INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

AN EMPIRICAL STUDY ON CYBER CRIME, CYBERSECURITY AWARENESS, AND PREVENTIVE TECHNIQUES AMONG INTERNET USERS

AUTHOR – MOHAMED JAMEER ALI H, LLM [CRIMINAL LAW] STUDENT, CRESCENT SCHOOL OF LAW, B.S. ABDUR RAHMAN CRESCENT INSTITUTE OF SCIENCE AND TECHNOLOGY, CHENNAI

BEST CITATION - MOHAMED JAMEER ALI H, AN EMPIRICAL STUDY ON CYBER CRIME, CYBERSECURITY AWARENESS, AND PREVENTIVE TECHNIQUES AMONG INTERNET USERS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (13) OF 2025, PG. 287-297, APIS – 3920 – 0001 & ISSN - 2583-2344

Introduction

The emergence of technology has given women the chance to discover their strengths and expand their abilities. As rapid modernisation occurs globally, the internet has integrated into our everyday routines. It is an effective means of communication. Nonetheless, as reliance on cyberspace grows, so too have internet crimes targeting women. Women globally have faced various forms of harassment for many years now. With the rise of technology and digitalisation, individuals can connect online with anyone, at any time, and from anywhere in the world. Cybercrime has become one of the outcomes of this modernisation. Digital platforms are frequently utilised to intimidate and mistreat women for the sake of voyeuristic enjoyment. A primary reason for its occurrence is that over fifty per cent of online users lack a complete understanding of how online platforms like WhatsApp, Skype, Facebook, etc., operate. Users receive very little sufficient training and education. Additionally, a lack of understanding regarding technological progress has paved the way for these atrocious acts. Women are frequently victims of cyber stalking, cyber pornography, impersonation, and other related crimes. Victims often place their trust in the perpetrator and reveal private data or information, leading to countless cybercrimes occurring each day. Owing to the fear of being defamed in society and insufficient evidence, pinpointing the source of the crime becomes quite challenging. Cybercrime has evolved into a notion where most victims are women who have succumbed to technological allure. A sharp rise in cybercrime rates has been noted in various nations, with the main focus consistently being on the safety of women. India ranks among.

Cyber Crime?

Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones".[460]

Cybercrime entails the utilisation of the internet and computers. It jeopardises a person's privacy by revealing or sharing their private or sensitive information online to undermine their reputation and inflict physical or psychological distress, whether directly or indirectly. Typically, women are the primary targets of these criminals due to their inexperience and lack of understanding of the online realm, making them susceptible to technological illusions.

Debarati Halder and K. Jaishankar enhance the understanding of cybercrime through a gender lens, describing "cybercrime against women" as offences aimed at women with the intent to

[460] https://www.igi-global.com/dictionary/securing-financial-inclusiveness-adoption-of-blockchain-fintech-compliance/103506

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 13 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

deliberately inflict psychological and physical harm, utilising modern telecommunications like the internet and mobile devices.

Development of cybercrime

Cybercrime has evolved from the Morris Worm to ransomware. Numerous nations, such as India, are striving to avert such offences or assaults; however, these aggressions are developing and influencing our nation. Cybercrimes encompass any illegal activity carried out using a computer. Systems or networks, either in alignment with their framework or in opposition to it. Theoretically, it encompasses any offence that can be carried out in the digital setting. In other terms, offences carried out through the use of e-computers in relation to processed information and utilised on the internet can be classified as cybercrimes.

Years Types of Attacks

In 1997, Cybercrimes and viruses initiated, including the Morris Code worm and others.

In 2004, Malicious, Trojan and Advanced worm.

In 2007, Phishing and identifying thieves.

In 2010, DNS attacks, SQL attacks and the Rise of Botnets.

In 2013, Botnets, Malicious Emails, Social Engineering, DOS Attacks, and Ransomware attacks.

Present Banking Malware, Keylogger, Android hack, Bitcoin wallet, Phone hijacking, Cyber warfare, etc.

Cybercrime and its categorisation

Cybercrime is a broad term that describes unlawful activities in which computer networks are employed as a resource, a goal, or a site for unlawful actions, and may encompass anything from digital breaches to service interruption attacks. It likewise pertains to traditional offences involving computers or networks that are utilised to enable the unlawful behaviour. David L. Charter offers the most comprehensive classification of computer offences, categorising them into three primary groups.

