legal obligations. It also highlights the need for better technology, stronger regulations, and user awareness to reduce cyber fraud effectively.

Keywords

Cyber Fraud; Online Platforms; Digital Security; Fraud Prevention; Artificial Intelligence; Data Protection; Cybersecurity; Online Scams; User Awareness; Platform Responsibility.

1. Introduction

The internet has revolutionized global connectivity, allowing people to interact and transact without geographical limitations. Online platforms enable millions of users to shop, socialize, work, and communicate daily. With the increase in digital transactions and data sharing, cyber fraud has emerged as one of the most serious threats in the digital era.[3]

Cyber fraud refers to fraudulent activities carried out using computers, the internet, or digital communication technologies. These crimes include phishing, identity theft, online scams, financial fraud, romance scams, fake investment schemes, and social engineering attacks. According to global cybercrime reports, cyber fraud causes billions of dollars in losses annually and affects individuals, businesses, and governments.[4]

[3] Manuel Castells, *The Rise of the Network Society* (2nd edn, Wiley-Blackwell 2010). Also refer to Internet and Mobile Association of India (IAMAI) Reports on digital adoption in India.
[4] European Union Agency for Cybersecurity (ENISA), *Threat Landscape Report* (latest edn); FBI Internet Crime Complaint Center (IC3), *Annual Cybercrime Report*.

Online platforms act as intermediaries between users. Because fraud often occurs through these platforms, they have become key stakeholders in preventing cybercrime. Their role now extends beyond providing services to ensuring user safety and digital trust.[5]

2. Understanding Cyber Fraud in Online Platforms

Cyber fraud in online platforms refers to deceptive practices where criminals exploit digital systems and user behaviour to gain unauthorized access to personal data or financial resources. With the increasing dependence on online services for communication, shopping, banking, and social interaction, fraudsters have developed more sophisticated methods to target users in virtual environments. These crimes are not limited to technical hacking but often rely on manipulating human trust, urgency, and emotional vulnerability.[6]

One of the most common forms is phishing, where fake messages or websites are designed to resemble trusted institutions in order to trick individuals into revealing sensitive credentials such as passwords or banking details. Another widespread category is identity misuse, in which stolen personal information is used to impersonate victims and carry out illegal financial transactions. Online marketplaces have also become vulnerable, where fraudulent sellers create fake listings or websites to collect payments without delivering any goods or services.[7]

In addition, romance-based scams have increased significantly, especially on social networking and dating platforms, where offenders build emotional relationships to gain financial advantage over victims. Similarly, investment-related frauds, including cryptocurrency scams, lure users with promises of unusually high returns, often resulting in large financial losses. These different forms of fraud highlight how online platforms are frequently used as tools or mediums for executing cybercrime, making platform-level monitoring, regulation, and user protection essential for reducing such threats.[8]

3. Why Online Platforms Must Prevent Cyber Fraud

Online platforms occupy a central position in the digital ecosystem because they directly facilitate communication, transactions, and the exchange of information between users. This position gives them both the capability and responsibility to identify and reduce cyber fraud. Unlike individual users, platforms have access to large-scale data, behavioural patterns, and technical tools that allow them to detect suspicious activities more effectively. As a result, their role in preventing cyber fraud is not optional but increasingly essential for maintaining a safe digital environment.[9]

One major reason for this responsibility is platform accountability. Since these platforms profit from user engagement, advertising, and digital transactions, they are expected to maintain a secure ecosystem. If fraud occurs repeatedly on a platform, it reflects inadequate

[5] Information Technology Act, 2000 (India), Section 2(w) defining “intermediary”; also see Shreya Singhal v Union of India (2015) 5 SCC 1 (Supreme Court of India).
[6] Susan W Brenner, *Cybercrime and the Law* (2nd edn, Northeastern University Press 2018); also see United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (latest report).
[7] Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (latest edition) – sections on phishing and online fraud trends.
[8] Reserve Bank of India (RBI), *Report on Digital Payment Fraud Trends in India* (latest available report).
[9] Information Technology Act, 2000 (India), Section 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

security practices and weak monitoring systems, raising questions about the platform's due diligence.[10]

