Cybercrime in the Digital Age: Analyzing Causes and Developing Preventive Strategies

Ayati Kothari[1], Himanshu Yadav[2], Akash Chauhan[3]

[1]Student, M.Sc. Cyber Security and Digital Forensics, School of Information Technology, Artificial Intelligence and Cyber Security (SITAICS), Rashtriya Raksha University, Gandhinagar, Gujarat.

[2]Assistant Professor, Department of Forensic Science, School of Allied Health Sciences, Sharda University, Greater Noida, Uttar Pradesh.

[3]Assistant Professor, Department of Forensic Science, College of Paramedical Sciences, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh.

ABSTRACT

Cybercrime is a growing global threat that risks individuals and organizations, affecting their privacy, financial security, and overall well-being. This study explores the factors driving cybercriminal behaviour, sheds light on the vulnerabilities in digital ecosystems, and examines the effectiveness of existing prevention strategies. Through a survey of 200 respondents from a specific region, the research highlights the alarming frequency of fraudulent activities, such as bogus calls, and their significant impact on people's mental health and financial stability. Additionally, it assesses public awareness of cybersecurity threats and the role of legal and ethical measures in tackling cyber risks. This study offers valuable insights into strengthening digital protection and developing better strategies to safeguard individuals and communities from online threats by analyzing current cybersecurity practices.

Keywords: Cybercrime, Victim, Survey, Cybersecurity, Awareness, Prevention.

INTRODUCTION

Cybercrime is a broad term used to describe criminal activities carried out using computers and the internet[1]. It includes a wide range of illicit activities that are intended to cause harm, steal valuable information, or generate financial gain, and can target individuals, businesses, organizations, and governments[2].

Between 30% and 60% of people are thought to have been victims of cybercrime, yet these numbers could not accurately reflect the situation because many crimes go undetected[3]. The fast digitization of financial and personal activities, the growth of internet-connected gadgets, and the always-changing strategies used by cybercriminals are some of the reasons for the pervasiveness of cyber threats[4]. Attack risk increases due to increased opportunities and weaknesses by technological advancements. In today's technology-driven landscape, while digital innovation offers substantial benefits, it has also contributed to a rise in cyber-related crimes, including identity theft, financial fraud, cyber espionage, and digital sabotage[5]. Therefore, individuals and organizations must remain vigilant and adopt proactive measures to safeguard against these threats. These criminals are often difficult to trace and capitalize on weaknesses in digital infrastructure and even human behaviour[2,6].

Cybercrime can cause a lot of trouble, affecting individuals, businesses, and governments. It can result in financial loss, breach of privacy, reputational damage, and even national security breaches[7]. Laws and policies struggle to keep up with the ever-changing technology, making it difficult to combat cybercrime effectively[8].

This study examines cybercrime to provide insights into its mechanisms, trends, and societal impacts. Utilizing a multidisciplinary approach that includes criminology, sociology, computer science, and law, it

aims to identify the motivations behind cybercriminal behaviour, assess vulnerabilities in digital ecosystems, and propose strategies for effective prevention and mitigation. The research seeks to contribute to the efforts to combat cybercrime and protect the integrity of our digital society[9].

Cybercrime Laws in India: A Legal Framework for Digital Security:

- **Information Technology Act, 2000 (Amended 2008)**: This act defines offenses including hacking (Sec. 43), identity theft (Sec. 66C), cyber fraud (Sec. 66D), and cyber terrorism (Sec. 66F)[9].
- **Bharatiya Nyaya Sanhita, 2023**: Criminalizes AI-driven misinformation, cyber fraud, and organized digital crime[9].
- **Bharatiya Nagarik Suraksha Sanhita, 2023**: Introduces digital FIRs, forensic tools, and AI-based investigation mandates[9].
- **Bharatiya Sakshya Adhiniyam, 2023**: Admissibility of digital evidence including logs, emails, and social media records[9].
- **Digital Personal Data Protection Act, 2023**: Mandates consent-based information handling and breach reporting and imposes fines up to ₹250 crore[9].
- **CERT-In Regulations (2022)**: Enforce cyber incident reporting within six hours and sector-specific cybersecurity compliance[9].