Types of Cyber Crime

1. Cyberstalking

In the contemporary world, it ranks among the most frequently perpetrated offences. It entails tracking someone's actions and secretly following him/her. It consists of collecting information that could be utilised to intimidate an individual or to make untrue allegations or threats. A cyber stalker utilises the internet to harass someone, meaning they don't present a direct physical danger to the person. However, the anonymity of online interactions makes it challenging to identify the cyber stalker, increasing the prevalence of this crime compared to physical stalking.

A primary focus of cyber stalking is women and children, who are often pursued by men and adult predators, primarily for revenge, sexual harassment, and ego. In many cases, the victim lacks awareness of internet usage and regulations, while user anonymity has played a role in the increase of cyber stalking as a type of crime. The individual committing this offence may face charges for violating confidentiality and privacy under Section 72 of the IT Act, 2000, since cyber stalking is not yet addressed by the current cyber laws in India. Additionally, sections 441 and 509 of the IPC are applicable for this as well.

2. Denial of Service attack

The victim's computer is overwhelmed with an excess of requests that it cannot manage, resulting in it failing. A Distributed Denial of Service (DDoS) attack is likewise a kind of denial-of-service assault, where the perpetrators are numerous and prevalent. Of course. E.g., Amazon, Yahoo.

3. Virus assault

Viruses are applications that link themselves to a computer or a document and then distribute themselves to other documents and to other machines on a network. They typically influence

the information on a computer, either by modifying or removing it.

4. Worm assaults

Unlike viruses, worms do not require a host to cling to. They simply create practical replicas of themselves and continue doing this until they've consumed all the Space that is accessible in a computer's memory. For example, the Love Bug malware impacted at least 5% of the world's computers. The Losses were reported to be $ 10 million. The globe's most well-known worm was the Internet worm released on the Internet by Robert Morris around 1988.

5. Logic bombs

These are programs that depend on specific events. This suggests that these programs are designed to accomplish a specific task only when a specific occurrence (referred to as a trigger event) takes place. Certain viruses can also be categorised as logic bombs due to their remaining inactive throughout the year and only becoming engaged on a specific date (similar to the Chernobyl virus).

6. Phishing

It involves trying to deceive users into revealing their private security details, their financial credit card numbers, banking information, or additional confidential data by pretending to be reliable companies in an electronic email. The messages might request the recipients to refresh, verify, or authenticate their account details. Phishing is a deceptive practice that involves tricking individuals into revealing sensitive information, such as usernames, passwords, or credit card details, typically through misleading emails or websites that appear legitimate. Twice victimised, initially by stealing a company's identity and subsequently by exploiting it.

7. Cyber Pornography

It poses a significant risk to the safety of women and children, as it entails sharing and distributing pornographic images, photographs, or texts via the internet, which can rapidly be duplicated on multiple electronic devices. It pertains to the depiction of sexual content online.

A.P. Mali states, "It is the visual, sexually explicit subjugation of women via images or language that encompasses pornography, consisting of verbal or visual content portraying or depicting sexual conduct that degrades or mistreats one or more participants, thereby endorsing such degradation." The choice or consent of a person to be harmed, abused, or coerced does not change the degrading nature of such actions. Approximately 50% of all websites on the internet host pornographic content featuring images of women, which poses risks to their integrity.

As per the IT Amendment Act 2008, "the crime of pornography under section 67-A refers to anyone who publishes, transmits, or causes to be published and transmitted in electronic format any material featuring sexually explicit acts or conduct, which can be classified as pornography." Sections 292/293/294, 500/506, and 509 of the Indian Penal Code, 1860 are also relevant, and the victim may file a complaint at the nearest police station to the location of the crime or where they become aware of it. Upon establishing guilt, the defendant may face a primary conviction leading to imprisonment for a duration of up to five years, along with a possible fine that could reach ten lakh rupees. In the second offence, the prison sentence can last up to seven years, and the fine may reach ten lakh rupees.

8. Cyber Morphing

It is a type of offence where the original image is altered by an unauthorised individual or someone with a false identity. Images of female users from their profiles are captured and subsequently altered before being shared by fake accounts on various platforms for pornographic reasons. The absence of user awareness incentivises criminals to engage in such dreadful acts. Cyber morphing or Cyber obscenity is punishable under sections 43 and 66 of the Information Act 2000.

