Quest Journals
Journal of Research in Humanities and Social Science
Volume 14 ~ Issue 7 (July 2026) pp: 154-161
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

Dark Reality of Rising Cybercrimes and Online Scams: Challenges and Preventive Measures in the Digital Age

Dr.S.Krishnan[1] and Mr. Mayank Sharma[2]

Abstract
The twenty-first century has witnessed an unprecedented digital revolution. The internet has transformed communication, commerce, education, governance, healthcare, and entertainment. Smartphones, cloud computing, Artificial Intelligence, and digital payment systems have made life more convenient and interconnected than ever before. However, the rapid expansion of digital technologies has also created new opportunities for criminal activities. Cybercrime and online scams have emerged as significant threats to individuals, businesses, and governments worldwide. As society becomes increasingly dependent on digital infrastructure, understanding cybercrime, online scams, and cyber security has become essential for ensuring a safe and secure cyberspace.

Keywords: *Online Scams, Cybercrime, Information Technology, Artificial Intelligence, electronic crimes*

*Received 14 July., 2026; **R**evised 26 July, 2026; **A**ccepted 28 July, 2026 © The author(s) 2026.*
P**ublished with open access at **www.questjournals.org

I. Introduction

The twenty-first century has witnessed an unprecedented digital revolution. The internet, smartphones, social media platforms, online banking, digital payment systems, cloud computing, and artificial intelligence have transformed human life. Governments, businesses, educational institutions, and individuals increasingly rely on digital technologies for communication, commerce, governance, and social interaction. While these technological advancements have created immense opportunities for growth and innovation, they have also opened new avenues for criminal activities. Cybercrime and online scams have emerged as some of the most serious threats confronting modern societies.

Cybercrime refers to unlawful activities conducted through computers, digital devices, networks, or the internet. Unlike conventional crimes, cybercrimes transcend geographical boundaries, making detection and prosecution significantly more challenging. Criminals can operate anonymously from one country while targeting victims in another. The rise of digital payments, online shopping, social networking, and remote working environments has expanded the attack surface for cybercriminals.

The alarming increase in cybercrime incidents worldwide demonstrates the dark side of digitalization. From identity theft and financial fraud to ransomware attacks and cyberterrorism, cybercriminals continuously exploit technological vulnerabilities and human psychology. Online scams have become increasingly sophisticated, utilizing artificial intelligence, deepfake technology, phishing techniques, and social engineering methods to deceive victims.

India, with one of the world's largest internet user populations, has become both a beneficiary and victim of digital transformation. Government initiatives such as Digital India, Unified Payments Interface (UPI), online governance systems, and digital banking have accelerated internet adoption. However, the rapid digital expansion has also exposed millions of users to cyber threats. Reports of digital arrest scams, fake investment schemes, phishing attacks, and social media frauds have become common.

This article examines the growing menace of cybercrimes and online scams, their causes, types, impacts, legal challenges, and possible solutions for creating a safer digital ecosystem.

[1] The Writer is an Academician and an Experienced Journalist based in Jaipur.
[2] The Writer is a 5th Year Student of BALLB in Seedling School of Law and Governance, Jaipur National University, Jaipur.

Understanding Cybercrime

Cybercrime involves unlawful activities that are committed using computers, mobile devices, or the internet. In some cases, computers serve as the target of criminal attacks, while in others they function as tools to facilitate illegal activities.

Cybercrime can be broadly classified into three categories:

1. Crimes Against Individuals

These offenses target specific individuals and include identity theft, cyberstalking, cyberbullying, phishing attacks, and online harassment. Victims often suffer financial losses, emotional distress, and reputational damage.

2. Crimes Against Property

These crimes involve unauthorized access to computer systems, theft of digital assets, intellectual property violations, data breaches, and malware attacks. Businesses are particularly vulnerable to such offenses.

3. Crimes Against Governments and Society

Cyber terrorism, attacks on critical infrastructure, espionage, and dissemination of harmful misinformation can threaten national security and public order.

The increasing sophistication of cybercriminals has transformed cybercrime into a global challenge requiring coordinated responses from governments, law enforcement agencies, technology companies, and citizens.

