

ORIGINAL ARTICLE

An Investigation into Cybercrime Awareness and Security Measures

Parul Garg¹, Jyoti Gaur², Ankit Goel³, Rajeev Kumar⁴

How to cite this article:

Garg P., Gaur J., Goel A., et al. An Investigation into Cybercrime Awareness and Security Measures. Indian J Forensic Med Pathol. 2025; 18(2): 206-212.

ABSTRACT

The widespread adaptation of the internet has integrated it into the daily routines of a vast majority of individuals for various transactions. Correspondingly, the user base of the internet has experienced significant growth, paralleled by a rise in cybercrimes. Cybercrime, executed through computers and networks, poses a persistent and escalating threat across professional and personal fields. The arising of the internet has transformed traditional crimes into new forms. This research aims to raise awareness about contemporary cybercrimes and promote heightened cybersecurity measures. Furthermore, it endeavours to examine the levels of computer crime alertness among internet users of various age groups and educational backgrounds. Utilizing a Linear predictive model, this study analyses both objectives. The findings reveal a correlation between respondents' age groups and educational qualifications. Therefore, it is incumbent upon all internet users to remain vigilant regarding cybercrime and cybersecurity, as well as to actively foster awareness among others.

KEYWORDS

• Cybercrime • Crimes • Cyber cell • Security Measures

INTRODUCTION

The rapid expansion of the internet in India has opened new avenues in entertainment, business, education, and various other sectors. As internet usage continues to increase, businesses are transcending geographical boundaries and reaching global customers.

In enterprises, computers have evolved beyond simple information processing tools to become strategic assets. However, this surge in digital connectivity has also led to the rise of modern-day offenses, collectively referred to as cybercrimes, which the Information Technology Act, 2000 was formulated

AUTHOR'S AFFILIATION:

¹ Assistant Professor, Amity University, Noida, Uttar Pradesh, India.

² Assistant Professor, Department of Management Studies, GL Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India.

³ Associate Professor, Maharaja Agrasen Institute of Management Studies, New Delhi, India.

⁴ Professor, Department of Forensic, Department of Forensic Science, Galgotias University, Greater Noida, India.

CORRESPONDING AUTHOR:

Parul Garg, Assistant Professor, Amity University, Noida, Uttar Pradesh, India.

E-mail: parulgarg.mba@gmail.com

➤ Received: 29-06-2024 ➤ Accepted: 17-06-2025



Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution NonCommercial 4.0 License (<http://www.creativecommons.org/licenses/by-nc/4.0/>) which permits non-Commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the Red Flower Publication and Open Access pages (<https://www.rfppl.co.in>)

to address. The accessibility of global information has made it more vulnerable to misuse, resulting in a notable rise in cyber attacks targeting Indian entities. India ranks prominently in several categories of cyber threats. According to Symantec's Internet Security Threat Report, 2018, India ranked third globally in malicious activity, second in malicious code dissemination, fourth in web attacks, and eighth in network attacks.¹⁵ Furthermore, the Indian Computer Emergency Response Team (CERT-In) reported that over 6.07 lakh cyber incidents were recorded in the first six months of 2021. These incidents included phishing, malware attacks, website defacements, cyber surveillance, crypto-extortion, and denial-of-service (DoS) attacks.² The frequency of cybercrime has increased substantially as per a report by The Times of India,⁵ one cybercrime was reported every 10 minutes in 2021, compared to every 12 minutes in 2020. According to the National Crime Records Bureau (NCRB), 65,893 cases of cybercrime were registered in 2022, reflecting a 24.4% increase from the 52,974 cases recorded in 2021. The crime rate per lakh population in this category rose from 3.9 in 2021 to 4.8 in 2022.¹² With internet usage rising, the risks associated with cyber navigation are increasing as well. As of 2023, the number of mobile internet users worldwide reached 5.4 billion, accounting for approximately 67% of the global population.³ The growing online presence, coupled with limited awareness, has