9. Cyberbullying

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Cyberbullying entails using the internet to embarrass or humiliate someone by disseminating their personal or private information, as well as sending, posting, or sharing harmful or misleading content through digital devices such as computers, tablets, laptops, and smartphones. It can occur via SMS, online gaming networks, internet forums, or social media platforms, where information can be shared online and is accessible to many individuals. Cyberbullying is ongoing and enduring, which can damage the online reputations of not only the victim but also both parties involved.

10. Email Forgery and Impersonation

It ranks among the most prevalent forms of cybercrime. It entails sending an email that indicates its source. In contemporary times, this type of crime has become increasingly prevalent, making it quite challenging to determine if the email received is genuinely from the actual sender. Email spoofing is primarily employed to illicitly obtain personal details and private photos of women, which are subsequently used for blackmail. A report indicates that phishing attacks have risen by 280% since 2016. Avanan's research indicates that approximately 4% of all emails received by an individual are fraudulent. In the Gujarat Ambuja Executive case, a 51-year-old cyber-criminal set up a false email account and, posing as a woman, engaged in a "cyber relationship," extorting Rs 96 lakh from a businessman in Abu Dhabi.

Email spoofing constitutes an offence as defined by section 66-D of the Information Technology Amendment Act, 2008, as well as sections 417, 419, and 465 of the Indian Penal Code, 1860. It is a cognizable, bailable, and compoundable offence, with the court's permission, where the prosecution of the offence is pending and is triable by any magistrate

11. Trolling on the Internet

It is a type of online aggression on social media platforms where individuals are allowed to express their opinions freely. Online abusers frequently target individuals who voice their views and hold beliefs that differ from accepted social standards. This section comprises women who face targeted harassment from social media bullies. The Digital Hifazat report states, "women expressing their thoughts online, particularly on subjects often considered to fall under 'male expertise' such as politics or religion, or concerning women's experiences like menstruation, sexuality, or challenging patriarchy, face severe trolling, primarily from self-identified right-leaning accounts on Twitter."

Online harassment impacts both the mental and physical well-being of those targeted. Abuse, derogatory language, and nasty remarks are the primary components of trolling. The primary outcomes of trolling include self-censorship and issues related to mental health.

Cyber offences targeting women in India

India, with around 688 million active users, ranks as the second-largest internet market globally. Platforms such as Facebook, YouTube, Twitter, Instagram, WhatsApp, and Snapchat are among the most popular in India. Although the number of internet users has risen, a gender gap still exists. A report by IAMAI (Internet and Mobile Association of India) on internet usage in India indicates that approximately 67% of users are male, whereas only 33% are female. This imbalance between male and female users is a significant factor contributing to the increase in cybercrime incidents targeting women.

Cybercrimes are unlawful acts that are prohibited by law and carried out through the internet and cyber technology. Cyber-crimes can target any individual, asset, or government; however, this paper specifically examines cyber-crimes directed at women. The National Crime Research Bureau reported a significant rise in the number of cybercrime cases in 2017 compared to previous years.

Since the 1990s, information technology has made significant advancements, and every

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

household with a modest income now has internet access. People of different ages can utilise it anywhere, from their residence to their job. It can be inferred that the internet has evolved into a self-contained world where individuals can exchange, embrace cultural values, or find opportunities. However, it has its drawbacks; the online realm has turned into a space for criminals to deceive women, with some sinking so low as to prey on children. The constant evolution of the internet is complicating detection and regulation, resulting in an increase in cybercriminals. Thanks to technological advancements, cyber criminals can engage in illegal activities under a false identity from anywhere globally. This implies that they have no tangible interaction with the real world and are largely evading consequences without facing any repercussions. By safeguarding anonymity, individuals can access various types of content on the internet, resulting in a vast quantity of anti-social, violent, and aggressive material.

A significant factor contributing to the increase in cybercrime against women, aside from the growth of the internet, is that Indian women often hesitate to report such incidents. They worry it will bring shame to their families. Often, they think it is their own responsibility for the occurrence of the crime. Cyberspace is a separate realm where individuals enter and exit freely. This allows cyber criminals to carry out offences and evade consequences effortlessly.

Requirement for laws addressing cybercrime

Legal actions are crucial for deterring and addressing cybercrime. These are essential in all domains, such as criminalisation, procedural authority, jurisdiction, international cooperation, and accountability and liability of internet service providers. At the national level, existing and proposed cybercrime laws often focus on criminalisation, underscoring a significant commitment to establishing specific offences for essential cybercrime activities.