Another important factor is trust and reputation. Digital platforms rely heavily on user confidence to sustain their services. Once users begin to experience scams, identity theft, or financial loss, their trust declines rapidly, often leading to reduced usage and long-term reputational damage. Therefore, preventing cyber fraud is also a business necessity for maintaining credibility and user retention.[11]

Finally, legal and regulatory obligations have become increasingly significant. Many countries now impose strict duties on intermediaries to monitor harmful content, remove fraudulent activity, and cooperate with law enforcement agencies. These legal frameworks ensure that platforms cannot remain passive observers and must actively contribute to preventing online harm.[12]

4. Technological Measures Used by Online Platforms

Technology is the backbone of modern cyber fraud prevention systems, as online platforms rely heavily on automated tools to identify, monitor, and respond to suspicious activities in real time. With the increasing sophistication of cybercriminal methods, manual monitoring alone is insufficient, making advanced technological solutions essential for ensuring digital safety and trust.[13]

A major development in this area is the use of Artificial Intelligence (AI) and Machine Learning (ML). These systems analyse large volumes of user data to detect unusual behaviour such as abnormal login attempts, rapid transaction patterns, creation of fake accounts, or suspicious messaging activity. By using behavioural analysis, fraud detection algorithms, and risk scoring models, AI systems help platforms predict and prevent fraud before it causes harm.[14]

Another widely used security feature is Two-Factor Authentication (2FA), which strengthens account protection by requiring users to verify their identity through an additional step such as OTPs, biometrics, or security keys. This reduces the risk of unauthorized access even if login credentials are compromised.[15]

Platforms also depend on encryption and data protection techniques to secure user information. End-to-end encryption ensures that data transmitted between users remains unreadable to unauthorized parties, thereby reducing the risk of interception or leakage during communication.

In addition, automated fraud detection systems continuously monitor platform activity in real time to identify suspicious messages, links, or financial transactions. These systems are

[10] Shreya Singhal v Union of India (2015) 5 SCC 1 (Supreme Court of India) – on intermediary liability and safe harbour principles.
[11] European Commission, *Digital Services Act (DSA)* (Regulation (EU) 2022/2065) – obligations of online platforms.
[12] OECD, *The Role of Online Platforms in the Digital Economy* (latest report) – platform responsibility and trust framework.
[13] OECD, *Digital Security Risk Management for Economic and Social Prosperity* (latest report) – role of AI and automation in fraud prevention.
[14] ENISA, *Artificial Intelligence Cybersecurity Challenges Report* (latest edition).
[15] Reserve Bank of India (RBI), *Guidelines on Digital Payment Security Controls* (latest circulars) – 2FA and authentication standards.

designed to immediately flag or block potentially harmful activities, reducing the response time between detection and action.[16]

Finally, identity verification systems, commonly known as KYC (Know Your Customer) procedures, are used to confirm the authenticity of users. By verifying identity documents and linking accounts to real individuals, platforms can significantly reduce the creation of fake profiles and fraudulent accounts.[17]

5. Policy and Governance Measures

Along with technological tools, online platforms also rely on structured policy and governance frameworks to prevent and control cyber fraud. These internal rules and regulatory mechanisms help platforms manage user behaviour, ensure compliance with legal standards, and create a safer digital environment. Since cyber fraud often involves human behaviour and social engineering, policies play a crucial role in complementing technical safeguards.[18]

A key component of this framework is community guidelines, which clearly define acceptable and prohibited activities on the platform. These rules typically ban scams, impersonation, misleading content, and fraudulent advertisements. By setting behavioural standards, platforms aim to reduce opportunities for fraud at the source itself.[19]

Another important mechanism is the reporting and complaint system, which allows users to flag suspicious accounts, messages, or activities. This user-driven approach helps platforms identify potential fraud quickly and respond before it spreads widely. It also encourages collective responsibility in maintaining platform safety.[20]