exposed individuals to financial, emotional, and ethical risks. Amidst this alarming landscape, it becomes imperative not only to combat cybercrime but also to prioritize awareness and digital security education among internet users. This study aims to explore critical questions: Are individuals truly aware of the types of cybercrimes they are susceptible to? To what extent does such awareness exist? And, if awareness is lacking, what interventions can be designed to enhance it? Cybercrime involves any illegal activity that uses a computer or network, either as a tool, a target, or both. It includes crimes committed via electronic communication platforms and the internet. While the term "cybercrime" is not explicitly defined in Indian legislation, the Information Technology Act, 2000 serves as the primary legal framework, supplemented by provisions under the Indian Penal Code (IPC) and Special and Local Laws (SLLs). To tackle the growing menace, various cybercrime units have been established across India. Initially, cyber offenses were mostly carried out by individuals or small groups. However, the current landscape includes a wide range of actors, such as professional hackers, organized cybercriminal groups, fraudsters, impostors, minors (aged 6–18), and cyber crooks, making the domain of cybercrime increasingly complex and dynamic. Cybercrimes can be neatly classified into four primary categories, delineated by their specific targets and ensuing repercussions.

Table 1: Classification of Cyber Crimes

Category	Description	Examples
Crimes Targeting Individuals	Cybercrimes aimed at causing harm to specific individuals.	- Digital hacking, cracking - Inbox intimidation -Cyber-stalking, electronic harassment -Slander -Distribution of indecent material -Email & SMS fraud -Credit card fraud & cheating -Child exploitation -Aggressive coercion -Network sabotage -Fabrication -Deceptive email tactics
Crimes Targeting Property	Cyber-attacks that affect an individual's or entity's assets and property.	- Intellectual property infringement - Cyber-squatting - Digital vandalism - Computer system breaches - Virus/ malware attacks - Trojan horses - Cyber trespassing - Internet time theft - Online monetary fraud or theft

Category	Description	Examples
Crimes Targeting Govt. / Firms / Groups	Crimes with the intent to disrupt, damage, or threaten organizations, governments, or groups.	- Cyber terrorism - Unauthorized possession/distribution of information - Software piracy - Domain hijacking - Micro-fraud schemes - Programmed sabotage
Crimes Impacting Society	Offenses that affect society at large either directly or indirectly.	- Dissemination of erotic material - Online betting - Forgery - Sale of illegal items - Phishing - Cyber terrorism

LITERATURE REVIEW

The importance of understanding cyber risks has led to numerous literature reviews in this field.⁴ conducted a thorough review of educational literature on Virtual/cyber danger and cyber insurance, identifying and categorizing 217 papers. The study highlighted open research questions, emphasizing the need for more comprehensive research because of the dynamic nature of cyber risks. Focus on information exchange between public and private sectors was stressed to enhance risk measurement accuracy and aid risk managers in determining appropriate cyber risk levels.¹⁴ Examined the underwriting procedures for cyber insurance and 235 American cyber insurance policies. Findings revealed varied pricing methodologies, ranging from simple flat rate pricing to more complex calculations based on factors like company asset value and industry standards.¹³ explored cyber insurance professional, Perspectives and hurdles regarding data collection and usage, underscoring the need for further data and understanding in this evolving field.¹ Suggested a multifaceted Hawkes framework. to predict cyber attack frequency, leveraging a public dataset on U.S. industry data breaches. They advocated for incorporating external data sources to enhance cyber risk assessment. Systematic reviews by^{8,10,16,9} focused on specific sectors or areas within cybersecurity. ⁸ emphasized the impact of technological advancements and federal policies on cyber risks in healthcare.¹⁰ highlighted unresolved issues in cybersecurity within emergency management, while¹⁶ examined cybersecurity risks in Colleges and universities.⁹ provided insights into IoT cybersecurity, presenting a four-step risk management framework. Several studies emphasized the importance

of datasets in cybersecurity research.⁶ and⁷ stressed the need for comprehensive and up-to-date datasets for effective intrusion detection system development.¹⁷ examined that the cybersecurity research papers to understand data creation, sharing, and utilization trends, highlighting the limited availability of publicly accessible datasets. This review stands out for its comprehensive summary of available datasets related to cyber risk and cybersecurity, serving both the researcher's community and stakeholders in cyber insurance and cybersecurity. By investigating and analysing datasets, this work facilitates efficient progress in cyber risk research and promotes dataset comparability for diverse research areas.

RESEARCH OBJECTIVES

In assessing awareness of cybercrime and security, the study employed the following objectives:

- To investigate the correlation between respondents' education levels and their awareness of cybercrime and digital security.
- To examine the relation between different age group of respondents and their knowledge of cyber-crime and digital security.
- To ascertain the internet usage patterns among respondents.
- To determine the level of knowledge regarding safety measures while using personal computers and the internet in relation to cyber-crimes.