In our modern tech-driven world, both the planet and criminal activities are becoming more digitally advanced. The Internet was initially created as a platform for research and information sharing in an unrestricted manner. As time went on, it became increasingly transactional, incorporating terms like e-business, e-commerce, e-governance, and e-procurement. Cyber laws tackle all legal issues stemming from internet-related crimes. The demand for cyber laws and their enforcement has risen alongside the growing population of internet users.

Lacuna in existing cyber law

The online verbal abuse that lacks sexual content is not adequately addressed. General sexist remarks have not been considered under Section 499 and Section 507 of the IPC, which address criminal defamation and criminal intimidation related to personal trolls. Additionally, doxing that does not involve the distribution of sexual content and lacks any form of intimidation is not considered. Section 66 of the IT Act makes hacking a criminal offence, but it does not clearly mention doxing as a result of hacking. Internet trolling, verbal harassment, and hacking for doxing have been considered personal and individual offences under Section 499 and Section 507 of the IPC, as well as Section 66 of the IT Act. It is crucial to recognise that this act of abuse is perpetrated against women solely because they are women. Historical evidence shows that the mistreatment is rooted in women's sexuality and caste.

Section 66E of the IT Act and Sections 354C and 354D of the Criminal Laws Amendment Act 2013 are exceptions to violence, emphasising physical harm rather than violations of bodily integrity and personal autonomy as described in other sections of the IT Act and IPC. These sections concentrate solely on physical privacy, excluding "informational privacy." Section 509 of the IPC references "Privacy," but it addresses privacy only in relation to women's modesty. "Sexual violence is primarily perceived as a means of upholding public morality by restricting obscenity and safeguarding women's

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

modesty." Additionally, it can be observed that this perspective can be retreated at any moment.

Psychological violence stemming from gender towards women is not acknowledged by the law beyond their family context. Recognition of psychological abuse involving the dissemination of personal information via violations of privacy that are not sexually related has not been achieved.

Moreover, legislation such as the Protection of Women from Domestic Violence Act, 2005, which addresses issues of psychological violence in households and cohabiting partnerships, does not address cybercrime concerning women.

Cybersecurity

Cybersecurity is outlined as the practice of forestalling unauthorised access, misuse, and harm to critical systems, networks, data, and information. It includes a broad range of plans, forms, and processes designed to protect the solitude, chance, and fullness of mathematical characteristics. Cybersecurity demands preventing, recognising, and fighting many dangers connected to the internet, dangers targeted at taxicab attempts, malware contaminations, data breaches, and additional cybercrimes.

Cybersecurity is vital in today's interconnected world to safeguard our algorithms, systems, and data from unauthorised entry, malicious actions, and possible disruptions. The need for effective cybersecurity solutions has become more pressing due to the rapid advancement of technology and increased dependence on digital systems. Modern technologies like cloud estimation, mobile estimation, online investment, and e-commerce require a high degree of security. Given that these electronics contain significant information about an individual, their privacy has become a primary concern. The safety and financial stability of every nation rely on improving cybersecurity and safeguarding the essential foundations of facts. For a society to effectively stop or recover from cyberattacks, all the systems, community, and resources must be in alignment. The processes of identification, evaluation, and correction are three vital freedom operations that can be enhanced through a comprehensive threat management approach. This introduction offers an overview of the key concepts and the importance of cybersecurity.

Challenges that the industry is facing today:

Ransomware Offences

A significant concern regarding high-tech protection in the mathematical era is ransomware. A significant number of ransomware incidents occurred in 2021–2022, with this trend expected to take second place in 2023. Research by ASTRA IT indicates that there are 1.7 ransomware attacks each epoch, impacting individuals in 2 seconds. The typical ransomware attack led to a loss of as much as $1.85 billion. The National Health Service (NHS) paid a reported $100 million in damages due to the WannaCry ransomware incident. The quantity of questionable ventures linked to ransomware SARs reported in the first half of 2021 was projected to reach $590 million, exceeding the total noted for the entire year of 2020 ($416 million), according to Fincen's (Financial Crime Enforcement Network) Financial Trend Analysis report.