Online Scams: A Growing Threat

Online scams have become one of the most common forms of cybercrime. Scammers exploit human trust, curiosity, fear, and greed to manipulate victims into revealing personal information or transferring money. Cybercriminals send fraudulent emails, text messages, or social media communications that appear to originate from legitimate organizations such as banks, government agencies, or e-commerce platforms. Victims are tricked into providing passwords, banking details, or personal information. Besides this, the growth of digital payment systems has led to a rise in banking frauds. Criminals use fake customer care numbers, malicious links, and fraudulent payment requests to steal money from unsuspecting users. In India, scams involving UPI transactions have become increasingly common. Lottery and Prize Scams, another type of scams, are rising, wherein victims receive messages claiming they have won a lottery, prize, or contest. To claim the reward, they are asked to pay processing fees or provide personal information. Once the payment is made, the scammer disappears. Fraudsters advertise fake job opportunities and demand registration fees, training charges, or security deposits. Job seekers are particularly vulnerable to such scams due to economic pressures.

Cybercriminals promise high returns through fake investment schemes, cryptocurrency trading platforms, or Ponzi schemes. Many victims lose substantial sums of money in pursuit of unrealistic profits. Scammers create fake profiles on social media and dating websites to establish emotional relationships with victims. After gaining trust, they request financial assistance for fabricated emergencies.

Fake websites and online stores attract customers with heavily discounted products. Victims make payments but either receive counterfeit goods or nothing at all.

Deepfakes have become the latest trends of online scams, which is Artificial Intelligence (AI) generated spoof images or videos intended to deceive or threaten people. This modifies reality and then deceives the audience and the person's supporters. This is typically done to harm the individual emotionally and psychologically, as well as to tarnish their reputation. There is a similar concept of image morphing, where someone digitally alters a photo to change a person's appearance, often to embarrass or defame them. This resulted in sextortion from the innocent, communal violence, and business dealings in the names of other famous people and celebrities.

Impact of Cybercrime and Online Scams

Cybercrime and online scams cause massive financial ruin, severe psychological trauma, identity theft, and operational disruptions for individuals and businesses worldwide. Fraudsters exploit digital networks for targeted operations—like fake investments, deepfake scams, and ransomware—costing the global economy hundreds of billions while severely eroding public trust in internet systems.

Understanding the widespread consequences highlights why implementing strong digital hygiene and utilizing local reporting mechanisms is critical:

- Victims often lose their life savings to high-yield investment scams, romance frauds, and digital arrest tactics. The invasion of privacy and the feeling of violation lead to long-lasting stress, anxiety, and social isolation. Stolen personal details are frequently used to open illicit lines of credit, ruin personal reputations, or target vulnerable family members.
- Attackers lock companies out of critical networks, causing costly downtime that can force small to medium-sized businesses into bankruptcy. Corporate espionage and data breaches result in the loss of

proprietary information and competitive advantage. A highly publicized data breach can shatter customer trust and lead to steep legal consequences and regulatory fines.

- State-sponsored cyberattacks or cyber-terrorism can incapacitate power grids, water supplies, and transportation systems, severely endangering public safety.
- Organized cyber-fraud operations—such as human trafficking rings forcing victims to run "pig butchering" scam centers—siphon billions out of legitimate local economies

Cyber Security: The First Line of Defense

Cyber security refers to the protection of digital systems, networks, devices, and data from unauthorized access, attacks, and damage. Effective cyber security requires a combination of technology, policies, and user awareness. First, Users should create unique and complex passwords for different accounts. Password managers can help generate and store secure credentials. Secondly, Multi-factor authentication adds an additional layer of security by requiring users to verify their identity through multiple methods. Third, Software developers regularly release patches to address security vulnerabilities. Keeping systems updated reduces exposure to known threats. Fourth, Encryption converts data into a coded format that can only be accessed by authorized users. Reliable antivirus programs help detect and remove malware before it causes damage. Regular backups ensure that important data can be restored in the event of ransomware attacks or system failures. Organizations should conduct regular cyber security awareness programs to educate employees about phishing, social engineering, and safe online practices.

