INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

SCAMMED BY AI: THE NEW AGE OF ONLINE CONSUMER FRAUD

AUTHORED BY - MR. DARSHAN G[1]

ABSTRACT

Artificial Intelligence has transformed modern society by making digital services faster, smarter, and more personalized. From online shopping and banking to customer support and entertainment, Artificial Intelligence has become deeply integrated into everyday consumer experiences. However, the rapid growth of Artificial Intelligence has also created new opportunities for cybercriminals. Fraudsters are now using Artificial Intelligence tools to create sophisticated scams involving deepfake videos, cloned voices, fake advertisements, automated phishing attacks, and impersonation frauds. Unlike traditional online scams, Artificial Intelligence-powered frauds are highly convincing, emotionally manipulative, and difficult to detect. Consumers are increasingly being deceived into sharing personal information, transferring money, or trusting fake digital identities.

India, as one of the world's largest digital economies, has witnessed a significant increase in Artificial Intelligence-enabled scams in recent years. The rise of digital payments, e-commerce platforms, and social media usage has made consumers more vulnerable to cyber fraud. Existing laws such as the Information Technology Act, 2000, the Consumer Protection Act, 2019, and the Digital Personal Data Protection Act, 2023 provide some protection, but the fast-changing nature of Artificial Intelligence creates major legal and regulatory challenges.

This article examines the growing problem of Artificial Intelligence-based consumer fraud, the different forms of scams used by cybercriminals, the impact on consumers, the legal framework in India, international approaches, ethical concerns, and the role of technology companies in consumer protection. The article also highlights the importance of digital literacy, stronger regulations, and responsible Artificial Intelligence governance in ensuring safer digital environments.

Keywords: Artificial Intelligence, Consumer Fraud, Cybercrime, Deepfake, Online Scams, Consumer Protection, Digital Fraud, Data Privacy, India, AI Governance.

[1] Author; Mysuru, Karnataka, INDIA

ISSN: 2582-6433

Introduction

The digital revolution has completely changed the way consumers interact with businesses and services. Today, people can purchase products, transfer money, attend classes, book travel tickets, and communicate globally within seconds through online platforms. Artificial Intelligence has become one of the driving forces behind this transformation. Artificial Intelligence systems are now used in recommendation algorithms, virtual assistants, online advertisements, customer service operations, fraud detection systems, and data analysis.

Although Artificial Intelligence has introduced convenience and innovation, it has also created serious risks for consumers. Criminals have started using Artificial Intelligence technologies to design highly advanced frauds that are more dangerous than traditional cybercrimes. These scams are difficult to identify because they imitate real human behaviour, voices, videos, and communication patterns. Consumers who once trusted digital content now face a world where seeing and hearing can no longer be considered reliable proof.

The misuse of Artificial Intelligence has led to a dramatic increase in online consumer fraud across the world.[2] Cybercriminals now use machine learning tools, deepfake software, automated chatbots, and data analytics to deceive consumers. Deepfake videos can show celebrities promoting fake investment schemes, while voice cloning software can imitate family members asking for urgent financial help.[3] Artificial Intelligence-generated phishing messages are more personalized and convincing than earlier scams.

India has become one of the major targets of Artificial Intelligence-enabled consumer fraud because of rapid digitalization, increasing internet penetration, and widespread use of online payment systems. Millions of consumers rely on digital transactions every day, creating opportunities for fraudsters to exploit technological vulnerabilities and human emotions.

The issue is not limited to financial loss alone. Artificial Intelligence scams also create psychological trauma, reputational damage, identity theft, and loss of trust in digital systems. The growing dependence on technology means that consumer protection mechanisms must evolve quickly to address these modern challenges.

This article discusses the rise of Artificial Intelligence-driven consumer fraud, examines the major types of scams, analyses the legal framework in India, explores international responses, and suggests preventive measures for protecting consumers in the digital age.