Content moderation is also widely used, where platforms actively review, detect, and remove harmful content such as fake profiles, phishing links, and scam-based advertisements. This process may involve both automated systems and human moderators to ensure accuracy and effectiveness.[21]

Finally, collaboration with law enforcement agencies strengthens fraud prevention efforts at a broader level. Platforms often share relevant data, logs, and user information (subject to legal procedures) with investigating authorities to support cybercrime detection and prosecution. This cooperation ensures that cyber fraud is not only removed from platforms but also legally addressed.[22]

6. Legal Framework and Platform Liability

In the digital age, governments across the world have developed and strengthened legal frameworks to ensure that online platforms act responsibly in preventing cyber fraud. These

[16] Financial Action Task Force (FATF), *Guidance on Digital Identity* (KYC frameworks and fraud prevention).
[17] International Organization for Standardization (ISO/IEC 27001:2022) – information security and encryption standards.
[18] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India) – duties of intermediaries including grievance redressal and content removal.
[19] Information Technology Act, 2000, Section 79 – safe harbour and due diligence requirements for intermediaries.
[20] European Commission, *Digital Services Act (DSA) 2022/2065* – content moderation and platform accountability framework.
[21] OECD, *Online Platforms Governance and Trust Report* (latest publication) – role of reporting systems and moderation.
[22] United Nations Office on Drugs and Crime (UNODC), *Cybercrime and Platform Cooperation Report* (latest edition).

laws aim to balance innovation and free expression with the need for user safety and accountability. As platforms play a central role in facilitating online interactions, they are increasingly being treated as regulated intermediaries rather than neutral service providers.[23]

A key concept in this area is intermediary liability, which determines the legal responsibility of platforms for third-party content. In many jurisdictions, platforms are granted "safe harbour" protection, meaning they are not automatically liable for user-generated content. However, this protection is conditional. If a platform fails to take prompt action after receiving actual knowledge or legal notice of illegal or fraudulent content, it may lose its immunity and become legally responsible for the harm caused.[24]

Another important aspect is data protection laws, which impose obligations on platforms to safeguard personal information of users. These laws require companies to adopt strict security measures, ensure lawful processing of data, and report data breaches to authorities and affected users. Since cyber fraud often involves misuse of personal data, strong data protection frameworks play a critical role in prevention.[25]

In addition, cybersecurity regulations require platforms and digital service providers to implement adequate technical and organizational safeguards to protect their systems. These include risk assessment procedures, incident response mechanisms, and continuous monitoring systems. Such regulations ensure that platforms do not remain passive actors but actively invest in maintaining secure digital infrastructure.[26]

7. Challenges Faced by Online Platforms

Despite significant advancements in technology and regulatory frameworks, online platforms continue to face several structural and operational challenges in effectively preventing cyber fraud. These challenges arise due to the global, dynamic, and constantly evolving nature of the digital ecosystem, which makes complete control and monitoring extremely difficult.[27]

One of the major issues is the scale of the internet, where billions of users generate vast amounts of data every second. Monitoring such a large volume of activity in real time is highly complex, even with advanced artificial intelligence systems. This makes it difficult for platforms to identify every fraudulent activity accurately and promptly.

Another significant challenge is the constant evolution of cybercriminal techniques. Fraudsters frequently adapt their methods by using new technologies, fake identities, encrypted communication channels, and social engineering tactics. This continuous innovation creates a gap between security systems and criminal strategies, making prevention an ongoing struggle.[28]

---

[23] Information Technology Act, 2000 (India), Section 79 – intermediary safe harbour and due diligence requirements.
[24] Shreya Singhal v Union of India (2015) 5 SCC 1 – interpretation of intermediary liability and "actual knowledge" principle.
[25] European Union, *Digital Services Act (Regulation (EU) 2022/2065)* – platform accountability and risk management duties.
[26] European Union, *General Data Protection Regulation (GDPR) 2016/679* – data protection and breach notification obligations.
[27] Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (latest edition) – challenges in cross-border cybercrime investigation.
[28] United Nations Office on Drugs and Crime (UNODC), *Cybercrime Global Study* – scale and complexity of digital fraud.