METHODOLOGY

A thorough investigation was conducted on Cybercrime in the Digital Age: Analyzing Causes and Developing Preventive Strategies. This inquiry involved a multi-disciplinary approach encompassing various fields such as criminology, psychology, and law.

a) Research Location and Population

The study was conducted in Gandhinagar District, Gujarat, targeting urban, suburban, and rural internet users.

b) Research Design

- Sampling Technique: Stratified Random Sampling
- Sample Size: 200 Participants
- Data collection: Online Questionnaire
- Tool: Google Forms
- Procedure: The questionnaire was distributed through multiple networks to reach a more comprehensive audience. Participants were encouraged to share the survey link with their contacts to expand the survey's reach.

c) Questionnaire Design and Preparation:

The questionnaire was developed following a structured and thematic approach to capture quantitative and perception-based cybercrime insights. It was designed after thoroughly reviewing existing literature on cybercrime behaviour, digital literacy, and cybersecurity strategies. The questionnaire consisted of 25 structured questions, categorized into four sections.

1. Research Objective Alignment

Each section of the questionnaire was aligned with the core objectives of the study:

- To assess cybercrime awareness among users
- To evaluate cyber behaviour and experiences
- To explore perceived causes of cybercrime
- To identify effective preventive strategies

2. Sectional Framework of the Questionnaire

The questionnaire was divided into four key sections:

- Demographics – age, gender, occupation, education, area (urban/rural/suburban), and screen time.
- Cybercrime Awareness and Experience – awareness levels, victimization experience, security habits (e.g., password usage).
- Cybercrime Causes – opinions on factors like unemployment, lack of awareness, or socio-economic conditions.
- Cybercrime Prevention – confidence in cybersecurity laws, use of preventive tools or strategies (MFA, antivirus), and views on education and government responsibility.

3. Question Format

- Close-ended questions (Yes/No, Multiple Choice) for measurable data
- Likert scale and rating questions for capturing confidence levels, perceptions, and beliefs
- Single-select and multi-select options to understand user behaviour patterns

4. Validation and Piloting

The initial draft was reviewed by two experts in cybersecurity and social science research. A pilot test with 10 participants was conducted to ensure:

- Clarity of language
- Logical flow between sections
- Ease of response on digital platforms (Google Forms)

Feedback from the pilot was incorporated to improve clarity, remove redundant items, and ensure the relevance of questions to the research objective.

d) Data Analysis

The collected responses were analyzed using Microsoft Excel sheets. This approach ensured that the data was thoroughly and accurately analyzed.

ETHICAL CONSIDERATIONS

Participants were informed of the study's goals, provided consent, and assured of data confidentiality and voluntary participation.

RESULT

Age:

The majority of respondents **(39.5%)** fell into the 18-24 age range, followed by the 45-54 age range **(37.5%)**, the 25-34 age range **(11%)**, and the 35-44 age range **(9%)**.

Gender:

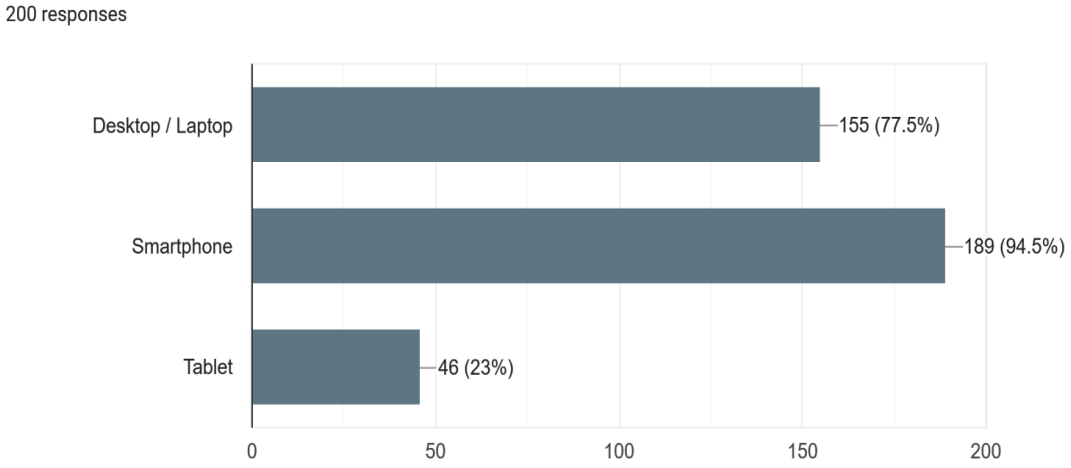
The survey sample comprised **59%** male, **40%** female respondents, and **1%** others.