METHODOLOGY

The respondents for this study were selected from the service sector in the NCR, covering a range of professions such as

finance, education, IT services, healthcare, and customer support. A well-organized questionnaire was administered to 156 respondents, all of whom are regular internet users in both their professional and personal lives. It was categorized into four parts: Part A focused on the Population characteristics of the respondents. Part B delved into the internet usage habits of the respondents. Part C addressed the level of awareness concerning cybercrime and security. Part D explored the awareness level regarding safety practices while using PC and the internet. The sample was composed of male and female respondents from various age groups, predominantly falling in the 18 to 45 years range, with a minimum educational qualification of higher secondary or above. Participants were selected through convenience sampling, and only those who voluntarily agreed to participate and provided informed consent were included in the study. This diverse demographic and occupational background ensured a comprehensive understanding of cybercrime awareness and the security measures adopted in the service sector. All responses were collected using a Likert scale of five points (1-Strongly Disagree, 2-Disagree, 3-Neutral, 4-Agree, 5-Strongly Agree) to analyse their awareness of vulnerability to various virtual crimes. Extensive information was gathered from various sources like various books, published domestic and international journals, web pages, etc. To analyse the study findings, Linear Regression technique was employed using SPSS Software version 23. Based on the stated objectives, the study aims to examine the below null hypotheses:

H_{01} : There is no significant relationship between the education level of respondents and their awareness of cyber-crimes.

H_{02} : There is no significant relationship between the various age groups of respondents and their knowledge of cyber-crimes.

Data Analysis and Discussions

A survey involving 156 respondents aimed to assess their Consciousness of cyber-crimes. The outcomes are outlined as follows:

- H_{01} : A correlation was observed between the educational background of respondents and their awareness of cybercrimes.

Table 2: Model Summary and Anova

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.912	.835	.832	.3478

a. *Predictors:* (Constant), Awareness about Cyber Crime, Awareness of Cyber cell

b. *Dependent Variable:* Education level of the respondent

ANOVA ^a						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	83.270	3	27.154	240.587	.000 ^b
	Residual	32.540	143	.235	—	—
	Total	115.810	146	—	—	—

a. *Dependent Variable:* Education level of the respondent

b. *Predictors:* (Constant), Awareness about Cyber Crime, Awareness of Cyber cell

Table 3: Coefficients

Coefficients ^a						
Model		Unstandardized Coefficients	Standardized Coefficients		t	Sig.
1	(Constant)	.352	.281		1.652	.109
	Awareness about Cyper Crime	.544	.094	.555	9.367	.002
	Awareness of Cyber cell	.176	.290	.124	.611	.524

a. *Dependent Variable:* Education level of the respondent

The analysis revealed a strong positive correlation ($R = 0.912$) between the educational background of respondents and their overall awareness of cybercrimes. The regression model proved to be statistically significant ($p = 0.00002$), confirming a reliable predictive relationship. However, upon examining the two components— Awareness of Cyber Crime and Awareness of Cyber Cell only the former was found to be statistically significant ($p = 0.002$). This indicates that individuals with higher educational qualifications tend to have a greater understanding of what constitutes cybercrime, but this does not necessarily translate to increased awareness about specific resources or institutions like cyber cells. Thus, H_{01} is partially accepted, highlighting the need for greater outreach and awareness campaigns around cyber law enforcement mechanisms, especially among educated populations.

- H_{02} : There is no significant relationship

between the various age groups of respondents and their awareness of cybercrimes.

Table 4: Model Summary and Anova

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.901 ^a	.813	.709	.253

a. Predictors: (Constant), Awareness about Cyber Crime, Awareness of Cyber cell

b. Dependent Variable: Age groups of the respondent

ANOVA ^a						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	24.166	3	8.054	5.987	.001 ^b
	Residual	219.740	161	1.335		
	Total	243.806	164			

a. Dependent Variable: the different Age groups for the respondent.

b. Predictors: (Constant), Awareness about Cyber Crime, Awareness of Cyber cell.