IoT (Internet of Things) Attacks

The Internet of Things, also known as IoT, is particularly vulnerable to threats to data security. The Internet of Things (IoT) encompasses all numerical, mechanical, computational, and intelligent systems capable of sending data over a network of web connections, similar to how laptops and smartphones operate. To access users' sensitive information, hackers primarily focus on the IoT sector. Over 14.4 billion connected schemes are anticipated to be prevalent by 2023. IoT Analytics reports that there will be more than 27 billion smart devices connected to the internet

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

by 2025. The report states that by 2022, there will be nearly 12 billion internet-connected devices, while the number of skilled workers will reach 25 billion by the end of 2030.

Malware for Mobile Banking

At first sight, this appears to be a major obstacle for those concerned about ATM skimming. Moreover, innovative methods are being created that will enable criminals to utilise tablets and smartphones to access bank accounts. Mobile banking malware, similar to earlier versions, exploits device vulnerabilities to capture login credentials, credit card information, and other sensitive user data. If their tactics work well, cybercriminals can empty your bank account in under 30 minutes. Consequently, this has transformed into one of the most dangerous challenges that banks will confront in 2023

AI assaults

In 2023, it is expected that consumers and businesses will use AI much more extensively. Cybersecurity may gain from this or be adversely affected. AI can aid security operations centre analysts, identify and prevent attacks, and oversee and detect fraud in the daily tasks of security teams. Almost 68% of research participants believed that artificial intelligence (AI) could be easily leveraged to target their businesses in spear-phishing and impersonation attacks in 2021. It also cautioned that AI could promote ransomware, posing risks to IT security.

Advantages of Cybersecurity

- Secure us from dangerous attacks
- Protection of Confidential Information
- Browse the same website
- Prevention of Financial Loss.

Disadvantages of Cybersecurity

- Cost and Resource Intensive
- False Sense of Security
- Potential for User Inconvenience
- Limited Effectiveness against Insider Threats

Importance of Cybersecurity

Cybersecurity is the process of preventing unauthorised approaches, misuse, and damage to computer systems, networks, data, and information. It involves a broad range of plans, forms, and procedures engaged to defend the confidentiality, accessibility, and dependability of mathematical assets. Cybersecurity requires preventing, spotting, and fighting many dangers connected to the internet dangers such as hack attempts, malware contaminations, data breaches, and different cybercrimes.

Evolving Cyber Threat

The cybersecurity threat landscape is always changing and getting more complex. To conduct cyberattacks, cybercriminals and other bad actors constantly create new methods and take advantage of weaknesses in software, networks, and user behaviour. Financial loss, reputational harm, operational interruptions, privacy violations, and even hazards to national security could be caused by these attacks. The attack surface has been further increased by the introduction of technologies like artificial intelligence, the Internet of Things, and cloud computing, posing new cybersecurity issues.

Purpose

Protecting calculating arrangements, networks, and data from unauthorised approach, use, disclosure, break, or destruction is the aim of cybersecurity. It requires dawdling in place a type of safeguards and processes to keep digital property, structures, and data processing infrastructure against potential dangers like hackers, malware, viruses, dossier breaches, and additional cyber-attacks. Cybersecurity is everything to ensure a delicate dossier from unauthorised access and damage to computing arrangements and networks by guaranteeing the integrity, availability and confidentiality of the dossier and information and confidentiality. To detect, respond to, stop, recognise and recover from cyber threats, a variety of technologies, techniques, and

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

procedures are used. Privacy, Security and trustworthiness of digital systems, networks and data are the main goals of cybersecurity. Effective cybersecurity solutions can help people, businesses, and governments lower the risks posed by cyber threats, safeguard confidential data, and ensure the availability and integrity of their digital assets.

Technology

Network freedom concludes with designated firewalls that monitor and control two interconnecting networks while selling products that adhere to established security arrangements. Between networks and outside networks (like the Internet), they present an image of a firewall, preventing unauthorised access and obstructing hateful traffic. IDS/IPS electronics attend to network traffic for some unusual patterns or behaviours that may be signs of an assault or interruption. They can spot potential inform administrators, protection breaches, and in certain positions, automatically take deterrent measures to hinder assaults in real-time for action or an event. Software for detecting and averting malware, containing as viruses, Trojan mares, ransomware, worms, Trojan mares, ransomware, and spyware, is known as an antimalware program. These finishes act programme, arrangement, and file flipping through in consideration of finding and quarantining malware infections. Cryptographic systems like TLS and SSL are used to secure connections to the Internet. They offer encryption and confirmation, making certain that information shipped between consumers and websites or middle through two-point structures is protected from eavesdropping and interception. Over open networks, like the Internet, VPNs build secure, encrypted connections. They authenticate a private network link, enabling consumers to link by chance or over public Wi-Fi networks and approach possessions carefully and privately.