Geographic distribution:

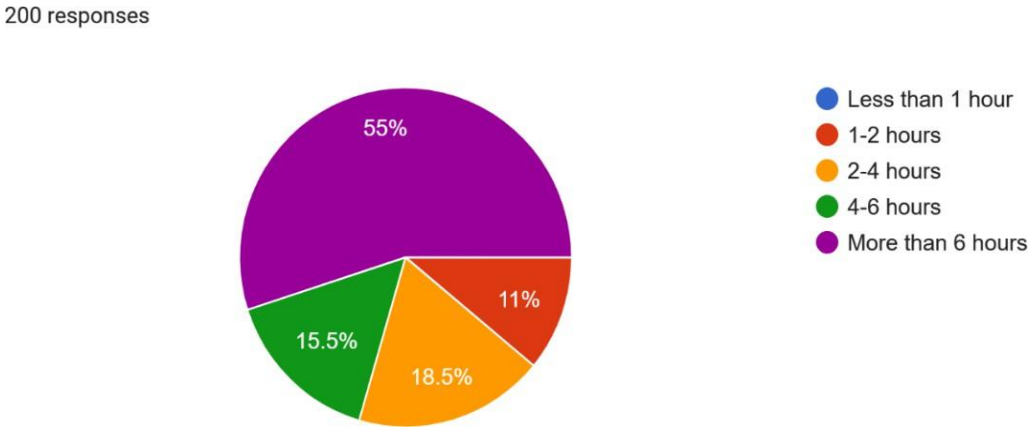
Participants were circulated across various regions, with **67%** from urban areas, **27.5%** from suburban areas, and **5.5%** from rural areas.

OPINION AND PREFERENCES OF PARTICIPANTS:

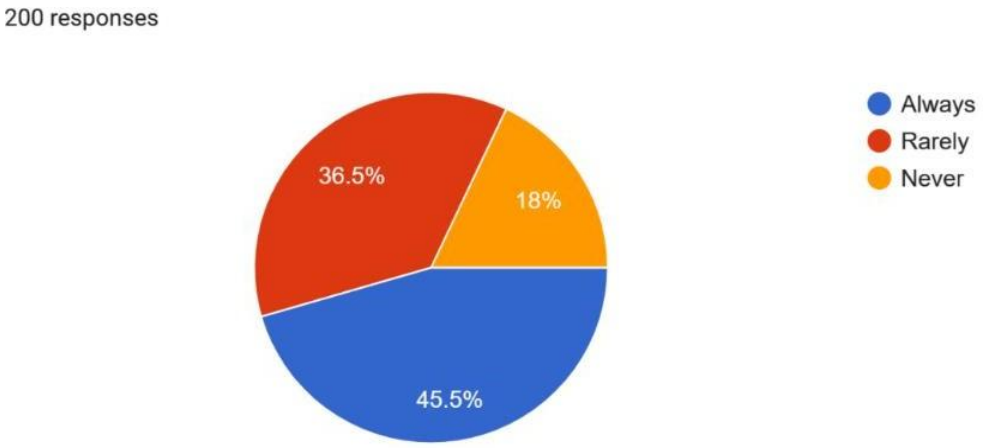
Device Usage



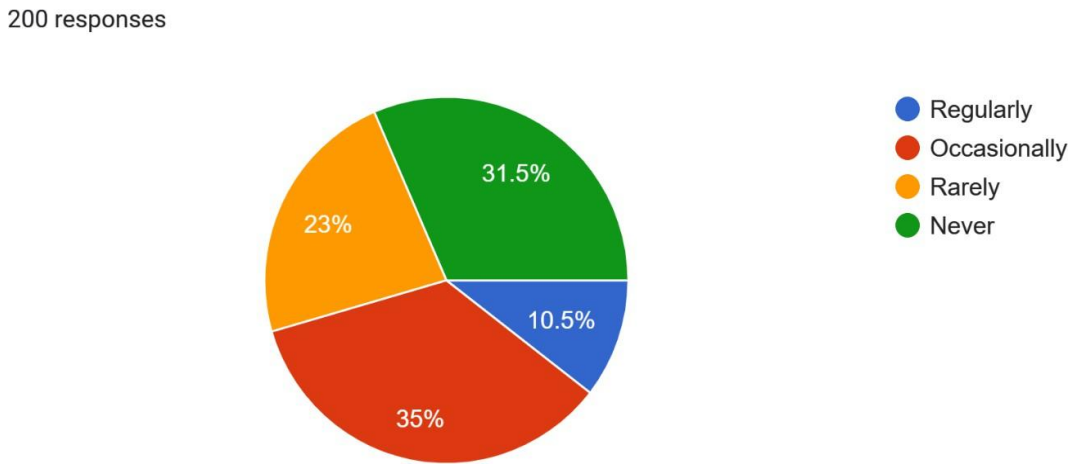
Screen Time



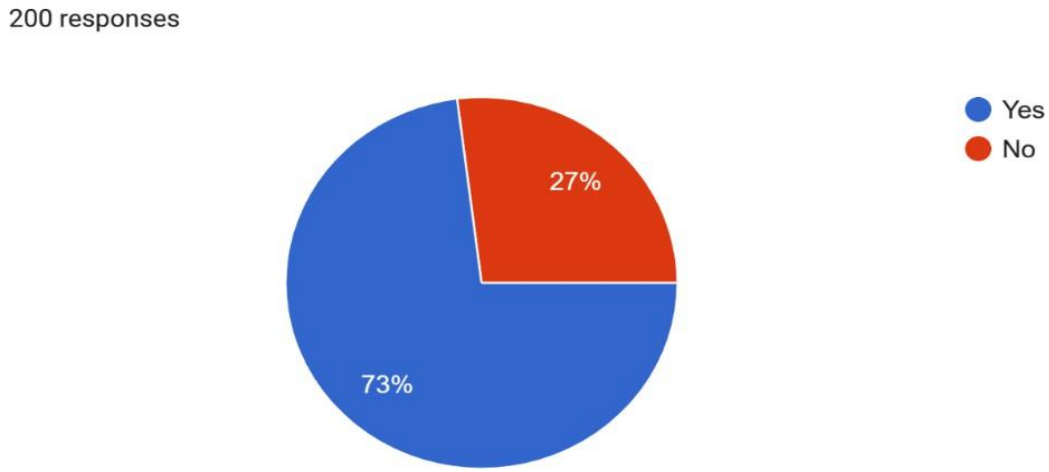
Password change pattern