Common Cybercrime Incidents

The common cybercrime incidents are related to online transaction fraud, identity theft, deep-fake creation, online stalking, sextortion, fake social media profiles and job scams. Overall, cybercrime has become one of the biggest threats to personal security and public trust in today's digital era. A few of the common cybercrimes that usually happen, and remedies to avoid them are discussed below:

1. Identity theft: Identity theft is the unlawful and dishonest use of another person's identity and private information, such as a name, photo, or identification number (ID number), for one's own benefit, usually with the intention of defrauding or defaming the person whose name is used. Many people now know that creating fake profiles or impersonating someone on social media to harm their reputation or attract attention is a common cybercrime, but they do not know how to get a remedy if they become the victim of that. Such acts can result in mental discomfort, embarrassment, and a loss of personal safety since private photos or information may be made public without consent. For instance, a man in Noida used a woman's pictures to make a fake Instagram profile without getting her permission and attempted to blackmail her by sharing her personal photos. A first information report (FIR) was registered against him under Section 66-C, Information Technology Act, 2000, for identity theft. Later, the police discovered that her colleague had made the fake account. Whenever anyone gets into this kind of situation, the victim can report the incidents on the "National Cybercrime Reporting Portal", which is accordingly converted into FIRs and subsequent action thereon is handled by the State/Union Territory (UT) law enforcement agencies concerned.

2. Cyber fraud: Cyber fraud is the illegal use of digital systems or data for financial gain. It may target individuals, companies, or even governmental organisations. Cybercriminals put individuals, companies, and governmental entities at risk by using technological flaws to commit online fraud and data breaches. For instance, a former employee of a private company was arrested for generating fake invoices to falsely claim input tax credit under the Goods and Services Tax (GST). He was booked under the Nyaya Sanhita, 2023 and the Information Technology Act, 2000. In another instance, in Mangaluru, police discovered a gang that forged Aadhaar cards and tenancy documents to help accused individuals secure bail using fake identities. This case showed how digital forgery can harm the credibility of legal processes.

3. Cyberstalking: Persistent online harassment, monitoring, or threatening messages are referred to as cyberstalking. The phrase itself implies that someone regularly monitors your online behaviour, even if they show no interest in you and occasionally, even specifically, instructs you not to message and follow. Usually, the accused would utilise a fake, or someone else's account, to accomplish this. In an instance, 23-year-old man was sentenced to three years in prison for stalking a 15-year-old girl on WhatsApp. He sent obscene messages and threatened to harm himself if she did not reply. The court convicted him under Section 354-D, Penal Code, 1860 and Section 11(4), Protection of Children from Sexual Offences Act, 2012 (POCSO Act), along with fines and victim compensation.

4. Deep-fake technology: Deepfakes are artificial intelligence (AI) generated spoof images or videos intended to deceive or threaten people. This modifies reality and then deceives the audience and the person's supporters. This is typically done to harm the individual emotionally and psychologically, as well as to tarnish their reputation. There is a similar concept of image morphing, where someone digitally alters a photo to change a

person's appearance, often to embarrass or defame them. This resulted in sextortion from the innocent, communal violence, and business dealings in the names of other famous people and celebrities.

In order to get protection from the deepfakes, citizens from throughout the country approach the Delhi High Court. As Delhi High Court is renowned for defending intellectual property rights. There is no culture like the one that emerged at the Delhi High Court to safeguard intellectual property anywhere in the country. This is the reason several celebrities petitioned this court to have their personality rights protected from AI-generated videos and altered photos. The Delhi High Court consequently issued a number of rulings in support of well-known people and celebrities to shield them from harm to their reputations caused by AI-generated videos.

Reported instance: One of the cases is of the famous journalist and editor-in-chief of DD News Sudhir Chaudhary, who also filed for the protection of personality rights before the Delhi High Court, where the Court has passed an interim order protecting the personality rights of the journalist from deepfake videos on YouTube from using in his name, image, likeness and voice, and regarding circulation of allegedly misleading and AI-generated videos against him on social media. The Delhi High Court recently addressed cases involving deepfakes and unauthorised use of celebrity images. The Court emphasised that personality rights, including names, voices, and likeness, should be legally protected under intellectual property principles. In a much-known instance, an influencer from Assam was targeted when her ex-boyfriend used AI tools to create sexually explicit deepfake images and sold them online. He earned nearly Rs 10 lakhs through subscriptions before being arrested. Police warned that sharing such fake content is also punishable.

5. Online banking and Unified Payments Interface (UPI) fraud: These are among the most common and fast-growing cybercrimes in India today, especially with the use of UPI (Google Pay, PhonePe, Paytm, etc.).