[2] Deepfakes and Financial Cybercrime: India's Multi-Layered Response, Observer Research Foundation (Jan. 15, 2026).
[3] Online Fraud and Scams in India, Safer Internet Lab Research Report (2025).

ISSN: 2582-6433

Understanding Artificial Intelligence and Consumer Fraud

Artificial Intelligence refers to computer systems capable of performing tasks that normally require human intelligence. These tasks include learning, decision-making, pattern recognition, speech generation, image creation, and data analysis. Artificial Intelligence systems can process massive amounts of information and generate outputs that appear natural and human-like.

Consumer fraud refers to deceptive practices intended to cheat or exploit consumers for financial or personal gain. Traditionally, online scams involved fake lottery messages, suspicious emails, and misleading advertisements. However, Artificial Intelligence has transformed fraud into a highly sophisticated activity.

Artificial Intelligence-powered fraud differs from traditional scams because it relies heavily on automation, personalization, and predictive behaviour analysis. Fraudsters collect information from social media accounts, online purchases, digital payment records, and public databases. This information is then used to create targeted attacks that appear trustworthy.

For example, a scammer may use Artificial Intelligence to analyse a consumer's online activity and send a fake message related to a recent online purchase or banking transaction. Since the message appears relevant and personalized, the consumer is more likely to trust it.

Another major concern is generative Artificial Intelligence, which can create realistic text, images, videos, and audio recordings. These technologies have made it easier for criminals to impersonate real individuals. Consumers may receive phone calls from cloned voices, interact with Artificial Intelligence-generated chatbots pretending to be customer service representatives, or watch fake videos of public figures promoting fraudulent schemes.

The increasing accessibility of Artificial Intelligence tools has made these scams more common. Earlier, creating realistic fake videos or sophisticated cyberattacks required technical expertise and expensive software. Today, many Artificial Intelligence tools are publicly available, making it easier for criminals to misuse them.

As a result, consumer fraud has entered a new era where technology is used not only to deceive people but also to manipulate emotions, trust, and behaviour on a massive scale.

Evolution of Online Consumer Fraud

Consumer fraud has existed for centuries, but technological development has continuously changed its methods. Earlier frauds relied on face-to-face deception, forged documents, or fraudulent telephone calls. With the growth of the internet, cybercrime expanded rapidly

ISSN: 2582-6433

through spam emails, fake websites, and online scams.

In the early stages of online fraud, scams were often poorly designed and easy to recognize. Consumers could identify suspicious emails because of grammatical errors, unrealistic promises, or unfamiliar website designs. However, the development of Artificial Intelligence has dramatically improved the quality and effectiveness of cyber scams.

Machine learning systems can now study human communication patterns and generate convincing messages that imitate genuine conversations. Artificial Intelligence-powered systems can produce realistic customer service interactions, persuasive advertisements, and emotionally manipulative content.

Deepfake technology represents one of the most alarming developments in this evolution. Deepfakes use machine learning algorithms to manipulate facial expressions, lip movements, and voices in videos. These manipulated videos can appear extremely realistic, making it difficult for ordinary consumers to detect fraud.

Similarly, voice cloning technology has evolved rapidly. Artificial Intelligence systems can now reproduce a person's voice using only a short audio sample collected from social media videos, voice notes, or interviews.

Fraudsters also increasingly rely on automation. Instead of targeting a small number of victims manually, Artificial Intelligence allows criminals to launch large-scale attacks against thousands of consumers simultaneously.

The evolution of Artificial Intelligence fraud demonstrates how cybercrime adapts to technological progress. Unfortunately, legal systems and consumer awareness often struggle to keep pace with these changes.

Major Types of Artificial Intelligence Consumer Scams

1. Deepfake Video Scams

Deepfake scams involve Artificial Intelligence-generated videos that imitate real individuals. Fraudsters create fake videos of celebrities, politicians, business leaders, and social media influencers promoting fraudulent products or investment schemes. Many consumers trust these videos because they appear authentic. Fraudsters often use deepfakes to advertise fake cryptocurrency investments, miracle health products, or fraudulent financial schemes.