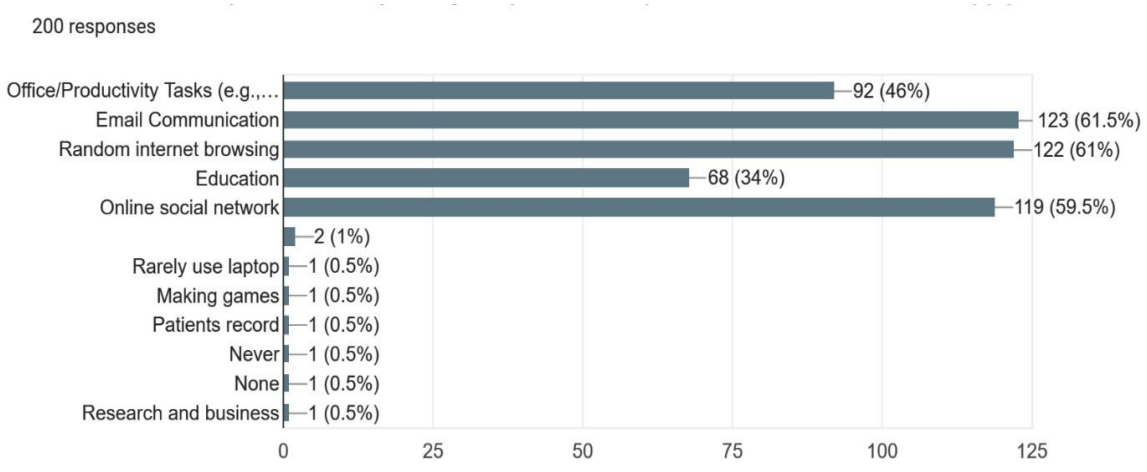
Password usage pattern



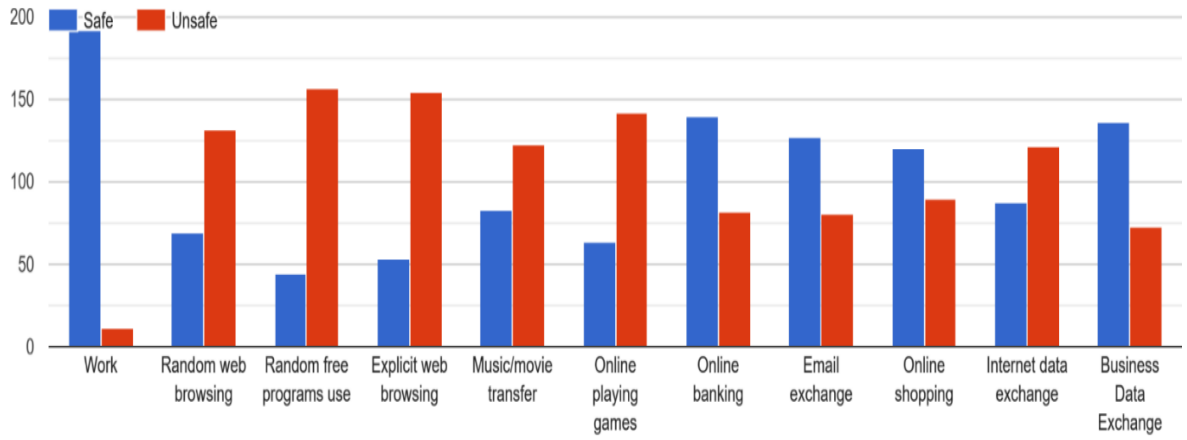
Device synchronization



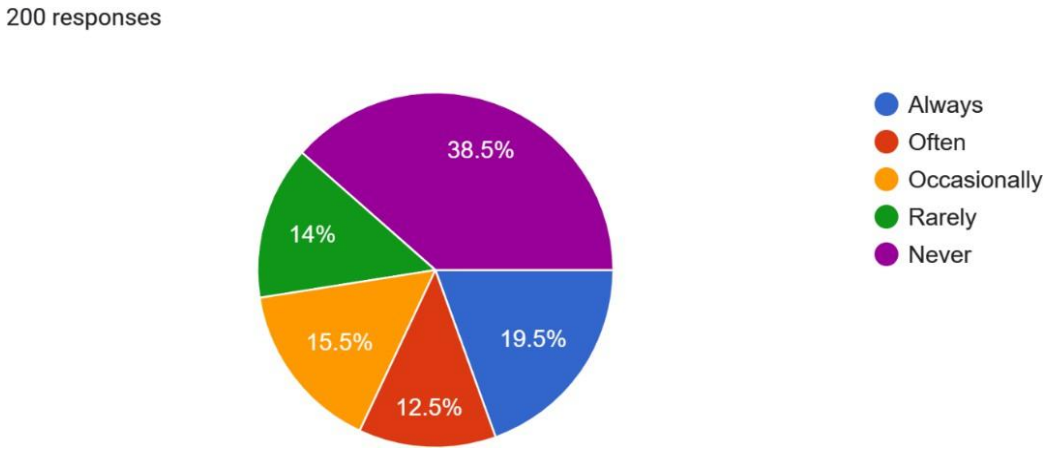
Usage of computers