Online transaction fraud typically occurs through gaming apps, betting apps, Telegram links, cryptocurrency platforms, peer-to-peer (P2P) transactions, and others. When a complaint about a fraudulent transaction is received by the cybercrime police or when they intercept it themselves, they mark the transaction on a layered basis and then proceed accordingly. If someone becomes a victim of online fraud and their account is marked under layers 1 and 2, there is a possibility of arrest, as the police can conduct searches and seizures, and may also call for the production of documents under Section 94, Nyaya Sanhita, 2023 (BNSS). Therefore, if someone is a victim of such a crime, they should file a representation with the cybercrime police and the bank. If the cybercrime police are from a different State, then send your grievance through email and speed post to get an appropriate response and understand the nature of the allegation imposed against you. Once you receive a reply to your representation and if the account hold exceeds the fraudulent transaction amount, you can request the bank to remove the lien or hold on the account due to enhanced due diligence (EDD). The victim can then instruct the bank to lift the hold on the account based on the cybercrime police report. You can also call on 1930 helpline number to know the reason for the lien or freeze of the account.

Mumbai Police in 2024 stated that they received 2000 to 2500 calls on a daily basis on the "1930" helpline number. After receiving the complaint, they transfer the complaint swiftly to the Nodal Police Officers of the banks, wallet or merchant concerned, to try and freeze the funds; who then coordinate and make every effort to save the money of the citizens.

In 2024, Mumbai Police reported an increase in UPI-related scams, where fraudsters sent fake payment links or one-time password (OTP) requests to trick victims into transferring money. Many scammers pretended to be buyers on platforms like OnLine eXchange (OLX) or Quikr. Victims were advised to never click on payment links or share OTPs and to verify UPI transactions directly on their bank app.

6. Ransomware attacks on institutions: These crimes lock down the data of businesses, companies, powerhouses, hospitals, or even universities and demand cryptocurrency or ransom payments. Sometimes they just sell it on the dark web. Attacks of this nature typically originate from foreign nations that wish to utilise the data to monitor other nations. They close the institutions in order to undermine the public's trust in the government and give them more options, which led to a resurgence of industry and services throughout the nation. In 2023, sensitive patient data was compromised in a significant ransomware attack that shut down hospital servers for several days at the All India Institute of Medical Sciences (AIIMS), Delhi. The attack demonstrated how even important government agencies can become targets of cyberattacks.

7. Job scams and phishing e-mails: Online job scams are becoming widespread, especially those promising remote work or part-time income. Fraudsters collect victims' personal and sensitive data and take money for becoming members through fake offers.

Sometimes they even send the money into the innocent victim's account by giving them false promise of a job where they give them a job of liking a post or sharing the post to other people, creating more accounts on their platforms, paying for viewing images for the certain times for which they reward them initially; when cybercrime raises the flag, to escape the liability of fraud, and real fraudsters show themselves as the victim and the real victim is treated as a fraudster by the police, and sometimes they even get arrested also.

In an instance in Hyderabad, the cyber police arrested a gang operating a fake job portal that offered "high-paying remote jobs", requiring victims to pay a registration fee. Over 200 jobseekers were defrauded before the website was taken down.

8. Cryptocurrency and investment frauds: Nowadays, scammers defraud individuals by using phoney trading apps or bitcoin sites. In order to avoid taxes and government liability, the fraudsters use various digital platforms to create a fake screen that shows unimaginable profits from cryptocurrency and shares. They then start offering investment ideas to the inexperienced viewers and ask them to register on the phishing links, which either deduct their money initially or cause their accounts to be frozen later. And occasionally, they do not file a complaint against the same, as they are afraid of the inquiry being conducted against them.

A Bengaluru-based tech worker lost Rs 12 lakhs in a cryptocurrency scam after being lured by a fake Telegram investment group promising high returns. The case showed how digital currency fraud is rising rapidly in India.

9. Cyberbullying and online harassment: The practice of bullying other users, including influencers, politicians and celebrities, is a global offense that has left no one unpunished. When it comes to leaving comments and messaging someone, there is no check and balance, just as there is no rigorous mechanism to restrict the same. However, in accordance with the Digital Personal Data Protection (DPDP) Regulations, if someone objects, the corporation must remove it within the stipulated time frame; if they do not, they might face a fine of up to 200 crores.