Deepfake scams are dangerous because visual content strongly influences human perception. Consumers naturally believe videos and may not realize that the content has been digitally manipulated. India has witnessed several incidents involving deepfake videos of public

ISSN: 2582-6433

figures.[4] Courts have also expressed concern regarding the misuse of deepfake technology and its impact on privacy and public trust.

2. Voice Cloning Fraud

Voice cloning technology allows Artificial Intelligence systems to imitate human voices with remarkable accuracy. Criminals collect voice samples from social media videos, interviews, or phone recordings. Victims often receive emergency calls from someone who sounds exactly like a relative or friend requesting urgent financial assistance.[5] The emotional panic created during such calls prevents rational thinking.

In many cases, victims transfer money immediately because they believe their loved ones are in danger. Elderly individuals are particularly vulnerable to such scams. Voice cloning fraud demonstrates how Artificial Intelligence can manipulate human emotions and exploit personal relationships for financial gain.

3. Artificial Intelligence-Powered Phishing

Phishing attacks traditionally involved fake emails requesting passwords or banking details. Artificial Intelligence has made phishing attacks more sophisticated and personalized. Artificial Intelligence systems analyse consumer behaviour, shopping history, and communication patterns to create highly convincing messages. Fraudsters may send fake delivery notifications, banking alerts, tax refund messages, or shopping offers.

Unlike older phishing emails filled with grammatical mistakes, Artificial Intelligence-generated messages appear professional and realistic. Consumers may unknowingly click malicious links or reveal sensitive information.

4. Fake Customer Support Scams

Artificial Intelligence chatbots and automated voice systems are increasingly used to imitate customer support services. Consumers searching online for technical assistance may contact fake customer service numbers operated by scammers. These fraudsters convince consumers to install remote access applications or disclose banking information under the pretext of solving technical problems.

The use of Artificial Intelligence chatbots makes these interactions appear natural and

[4] Truly Alarming: Bombay High Court Orders Removal of Deepfake Content Infringing Akshay Kumar's Personality Rights, Times of India (2025).
[5] AI Voice Scam in India: Spot, Stop & Recover, RTI Wiki (2026).

ISSN: 2582-6433

professional, increasing consumer trust.

5. Investment and Cryptocurrency Scams

Artificial Intelligence-generated advertisements and deepfake celebrity endorsements are commonly used to promote fake investment opportunities. Consumers are promised high returns with minimal risk.[6] Fraudsters often exploit fear of missing out by creating urgency and fake success stories.

Cryptocurrency scams have become particularly common because digital currencies operate in decentralized environments with limited regulation.

6. Digital Arrest and Government Impersonation Scams

India has witnessed a rise in so-called digital arrest scams where criminals impersonate police officers, tax officials, or investigative agencies.

Victims receive threatening video calls and fake legal notices claiming involvement in illegal activities. Fraudsters use Artificial Intelligence-generated identities, forged documents, and manipulated video interactions to appear legitimate. Consumers are psychologically pressured into transferring money to avoid arrest or legal action.

Psychological Manipulation Behind Artificial Intelligence Fraud

One of the most disturbing aspects of Artificial Intelligence scams is the psychological manipulation involved. Fraudsters no longer rely only on technical deception. They exploit human emotions such as fear, urgency, trust, curiosity, and greed.

Artificial Intelligence allows scammers to personalize attacks based on individual behaviour and preferences. For example, scammers may know a consumer's recent online purchases, travel plans, or family relationships through social media data. Fear is commonly used in digital arrest scams and fake banking alerts. Victims panic when they believe they are facing legal trouble or financial loss.

Emotional attachment is exploited through voice cloning scams. Hearing a loved one's voice creates immediate emotional trust. Urgency is another powerful technique. Fraudsters pressure consumers to act quickly before verifying information.