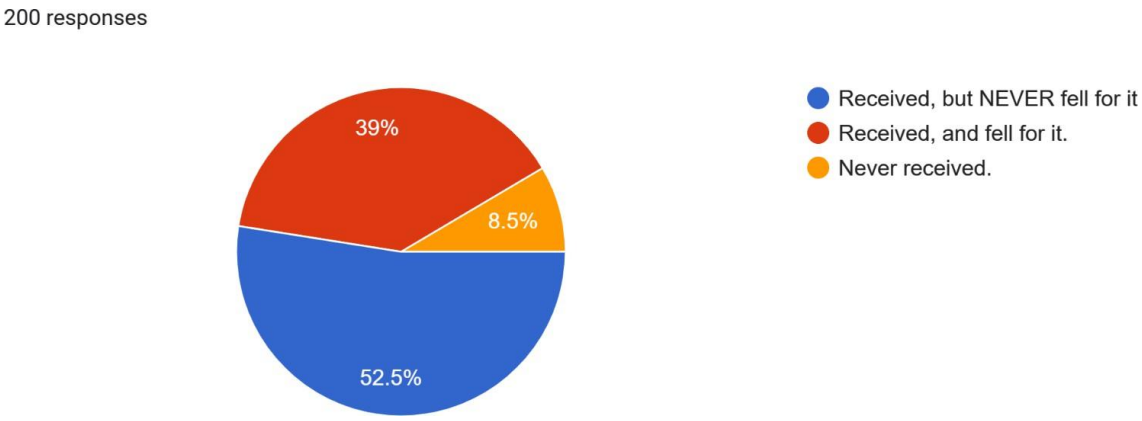
Safe/Unsafe usage



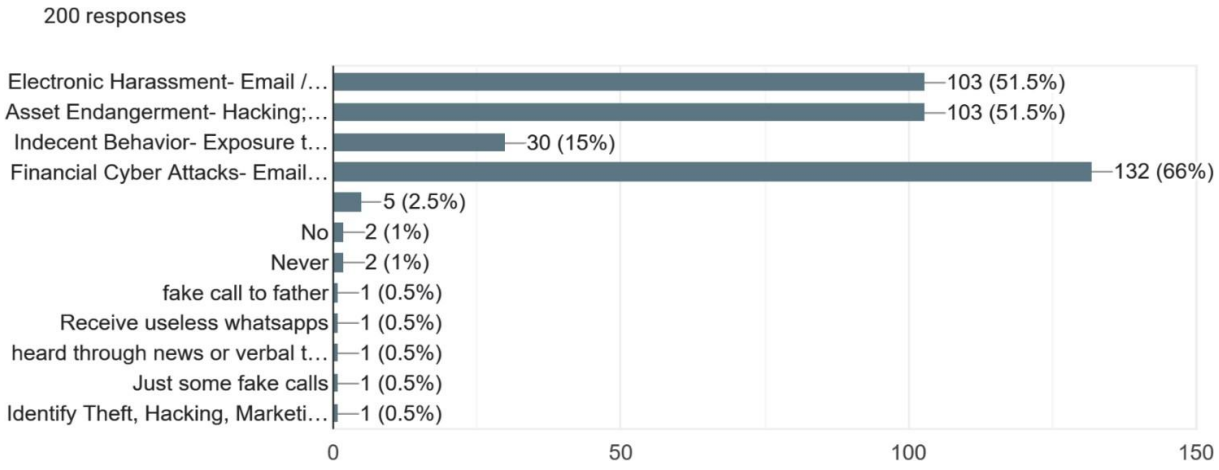
Reading Terms & Conditions



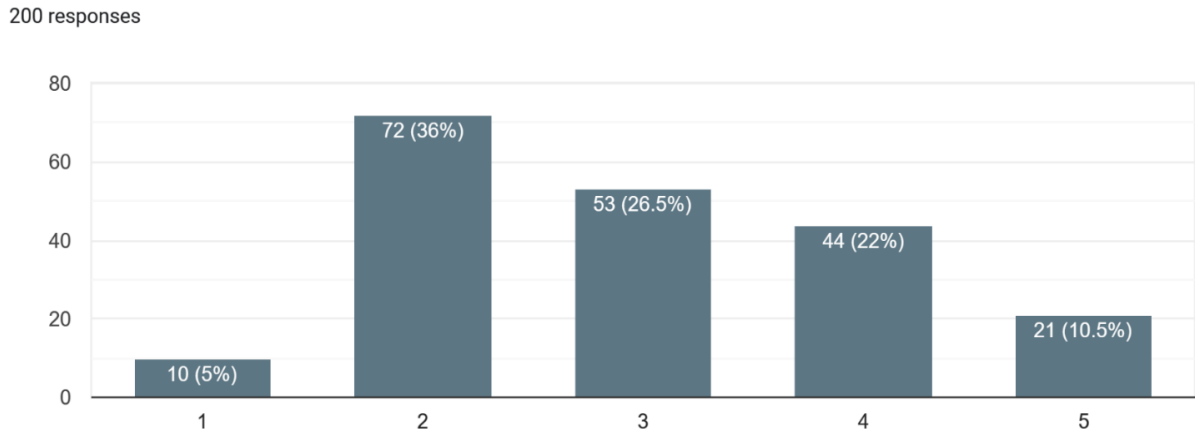
Received a fake/spam call and fell for it