A further difficulty lies in the privacy versus surveillance debate. While platforms are expected to detect and prevent fraud, excessive monitoring of user activity may raise concerns regarding privacy rights and data protection. Striking a balance between user privacy and effective surveillance remains a critical legal and ethical issue.[29]

Lastly, cross-border jurisdictional problems complicate enforcement efforts. Cyber fraud often involves actors operating from different countries, each with different legal systems and enforcement mechanisms. This makes investigation, evidence collection, and prosecution highly challenging, as cooperation between international authorities is not always efficient or timely.

8. Role of User Awareness

User awareness plays a fundamental role in preventing cyber fraud because even the most advanced technological systems cannot fully eliminate risks if users themselves are not cautious. In many cases, cyber fraud succeeds not due to system failure but because users unknowingly share sensitive information, click on malicious links, or trust unverified sources. Therefore, users act as the first and most important line of defence in maintaining online security.[30]

To strengthen this defence, online platforms actively promote security alerts and warnings, which notify users about suspicious login attempts, unusual account activity, or potentially harmful links. These real-time alerts help users take immediate action and avoid falling victim to fraud.[31]

Platforms also conduct awareness campaigns to educate users about common cyber fraud techniques such as phishing, fake profiles, and online scams. These campaigns aim to build long-term behavioural awareness and encourage safe online practices.

In addition, fraud prevention tips are regularly shared through platform interfaces, emails, and notifications. These tips guide users on how to create strong passwords, identify suspicious activity, and protect their personal data.

Furthermore, platforms provide educational resources such as help centres, tutorials, and safety guides that improve digital literacy. Higher levels of digital literacy empower users to recognize threats early and respond appropriately, thereby significantly reducing the success rate of cyber fraud attempts.[32]

9. Case Studies of Platform Initiatives

Online platforms across different sectors have adopted several proactive measures to reduce the risk of cyber fraud. These initiatives demonstrate how platform governance, when combined with technology and policy enforcement, can significantly enhance user safety and reduce fraudulent activities.

In the case of social media platforms, advanced artificial intelligence tools are widely used to detect and remove fake accounts, bot networks, and scam-related advertisements. These platforms continuously monitor user behaviour patterns and content uploads to identify

[29] OECD, *Privacy and Data Protection in the Digital Age* (latest report) – privacy vs surveillance concerns.
[30] OECD, *Digital Literacy and Online Safety Report* (latest edition) – role of user awareness in cybercrime prevention.
[31] European Union Agency for Cybersecurity (ENISA), *Cyber Hygiene Guidelines* (latest report).
[32] Federal Trade Commission (FTC), *Consumer Education on Online Fraud Prevention* (annual guidance materials).

suspicious activity. Once detected, fraudulent accounts are either restricted or permanently removed to prevent further misuse.[33]

E-commerce platforms have also introduced structured protection mechanisms to safeguard buyers and sellers. These include seller verification systems, secure payment gateways, and buyer protection policies that ensure refunds in cases of fraud or non-delivery of products. Such measures help in building trust and reducing financial risks associated with online shopping.

Similarly, digital payment platforms implement real-time transaction monitoring systems that analyse payment behaviour and flag unusual or high-risk transactions. If any suspicious activity is detected, the system may automatically block or delay the transaction for verification. These preventive controls play a crucial role in reducing financial fraud and unauthorized transfers.

Collectively, these initiatives highlight that proactive governance by online platforms, supported by technological innovation and user protection policies, can significantly reduce the incidence and impact of cyber fraud.[34]

10. Conclusion

In conclusion, online platforms have become an essential part of everyday life, influencing how people communicate, shop, work, and make financial transactions. Because of this deep integration into society, these platforms now play a very important role in dealing with the growing problem of cyber fraud. Earlier, they were mainly seen as intermediaries that only provided services, but now their responsibility has expanded to actively protecting users and maintaining safety within the digital environment.

This shift has been possible due to the use of advanced technologies such as artificial intelligence, machine learning, and automated security systems, along with strong internal policies and cooperation with government authorities. These combined efforts help in identifying, preventing, and responding to fraudulent activities more effectively.