In Pune, a teenage boy was booked for sending threatening messages and edited images to classmates on social media. The case raised awareness about the impacts of mental health and the importance of cyber ethics in schools.

Case Studies of the Cybercrimes

1. **Belagavi Senior Citizens Fraud Ring (2025)**:

In late 2024 and early 2025, police in Belagavi, Karnataka discovered and dismantled a sophisticated fraud ring that had defrauded senior citizens of over Rs 2.3 crore. The case highlights how dark web data can enable real-world fraud. The gang obtained databases of personal information names, phone numbers, email addresses, and even some banking details through dark web markets. These databases came from previous data breaches of Indian e-commerce sites, social media platforms, and telecom companies. Using this data, the gang created profiles impersonating U.S. government officials, immigration officers, and business executives. They contacted elderly Indians via phone and email, claiming that the victim had won a lottery, or that their bank account had been compromised and required verification, or that they were eligible for U.S. immigration sponsorship. Through social engineering, the gang convinced victims to either wire money for supposed "processing fees," or to disclose banking credentials that the gang then used to steal directly from bank accounts. The investigation began when multiple victims complained to the local police about receiving calls from people claiming to be U.S. officials. Police cross-referenced the phone numbers and communication patterns and identified a group operating out of a few locations in Belagavi. Raids on their premises revealed computers with access to multiple dark web markets, evidence of purchasing stolen databases, and logs of successful fraud conversations. Approximately 30 individuals were arrested, and the gang was prevented from committing further fraud. The investigation also traced the stolen data they had purchased back to the original data breach sources, leading to additional investigations into security practices at major Indian companies.

2. **The Raj Kundra Bitcoin Scam (2025)**

In 2025, the Enforcement Directorate charged Raj Kundra, a prominent businessman, with involvement in a Rs 150+ crore Bitcoin scam. The investigation alleged that money from various financial frauds and illegal activities was being funneled into Bitcoin purchase schemes, and then the Bitcoin was being used to purchase property and other assets to legitimize the proceeds. The case highlighted how cryptocurrency can be integrated into larger money laundering operations and how the ED is developing capacity to investigate such schemes.

3. **Maharashtra Cryptocurrency Money Laundering Operation (2025):**

In mid-2025, the Enforcement Directorate (ED) began investigating a major money laundering operation in Maharashtra that moved approximately Rs 850 crore through cryptocurrency channels. The Operation The operation functioned as follows: illegal money (from drug trafficking, extortion, and other crimes) was converted to cryptocurrency on unregulated exchanges. The cryptocurrency was then moved through multiple wallets and exchanges, both regulated and unregulated, to obscure its origins. Eventually, the cryptocurrency was converted back to rupees through regulated exchange services, or moved to foreign bank accounts. The investigation revealed connections to dark web activity, with some of the illegal funds originating from dark web drug marketplaces where Indian drugs were sold internationally, with payments received in Bitcoin. The ED became aware of the operation through its monitoring of large cryptocurrency transactions and unusual patterns. This led to seizure of cryptocurrency wallets, interviews with exchange operators, and eventually arrests of key individuals in the operation. Hundreds of crores of rupees in cryptocurrency assets were seized,

and investigations into money laundering links to organized crime and international criminal organizations are ongoing.

4. Delhi-NCR Healthcare Sector Ransomware Attacks (2024):

Throughout 2024, several hospitals and healthcare facilities in Delhi and surrounding areas experienced ransomware attacks, with attackers demanding payment in Bitcoin. The attacks typically began with a phishing email sent to hospital staff members. The email appeared to come from a legitimate source (sometimes the hospital's own administration) and contained an attachment or link that, when clicked, installed ransomware on the victim's computer. Once installed, the ransomware spread laterally through the hospital's network, eventually encrypting critical medical systems, patient databases, and administrative systems. The attackers then demanded substantial ransom payments (ranging from Rs 10 lakh to Rs 5 crore depending on the size of the hospital) in Bitcoin. The attacks were detected when hospital staff noticed systems going offline and ransom notes appearing. The hospitals and law enforcement discovered dark web connections through analysis of the ransom notes, which included links to dark web chat rooms for negotiations. Investigation revealed that the ransomware had been developed by a criminal group operating out of Eastern Europe, but had been leased (through a Ransomware-as-a-Service model) to affiliates who deployed it against Indian targets. While some hospitals paid ransom (paying cybercriminals is controversial and often discouraged by law enforcement as it incentivizes further attacks), others did not and instead worked with cybersecurity firms to remove the ransomware and restore systems from backups. Law enforcement conducted international cooperation efforts to identify the attackers, but prosecution has been complicated by the attackers' location outside of Indian jurisdiction.