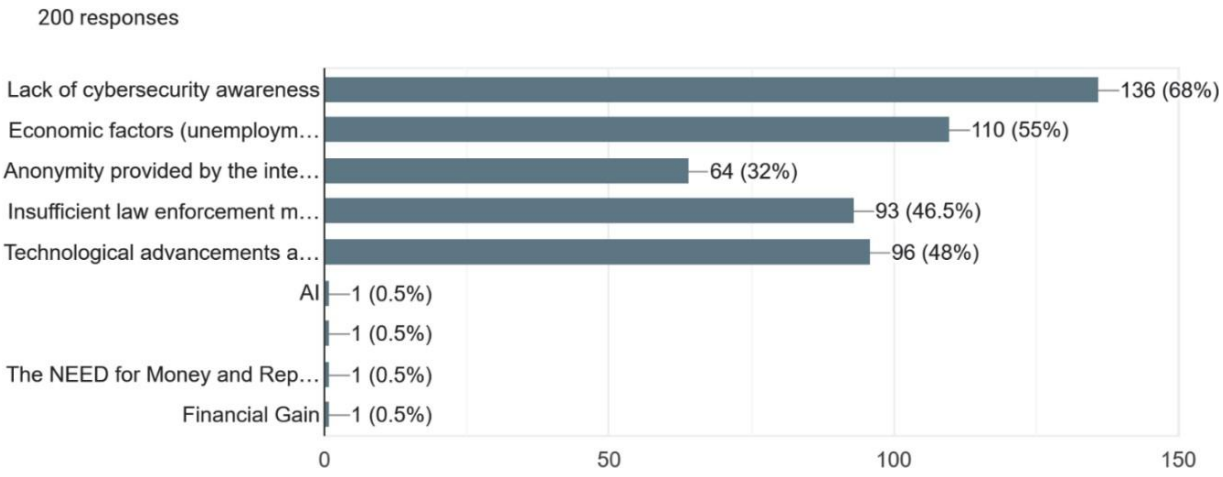
Victim of Cybercrime



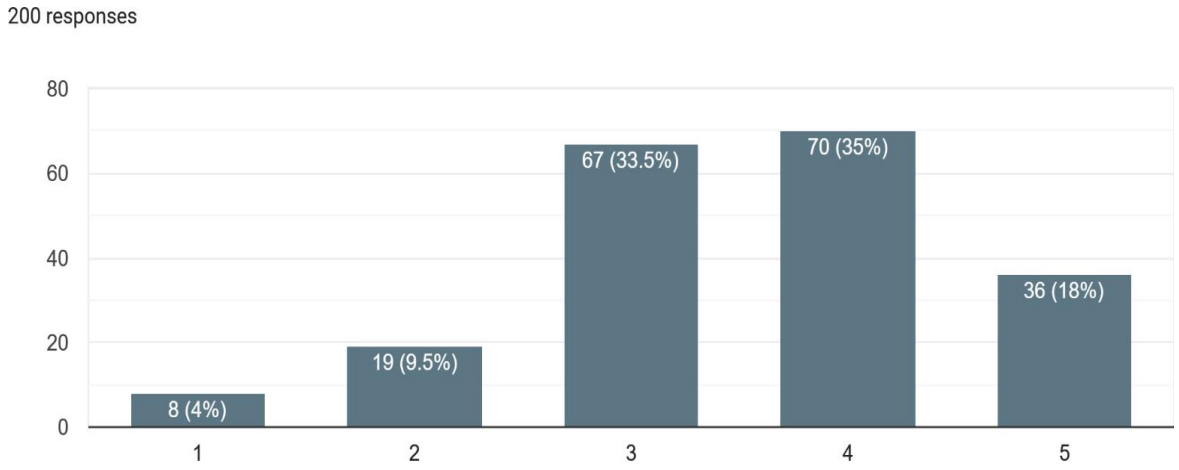
Awareness level about cybercrime



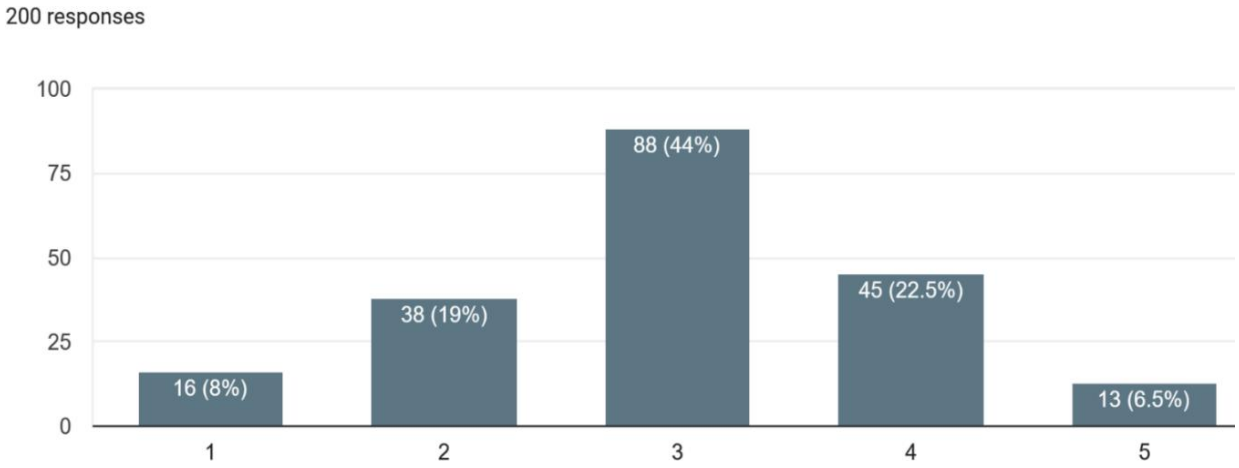
The main motivations behind individuals engaging in cybercriminal activities