Cybersecurity techniques/ technical countermeasures against cyber crimes

Numerous technical defences can be employed to discourage hackers and strengthen systems against breaches. Undoubtedly, these countermeasures are already in place; however, it is essential to enhance and fortify them to effectively combat the attacks, as perpetrators are leveraging the latest tools and technology to bypass them. Cryptographic methods can be utilised to encrypt data through various algorithms to conceal information during storage or transmission.

Malware detection tools: This software scans all files and documents in the system for harmful code or viruses. Malware denotes detrimental software like viruses, worms, and Trojan horses.

Firewalls based on networks or hosts are regarded as the primary line of defence in computer network security since they set up Access Control Lists (ACLs) to stipulate which services and traffic are allowed to traverse the checkpoint. To prevent the dissemination of harmful malware, utilise the latest antivirus software. To ensure the safety of computers within a network, it is essential to frequently update virus definitions, as well as operating system hotfixes, service packs, and patches.

Network vulnerability assessment: In this method, technicians or automated tools can perform comprehensive evaluations or assess specific devices, systems, and passwords within a network to gauge their security level.

Physical barriers like locks, card access keys, or biometric devices can serve to stop criminals from gaining physical entry to a networked system. Robust password security for computer system access and BIOS serves as a powerful deterrent against cybercriminals.

Finding

Section A: Demographic Insights

The study covered respondents belonging to two major categories — law students and practising advocates. Most respondents were

frequent internet users, spending more than three hours per day online. The sample included both young learners familiar with digital tools and experienced professionals who use the internet primarily for professional communication, legal research, and case-related correspondence.

Section B: Internet Usage and Online Activities

Most respondents used the internet for multiple purposes, such as communication through social media, academic research, e-filing, online payment of court fees, and professional networking.

A majority of respondents used smartphones as their primary device for internet access. However, many admitted that they occasionally shared personal information online, especially on professional or educational platforms.

It was also observed that only a limited number of participants consistently verified the security of websites (HTTPS/lock icon) before entering sensitive information, indicating a casual approach towards online safety practices.

Section C: Awareness of Cyber Crimes

The term cybercrime was familiar to almost all respondents due to their legal background. Law students demonstrated theoretical awareness gained through academic exposure, whereas advocates had a more practical understanding due to experience in handling cyber-related cases or complaints.

Commonly recognised offences included phishing, hacking, and online fraud. However, awareness of emerging cyber threats like ransomware and deepfake-related crimes was comparatively lower.

Most respondents reported that their primary sources of cybersecurity knowledge were academic materials, online platforms, and media reports rather than formal training. While a majority knew that cybercrimes can be reported to the police or cyber cells, only a few were aware of the detailed procedural mechanisms or the functioning of government cyber portals.

Awareness of the Information Technology (IT) Act, 2000 existed, but respondents expressed that they were only partially aware of its provisions and recent amendments.

Section D: Experience with Cyber Crimes

A notable portion of respondents either personally experienced or knew someone who had faced cyber offences such as online fraud, hacking of social media accounts, or phishing emails.

Despite this, most cases were not formally reported to the authorities. The main reasons cited were lack of awareness regarding complaint mechanisms, fear of reputational harm, and the belief that the issue was minor or would not be resolved effectively.

Those who did report incidents expressed dissatisfaction with the slow response and lack of technical expertise among enforcement agencies.

Section E: Cybersecurity Practices and Techniques

Although respondents possessed theoretical knowledge of cybersecurity, their personal safety practices were inconsistent. Only a few law students and advocates updated passwords regularly or used multi-factor authentication.

Software updates, antivirus use, and data backups were performed irregularly by most participants. While some advocates working with sensitive client data maintained firewalls and encryption tools, others relied primarily on default device protection.

This revealed a gap between knowledge and actual implementation of cybersecurity techniques among the respondents.

Section F: Awareness Level and Attitude

Most respondents rated their cybersecurity awareness as average or good, reflecting moderate confidence. However, when asked

about the safety of their personal data online, many expressed uncertainties, acknowledging the unpredictable nature of cyber threats. Few respondents had attended formal cybersecurity workshops or training sessions, suggesting a lack of institutional initiatives to build digital literacy even among the legal community. When asked about responsibility for preventing cybercrime, most believed it was a shared responsibility involving individuals, government agencies, internet service providers, and educational institutions.