How Cybercriminals Weaponize AI

Generative AI's abilities to assist with coding, create content that looks legitimate, and quickly create large quantities of content are especially notable vis-à-vis criminal activity. Major areas of concern are bias and discrimination, privacy invasion, security risks, misinformation, and deepfakes. Many traditional criminal activities are made more effective through the use of AI technologies. For example, spear phishing becomes more convincing with AI-generated personalized emails, and market manipulation can be executed more efficiently using AI algorithms to analyze and exploit financial data. Crimes that were out of reach for some bad actors become possible when AI can fill skill gaps, such as AI coding assistants for the creation of malware.

- **Deepfakes & Voice Cloning:** Hackers synthesize hyper-realistic video and audio to bypass identity verification and execute highly convincing Business Email Compromise (BEC) scams and financial fraud. The use of AI in elder fraud is a growing concern, as it enables more convincing and sophisticated scams targeting vulnerable older adults. These scams often involve the use of AI technologies like voice cloning and emergency scams, exploiting the trust and emotions of the elderly. In a real-world incident, an 82-year-old man in Texas was defrauded of $17,000 after receiving a call from someone using AI to clone his son-in-law's voice, falsely claiming to be in jail and in need of bail money. Another case involved a woman who received a call from what sounded like her daughter, claiming to be kidnapped. The AI-generated voice was so convincing that she nearly wired money to the scammers before realizing it was a fraud. The U.S. Senate Committee on Aging has highlighted this growing threat in its annual fraud report, noting that AI-driven scams targeting older Americans are on the rise, with estimated losses reaching $1.6 billion in 2022.
- **Intelligent Phishing:** Generative AI allows attackers to bypass traditional spam filters, producing native-sounding, culturally tailored emails and messages that trick users into surrendering sensitive information. One specific type of phishing is spoofing. In this instance, the fraud actor impersonates a person or company with an email or website made to imitate the logos of a well-known business or individual. Once a person falls victim to this scam, they can lose money, have their identities stolen, or be infected with malware that allows attackers to take control of their computers. Spear phishing has proven to be the largest, most common, and most costly form of cyber threat, with an estimated 300,000 reported victims in 2021 representing $44 million in reported losses in the United States alone. There were over 2.76 million complaints filed with the FBI between 2017 and 2022, with both the number and the total dollars lost increasing every year.
- **Malware Development & Evasion:** Cybercriminals utilize uncensored Large Language Models (LLMs) to rapidly write, obfuscate, and mutate malicious code, effectively bypassing traditional antivirus and security software. In July 2023, for example, cybersecurity researchers discovered a new AI malware tool called WormGPT, which is being marketed on dark web forums as a BlackHat alternative to ChatGPT. AI is also changing the way cybercriminals create and deploy malware, making it more dangerous and harder to detect. This new breed of malware, known as AI-powered malware, uses advanced technology to outsmart traditional security measures. Traditional security tools are struggling to keep up with these smart, AI-powered threats. The malware's ability to change and hide makes it a serious challenge for cybersecurity experts. To fight this new threat, cybersecurity

teams are also turning to AI by developing advanced detection methods that can spot unusual behavior and adapt to new threats quickly. As AI continues to evolve, both attackers and defenders will keep pushing the boundaries of this technology. Staying informed and adapting quickly will be crucial in the ongoing battle against AI-powered malware.

Defensive AI & Cybersecurity

To counter the increasing volume and sophistication of modern cyber threats, both local enterprises and global organizations are deploying AI-driven solutions to secure their networks:

- **Predictive Analytics:** AI continually analyzes large datasets and user behavior patterns to build baselines, immediately flagging anomalous activities that indicate unauthorized access.
- **Automated Threat Mitigation:** Security systems can automatically isolate compromised devices, patch vulnerabilities, and restrict permissions before a threat fully escalates.
- **Endpoint Protection:** Vendors utilize behavioral AI to detect malicious processes and thwart ransomware deployment, blocking attacks at the device level.

Legal Framework for Cybercrime in India

India has established a legal framework to address cybercrime and strengthen cyber security.