Table 5: Coefficients

Coefficients ^a						
Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	
	B	Std. Error				Beta
1	(Constant)	4.752	.481		11.459	.000
	Awareness about Cyber Crime	-1.754	.206	-.812	-8.376	.000
	Awareness of Cyber cell	-.096	.066	-.134	-1.611	.158

a. Dependent Variable: Education level of the respondent

Contrary to the stated null hypothesis, the results demonstrated a strong correlation ($R = 0.901$) between age and awareness of cybercrimes. The regression analysis showed that the model was statistically significant ($p = 0.001$), again validating the strength of the relationship. Similar to H_{01} , only the variable Awareness of Cyber Crime showed significance ($p = 0.00002$), while Awareness of Cyber Cell did not. These results suggest that awareness levels vary across different age groups, with certain demographics possibly more informed or engaged than others. Therefore, H_{02} is also partially accepted, and it underscores the importance of tailoring

cybersecurity education efforts to different age groups to bridge awareness gaps.

c. Awareness of Various Types of Cybercrimes

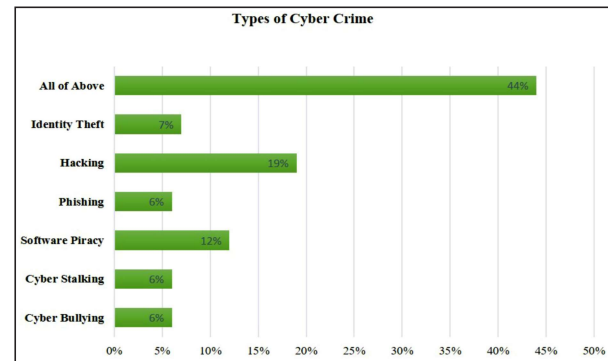


Figure 1: Types of Cyber Crimes in Ordinary Life

As illustrated in Figure 1, the level of specific cybercrime awareness among respondents varied considerably. While 44% of respondents reported being aware of all types of cybercrimes, the rest demonstrated selective or limited knowledge. For instance, 19% were only familiar with hacking, while smaller percentages were aware of phishing, cybers talking, and cyberbullying (6%), software piracy (12%), and identity theft (7%). These statistics indicate that despite general awareness, there is still a lack of deep understanding about the full spectrum of cyber threats. This points to a pressing need for more focused educational efforts on lesser-known but equally harmful cybercrimes.

d. Perceived Vulnerability of Different Sectors to Cybercrime

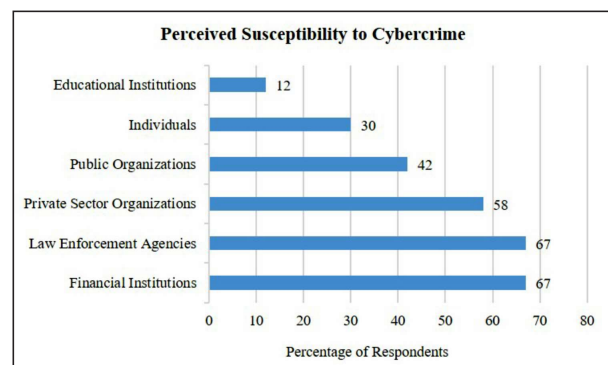


Figure 2: Perceived Susceptibility to Cybercrime

Figure 2 highlights public perception regarding which sectors are most at risk from cybercrime. A significant number of respondents identified financial institutions (67%) and

law enforcement agencies (67%) as being highly susceptible, followed by private sector organizations (58%) and public institutions (42%). Interestingly, only 12% recognized educational institutions as vulnerable, and 30% acknowledged that individuals themselves are also at risk. These findings reveal a nuanced understanding among the population, showing that while institutional threats are well-recognized, the personal risk of cybercrime may be underappreciated. It also suggests a potential blind spot regarding the cybersecurity challenges faced by the education sector.

Conclusion and Recommendations

As internet usage continues to surge, a parallel rise in cyber-crimes is evident. These crimes encompass a wide array of malicious activities occurring in our daily lives. However, there remains a significant lack of awareness among the general populace regarding the breadth of cyber threats. While hacking and viruses are commonly recognized, lesser-known dangers such as phishing, defamation, identity deception, and online stalking often go unnoticed. It is imperative for individuals to equip themselves with knowledge about these internet-related crimes. Findings from our study reveal troubling trends: nearly half of respondents admit to sharing personal information with unfamiliar individuals, and a majority acknowledge frequent damage to their PCs from viruses. Internet users grapple with persistent challenges such as fraud emails, attempts of phishing, and requests for very personal information like mobile numbers, bank account details, and addresses. Basic cyber security awareness is essential for mitigating these risks. Cyber security encompasses a range of technologies and protocols designed to safeguard of computers, networking, and data from unwanted accesses and digital attack orchestrated by cyber criminals. It is incumbent upon each of us to acquaint ourselves with fundamental cyber security measures, including (a) Installing reputable security suites to defend against viruses and worms. (b) Activating the threat detection and response firewall, and Anti-virus software. (c) Employing very strong, alphanumeric passcodes for enhanced security. (d) Restricting the transmission of personal information to trusted sources via phone or secure websites. (e) Exercising caution when