Artificial Intelligence increases the effectiveness of psychological manipulation because it can

[6] Shah Rukh Khan, Alia Bhatt, and Elon Musk Top Deepfake Scam List in India, McAfee Press Release (Nov. 24, 2025).

ISSN: 2582-6433

imitate human communication styles and emotional responses. This raises serious ethical concerns about how technology can be weaponized against human psychology.

Impact of Artificial Intelligence Fraud on Consumers

Financial Loss

Financial damage is the most immediate consequence of Artificial Intelligence fraud. Consumers lose money through fake investments, online shopping scams, unauthorized bank transfers, and phishing attacks. Many victims lose their life savings because the scams appear highly convincing.

Emotional and Psychological Trauma

Victims often experience stress, anxiety, embarrassment, and emotional trauma after realizing they have been deceived.[7] Consumers may also develop distrust toward digital platforms and online communication.

Voice cloning scams are particularly traumatic because victims feel emotionally manipulated by someone who sounded like a loved one.

Identity Theft

Artificial Intelligence tools make identity theft easier than ever before. Criminals can create fake digital identities using stolen images, videos, and voice recordings. Victims may face fraudulent loans, fake social media profiles, reputational damage, and financial complications.

Privacy Violations

Artificial Intelligence scams heavily depend on personal data collection. Fraudsters gather information from social media accounts, online applications, and public databases. Deepfake misuse also violates personal dignity and privacy because individuals' images and voices are manipulated without consent.

Social Impact

Artificial Intelligence fraud affects society beyond individual victims. Public trust in digital systems decreases when consumers fear manipulation.

Businesses also suffer reputational damage because consumers become hesitant to engage in

[7] Intergenerational Support for Deepfake Scams Targeting Older Adults, arXiv (2025).

ISSN: 2582-6433

online transactions. The spread of misinformation through Artificial Intelligence-generated content can also influence public opinion and social stability.

Artificial Intelligence Fraud in India

India has become one of the fastest-growing digital economies in the world. The expansion of smartphone usage, digital payments, e-commerce platforms, and social media networks has created enormous opportunities for economic growth. However, rapid digitalization has also increased cybercrime risks. India's large online population provides fraudsters with access to millions of potential victims.

The widespread use of the Unified Payments Interface system has revolutionized digital transactions but also increased online payment fraud.[8]

Consumers in India are increasingly targeted through fake investment schemes, phishing attacks, online shopping scams, and impersonation fraud. Social media platforms have become major sources of consumer manipulation. Fraudsters use Artificial Intelligence-generated advertisements, fake celebrity endorsements, and manipulated videos to gain public trust.[9]

Many consumers are unaware of how deepfakes and Artificial Intelligence-generated content operate. This lack of digital literacy increases vulnerability. The rise of digital arrest scams has also exposed weaknesses in public awareness and law enforcement mechanisms. Several victims have reportedly transferred large sums of money after being threatened by fake officials through video calls.

Rural consumers and elderly individuals are especially vulnerable because they may have limited awareness regarding cybercrime prevention. India therefore faces the dual challenge of encouraging digital growth while ensuring strong consumer protection.

Legal Framework in India

Information Technology Act, 2000

The Information Technology Act, 2000 is the primary cyber law legislation in India.[10] It addresses offenses such as hacking, identity theft, cheating by impersonation, and unauthorized access to computer systems. Sections dealing with identity theft and cheating by personation may apply to Artificial Intelligence fraud cases involving fake identities, phishing attacks, and

[8] Online Fraud and Scams in India, Safer Internet Lab Research Report (2025).
[9] AI-Driven Scams Target Indian Shoppers as 96% Go Online for Prime Day Deals, Digital Terminal (July 9, 2025).
[10] Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

ISSN: 2582-6433

digital impersonation.

However, the Act was enacted long before the rise of deepfake technology and modern Artificial Intelligence systems. Therefore, certain legal gaps remain.

Consumer Protection Act, 2019

The Consumer Protection Act, 2019 protects consumers from unfair trade practices and misleading advertisements.[11] Artificial Intelligence-generated fake advertisements and deceptive endorsements may fall under misleading advertising practices.