Respondents strongly recommended that cybersecurity education and practical awareness programs should be incorporated into law curricula and professional training for advocates.

General Observations

Law students and advocates show high awareness of cyber laws but relatively low practical cyber hygiene. Reporting of cybercrimes remains limited due to procedural complexity and a lack of confidence in authorities. There is a need for regular cyber awareness workshops and integration of cybersecurity practices in legal education. Advocates handling client information require specific training on digital confidentiality and data protection. Strengthening coordination between law enforcement and legal professionals can enhance cybercrime reporting and prosecution.

Overall Finding Summary

While legal knowledge of cyber offences among law students and advocates is satisfactory, practical cybersecurity behaviour remains inadequate. There exists a significant gap between awareness and implementation, emphasising the need for skill-based, practice-oriented cyber awareness initiatives in the legal sector.

Conclusion

The study reveals that cybercrime has become an unavoidable reality in today's digital age, affecting individuals, institutions, and even legal professionals. Among the respondents — law students and advocates — awareness of cybercrime as a concept is considerably high, primarily due to academic exposure and professional engagement with technology. However, the research finds a noticeable gap between legal awareness and practical cybersecurity behaviour.

While most respondents understood the broad provisions of the Information Technology Act, 2000, only a few were aware of the procedural aspects of reporting and investigating cyber offences. Many admitted to not following safe online practices such as regularly updating passwords, using multi-factor authentication, or verifying website security.

The findings further reveal that cybercrime incidents are often under-reported due to a lack of awareness about complaint mechanisms, procedural delays, and hesitation caused by privacy or reputational concerns. This under-reporting not only weakens the effectiveness of cyber laws but also emboldens offenders.

Overall, the study concludes that although law students and advocates possess satisfactory legal knowledge about cybercrime, there is an urgent need to enhance their technical literacy and practical cybersecurity skills. Digital safety should not remain only a matter of legal theory but should evolve into a daily professional practice within the legal community.

Suggestions

Integration of Cybersecurity in Legal Education

Law schools should include practical modules on cybersecurity, data protection, and digital forensics in their curriculum. Hands-on sessions on identifying phishing, encryption, and reporting procedures should accompany theoretical teaching.

Workshops and Training for Advocates

Bar councils and law associations should organise periodic workshops on cyber hygiene, safe digital communication, and confidentiality

in electronic records to ensure that practising advocates can protect client data effectively.

Awareness Campaigns and Outreach

Universities, legal aid clinics, and NGOs should collaborate to conduct awareness drives on safe internet usage, emphasising the importance of protecting personal and professional digital identities.

Simplification of Reporting Mechanisms

Cybercrime reporting portals and police units should be made more user-friendly and responsive. Legal professionals can play a key role in guiding victims to the proper channels for redressal.

Development of Institutional Cybersecurity Policies

Law colleges, courts, and law firms should adopt internal cybersecurity policies that include password protocols, secure cloud storage, and regular system audits.

Encouraging Ethical Digital Behaviour

Since cybercrime prevention begins with responsible online conduct, institutions should promote ethical use of social media and professional platforms, discouraging the casual sharing of sensitive data.

Government-Legal Collaboration

Stronger coordination between the judiciary, law enforcement agencies, and cyber experts is essential to create effective investigation frameworks and capacity-building programs for officers and advocates alike.

Continuous Professional Development

Advocates should treat cybersecurity as an ongoing learning process and stay updated on new cyber threats, technologies, and legal developments through continuous legal education (CLE) programs.

Establishment of Campus Cyber Cells

Law colleges may set up student-led cyber awareness cells to assist peers in understanding cyber laws, reporting mechanisms, and digital security practices.

Promotion of Digital Literacy Beyond Legal Circles

As future policymakers and legal educators, law students and advocates can play a key role in spreading cybersecurity awareness among the general public, ensuring safer digital participation across all sections of society.

Final Observation

Cybersecurity today is not just a technological concern but a legal and social responsibility. For the legal community — entrusted with upholding justice and privacy — the challenge lies in translating their legal understanding into active, informed, and ethical digital behaviour. Strengthening cybersecurity awareness among law students and advocates will contribute to building a safer, more resilient, and legally conscious cyberspace.