encountering unfamiliar links, downloads, or email attachments. (f) Remaining vigilant against phishing attempts and suspicious Floating ads. (g) Implementing a robust system to ensure the continual updating of antivirus software and computer operating systems. (h) Verifying the authenticity of websites, Uniform Resource Locators, and http addresses to mitigate risks.

Efforts by governmental bodies to regulate cyber-crimes are underway, with initiatives such as the Information Technology (IT) Act of 2000 addressing cyber-related offenses. However, combatting cyber-crime requires collaboration between governments and individuals. Victims of cyber-crimes are encouraged to report incidents to specialized cybercrime units, facilitating collective action against perpetrators. In conclusion, heightened awareness of cyber-crimes and security measures is imperative in today's digital landscape. By empowering individuals with knowledge and fostering collaboration between stakeholders, we can effectively confront the challenges posed by cyber threats.

REFERENCES

1. Bessy-Roland, Y., Boumezoued, A., & Hillairet, C. (2021). Multivariate Hawkes process for cyber insurance. *Annals of Actuarial Science*, 15(1), 14–39. <https://doi.org/10.1017/S1748499520000155>
2. CERT-In. (2021). *Cyber Security Incidents Report*. Retrieved from <https://www.cert-in.org.in>
3. DataReportal. (2023). *Global Digital Overview*. Retrieved from <https://datareportal.com>
4. Eling, M. (2020). Cyber risk research in business and actuarial science. *European Actuarial Journal*, 10(2), 303–333. <https://doi.org/10.1007/s13385-020-00234-0>
5. Johnson, R. (2021). India logs 1 cybercrime every 10 minutes. *The Times of India*. Retrieved from <https://timesofindia.indiatimes.com>
6. Kilincer, I.F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*, 188, 107840. <https://doi.org/10.1016/j.comnet.2021.107840>
7. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2(1), 1–22. <https://doi.org/10.1186/s42400-019-0038-7>

8. Kruse, C.S., Frederick, B., Jacobson, T., & Monticone, D.K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1-10. <https://doi.org/10.3233/THC-161263>
9. Lee, S., Kim, J., Lee, J., Kim, H., Kim, Y., & Kim, H. (2020). IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction. *IEEE Access*, 8, 65520-65529. <https://doi.org/10.1109/ACCESS.2020.2985604>
10. Loukas, G., Gan, D., & Vuong, T. (2013). A review of cyber threats and defence approaches in emergency management. *Future Internet*, 5(2), 205-236. <https://doi.org/10.3390/fi5020205>
11. Mokha, A.J. (2017). A study on awareness of cyber-crime and security. *Research Journal of Humanities and Social Sciences*, 8(4), 459-464. <https://doi.org/10.5958/2321-5828.2017.00067.5>
12. National Crime Records Bureau. (2023). Crime in India 2022. Ministry of Home Affairs, Government of India. Retrieved from <https://ncrb.gov.in>
13. Nurse, J.R.C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2020, June). The data that drives cyber insurance: A study into the underwriting and claims processes. In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-8). IEEE. <https://doi.org/10.1109/CyberSA49311.2020.9139638>
14. Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1), tyz002. <https://doi.org/10.1093/cybsec/tyz002>
15. Symantec. (2018). *Internet Security Threat Report, Volume 23*. Retrieved from <https://www.broadcom.com>
16. Ulven, J.B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39. <https://doi.org/10.3390/fi13020039>
17. Zheng, M., Robbins, H., Chai, Z., Thapa, P., & Moore, T. (2018). Cybersecurity research datasets: Taxonomy and empirical analysis. In 11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18). USENIX Association. <https://www.usenix.org/conference/cset18/presentation/zheng>
18. <http://www.ncrb.nic.in/>