The Act also recognizes e-commerce transactions and establishes consumer dispute redressal mechanisms. However, enforcement becomes difficult when fraudsters operate anonymously or outside India.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 aims to regulate personal data processing and protect consumer privacy.[12]

Since Artificial Intelligence scams heavily depend on personal data collection, stronger data protection laws are essential for preventing misuse. Consumers now have greater rights regarding consent, data access, and data correction.

Bhartiya Nyaya Sanhita and Criminal Laws

Traditional criminal laws relating to cheating, forgery, criminal intimidation, extortion, and fraud can also apply to Artificial Intelligence scams. Digital arrest scams, fake legal notices, and impersonation fraud may attract criminal liability under these laws.

International Approaches Toward Artificial Intelligence Fraud

Countries across the world are struggling to regulate Artificial Intelligence misuse.

The European Union has introduced the Artificial Intelligence Act, which focuses on risk-based regulation of Artificial Intelligence systems.[13] High-risk Artificial Intelligence applications face stricter compliance requirements. The European Union also emphasizes transparency obligations, especially regarding deepfakes and manipulated media.

The United States has focused on sector-specific regulations and enforcement actions through

[11] Consumer Protection Act, No. 35 of 2019, INDIA CODE (2019).
[12] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
[13] European Union Artificial Intelligence Act, 2024 O.J. (L).

ISSN: 2582-6433

agencies such as the Federal Trade Commission.

China has introduced regulations requiring labels for Artificial Intelligence-generated content and stricter controls on deepfake technology. Several countries are also debating mandatory watermarking systems for Artificial Intelligence-generated media.

International cooperation is essential because cybercrime frequently operates across borders.

Challenges in Regulating Artificial Intelligence Fraud

Rapid Technological Development

Artificial Intelligence evolves faster than legal systems. By the time governments introduce regulations, scammers often develop newer technologies.

Difficulty in Detecting Deepfakes

Deepfake content has become highly realistic.[14] Even experts sometimes struggle to identify manipulated videos and audio recordings. Ordinary consumers are even more vulnerable.

Cross-Border Cybercrime

Many scams originate from international criminal networks.[15] Jurisdictional issues complicate investigation and prosecution.

Different countries also have varying cybercrime laws and enforcement mechanisms.

Lack of Consumer Awareness

Digital illiteracy remains a major challenge.

Many consumers are unaware of Artificial Intelligence technologies and therefore cannot recognize manipulated content.

Platform Accountability Issues

Social media platforms often struggle to remove harmful content quickly.

Artificial Intelligence-generated scams spread rapidly before authorities can intervene.

Role of Technology Companies

Technology companies have an important responsibility in protecting consumers from

[14] Detection of AI Deepfake and Fraud in Online Payments Using GAN-Based Models, arXiv (2025).
[15] The Clever New Scam Your Bank Can't Stop, Business Insider (2025).

ISSN: 2582-6433

Artificial Intelligence fraud.

Platforms should invest in stronger fraud detection systems, deepfake identification technologies, and verification mechanisms. Artificial Intelligence itself can also be used for cybersecurity purposes.[16] Machine learning systems can identify suspicious patterns, detect fake accounts, and flag manipulated media.

Companies should also improve transparency regarding Artificial Intelligence-generated content. Consumers should be informed when advertisements, videos, or interactions involve Artificial Intelligence systems.[17]

Social media platforms must respond quickly to reports of fraud and remove harmful content before it spreads widely. Technology companies should also cooperate with governments and law enforcement agencies in cybercrime investigations.

Ethical Concerns Associated with Artificial Intelligence Fraud

Artificial Intelligence fraud raises serious ethical questions regarding privacy, consent, trust, and accountability.[18]

Deepfake technology can damage reputations and spread misinformation. Voice cloning technology can manipulate emotional relationships. Artificial Intelligence systems are often trained using large amounts of personal data collected from users.