- **Information Technology Act, 2000**

The Information Technology Act, 2000 serves as the primary legislation governing cybercrime in India. It addresses offenses such as unauthorized access, hacking, identity theft, cyber terrorism, and data theft.

- **Digital Personal Data Protection Act, 2023**

The Act seeks to protect personal data and establish accountability for organizations processing digital information.

- **Bharatiya Nyaya Sanhita, 2023**

Several provisions of the Bharatiya Nyaya Sanhita complement cybercrime laws by addressing cheating, fraud, forgery, criminal intimidation, and related offenses committed through digital means.

Cyber Crime Reporting Portal

The Government of India has established the National Cyber Crime Reporting Portal, enabling citizens to report cybercrime incidents and online frauds.

Way Ahead

Cybercrime and online scams have become inevitable challenges of the digital age. While technological advancements have created immense opportunities for economic growth and social development, they have also expanded the scope for criminal exploitation. Cybercriminals continuously evolve their tactics, targeting individuals, businesses, and governments through sophisticated attacks and deceptive schemes.

Strong legal frameworks, technological safeguards, public awareness campaigns, and responsible digital behavior are essential components of a comprehensive cyber security strategy. Through vigilance, education, innovation, and international cooperation, a safer and more secure digital future can be achieved for all.

References

[1]. Christin, N. (2023). "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace." In Proceedings of the 22nd International Conference on World Wide Web (pp. 213-224).

[2]. ACM. Finklea, K. M. (2015). "Deep Web and the Darknet: A brief overview." Congressional Research Service Report, 7-5700, 2-10.

[3]. Barratt, M. J., & Aldridge, J. (2016). "Everything you always wanted to know about drug cryptomarkets but were afraid to ask." International Journal of Drug Policy, 35, 1-6.

[4]. Dingledine, R., Mathewson, D., & Syverson, P. (2004). "Tor: The second-generation onion router." In USENIX Security Symposium (Vol. 4, pp. 303-320).

[5]. Thiel, P. (2014). "The dark web." In The Atlantic (March 2014 issue).

[6]. Stamm, S., & Husted, S. (2007). "Anonymity, pseudonymity, and identity: How to stay anonymous on the Internet." Computer & Security, 17(5), 362-378.

[7]. Dingledine, R., & Mathewson, D. (2006). "Anonymity loves company: Usability and the network effect." In The 5th Workshop on Economics of Information Security (WEIS 2006).

[8]. Bergman, A. (2016). "Silk Road: A digital hunt." In The New Yorker (December 2016).

[9]. Yip, M., Webber, N., & Shaikh, S. A. (2013). "Structural analysis of the dark web." IEEE Internet Computing, 17(5), 32-40.

[10]. Kshetri, N. (2017). "Can India harness artificial intelligence for development?" Journal of Global Information Technology Management, 20(4), 278-298.

[11]. Belagavi Police Department. (2025). "Case Report: Senior Citizens Fraud Ring." Unpublished Government Report. (Obtained through PIB Release, November 2025).

[12]. Evan Carmen. "AI Making Scams More Believable: We Need To Stay Ahead of the Curve." B'nai B'rith International. Accessed June 22, 2025. https://www.bnaibrith.org/ai-scams/.

[13]. Ed Prince. "Generative AI Threatens Seniors." Rethinking65. January 31, 2024. Accessed June 22, 2025. https://rethinking65.com/2024/01/31/generative-ai-threatens-seniors/.

[14]. Fox News. "Scams Targeting Older Americans, Most Using AI, Caused Over $1 Billion in Losses in 2022." Fox News. Accessed June 22, 2025. https://www.foxnews.com/politics/scams-targeting-older-americans-most-usingai-caused-1-billion-losses-2022
[15]. Shawn Davis and Gorkem Batmaz. "Generative AI and Accelerated Computing for Spear Phishing Detection." NVIDIA Technical Blog, September 12, 2023. Accessed July 09, 2026. https://developer.nvidia.com/blog/generative-ai-and-accelerated-computing-for-spear-phishing-detection/.
[16]. Abby Miller. "The Real Cost of Spearfishing, Spoofing and Phishing." DM News. January 4, 2023. Accessed June 22, 2026. https://cdn-1.dmnews.com/spearfishing-spoofing-phishing/.