However, cyber fraud cannot be completely eliminated by platforms alone. It requires a joint effort where platforms, governments, and users all share responsibility. Users must remain aware and cautious, governments must strengthen laws and enforcement, and platforms must continuously improve their security systems.

As digital technology continues to develop, cyber threats will also become more advanced. Therefore, online platforms must regularly update and strengthen their security measures to stay ahead of fraudsters. Ultimately, the future of the digital economy depends on creating a safe and trustworthy online environment where users can participate confidently without fear of fraud or exploitation.

11. Recommendations

To effectively strengthen the role of online platforms in preventing cyber fraud, several practical and policy-based measures are required. These recommendations focus on improving regulation, technology, user protection, and accountability so that digital ecosystems become more secure and reliable.

[33] Reserve Bank of India (RBI), *Digital Payment Security and Fraud Prevention Guidelines* (latest circulars).
[34] European Commission, *Digital Services Act (Regulation (EU) 2022/2065)* – obligations of online platforms for risk mitigation.

Firstly, there is a need for stronger global regulatory cooperation, because cyber fraud is not limited to one country. Criminals often operate across borders, making it necessary for different nations to share information, coordinate investigations, and develop common standards to combat cybercrime effectively.

Secondly, mandatory cybersecurity standards should be enforced for all online platforms. These standards would ensure that companies implement minimum security requirements such as encryption, secure authentication systems, and regular security audits to protect users from fraud.

Thirdly, platforms must invest in improved AI-based fraud detection systems. Advanced artificial intelligence can help identify suspicious behaviour, detect fake accounts, and prevent fraudulent transactions in real time, making fraud prevention more proactive than reactive.

Fourthly, enhanced user education programs are essential. Users should be continuously informed about cyber threats, safe online practices, and fraud prevention techniques so they can protect themselves more effectively.

Fifthly, transparent reporting of cyber incidents should be encouraged. Platforms should regularly disclose fraud statistics and security breaches, which will improve accountability and help regulators understand emerging risks.

Sixthly, faster complaint redressal mechanisms are necessary so that victims of cyber fraud can quickly report issues and receive timely support or compensation. Delayed responses often increase financial and emotional damage.

Lastly, stronger penalties for negligent platforms should be introduced. If a platform fails to implement adequate security measures or ignores known risks, it should face legal consequences. This will ensure greater responsibility and encourage better compliance with cybersecurity norms.

References

Books

- Brenner, Susan W., *Cybercrime and the Law*, 2nd edn (Northeastern University Press, 2018).
- Castells, Manuel, *The Rise of the Network Society*, 2nd edn (Wiley-Blackwell, 2010).
- Yar, Majid, *Cybercrime and Society* (Sage Publications, 2013).

Reports / International Sources

- European Union Agency for Cybersecurity (ENISA), *Threat Landscape Report* (latest edition).
- Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (latest edition).
- United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (latest report).
- Organisation for Economic Co-operation and Development (OECD), *Digital Security Risk Management and Cybercrime Reports* (latest editions).
- World Bank, *Digital Financial Services and Cyber Risk Reports* (latest edition).

- Federal Trade Commission (FTC), *Consumer Fraud Reports* (annual reports).

Indian Legislations / Legal Sources

- Information Technology Act, 2000 (India).
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- Digital Personal Data Protection Act, 2023 (India).

Case Laws

- *Shreya Singhal v Union of India*, (2015) 5 SCC 1.
- *Avnish Bajaj v State (NCT of Delhi)*, 2008 CriLJ 446.
- *State of Tamil Nadu v Suhas Katti*, 2004 (Madras High Court).

Institutional / Regulatory Reports

- Reserve Bank of India (RBI), *Report on Digital Payment Security and Fraud Prevention* (latest circulars).
- International Organization for Standardization (ISO/IEC 27001:2022), Information Security Management Standards.
- Financial Action Task Force (FATF), *Guidance on Digital Identity and AML/CFT*.