This creates concerns regarding surveillance and misuse of consumer information.[19]

Another ethical issue involves accountability. When Artificial Intelligence systems are misused, determining responsibility becomes difficult. Developers, platforms, users, and governments all share some level of responsibility. Ethical Artificial Intelligence development should prioritize transparency, fairness, and consumer safety.

Preventive Measures and Consumer Awareness

Consumer awareness is one of the most effective defences against Artificial Intelligence fraud. Consumers should verify information before transferring money or sharing personal data. People should avoid trusting urgent messages or calls without independent verification.

Important preventive measures include:

1. Using strong passwords and multi-factor authentication.

[16] Detection of AI Deepfake and Fraud in Online Payments Using GAN-Based Models, arXiv (2025).
[17] The Clever New Scam Your Bank Can't Stop, Business Insider (2025).
[18] Beyond Cash: How Deepfakes Are Violating Privacy, Robbing People of Dignity, Economic Times (2025).
[19] Deep Fake Website Explained: Deepfake Scams and Risks, Bajaj Finserv (2026).

ISSN: 2582-6433

2. Verifying customer support numbers from official websites.
3. Avoiding suspicious links and attachments.
4. Limiting personal information shared on social media.
5. Updating software regularly.
6. Reporting suspicious activities immediately.
7. Educating family members, especially elderly individuals.

Families may also use secret verification codes during emergencies to prevent voice cloning scams.[20]

Governments and educational institutions should conduct public awareness campaigns regarding deepfakes, phishing attacks, and digital fraud prevention. Digital literacy must become an essential part of modern education.[21]

Recommendations for Strengthening Consumer Protection

India requires stronger legal and institutional mechanisms to combat Artificial Intelligence fraud. First, dedicated legislation addressing deepfakes and Artificial Intelligence misuse should be introduced.

Second, stricter obligations should be imposed on social media platforms and digital companies to detect and remove fraudulent content. Third, faster grievance redressal mechanisms should be established for cyber fraud victims.

Fourth, international cooperation should be strengthened for investigation of cross-border cybercrime. Fifth, digital literacy programs should be expanded across urban and rural areas.

Sixth, Artificial Intelligence developers should implement ethical safeguards and watermarking systems for generated content. Finally, law enforcement agencies require specialized training in Artificial Intelligence-related investigations.

Conclusion

Artificial Intelligence has transformed the modern digital world by improving efficiency, convenience, and innovation. However, the same technology has also created new opportunities for cybercriminals to exploit consumers. Artificial Intelligence-powered scams involving deepfakes, voice cloning, phishing attacks, fake customer support services, and impersonation fraud have become increasingly common across the world.

[20] AI Voice Scam in India: Spot, Stop & Recover, RTI Wiki (2026).
[21] New Cybersecurity Survey 2025: AI, Scam Fears and Fraud, Mastercard (Oct. 6, 2025).

ISSN: 2582-6433

These scams are more dangerous than traditional frauds because they imitate real human behaviour and manipulate emotions with remarkable accuracy.

India faces significant challenges due to rapid digitalization and growing dependence on online transactions. Existing laws provide some protection, but they are not fully equipped to address the complexities of Artificial Intelligence misuse. The fight against Artificial Intelligence fraud requires a combination of stronger laws, ethical Artificial Intelligence governance, technological safeguards, corporate responsibility, and consumer awareness.

Technology companies must improve fraud detection systems and ensure transparency regarding Artificial Intelligence-generated content.

Governments should introduce modern legal frameworks capable of addressing deepfakes, identity manipulation, and cross-border cybercrime. Consumers must also become more cautious and digitally aware. In the age of Artificial Intelligence, critical thinking and verification are essential for online safety.

Artificial Intelligence itself is not the enemy. The real challenge lies in preventing its misuse. If society can successfully balance innovation with responsibility, Artificial Intelligence can remain a powerful tool for progress rather than becoming a weapon of deception.