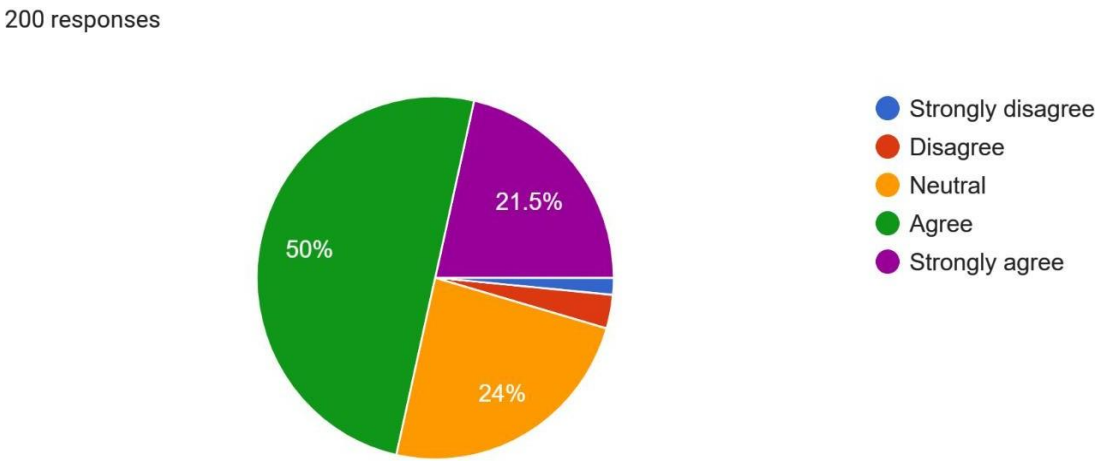
Socio-Economic Inequality



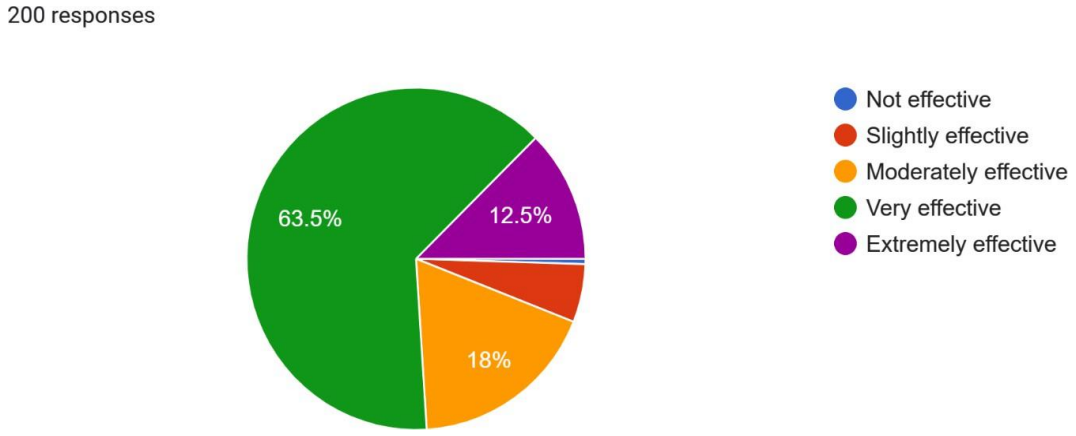
Confidence in the effectiveness of current cybersecurity measures (Moderate)



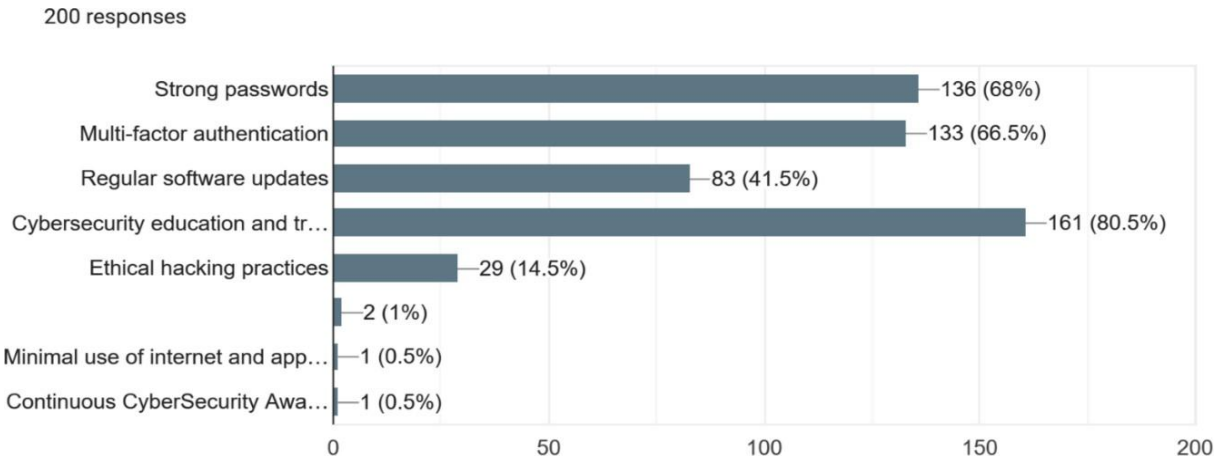
Trust in international law enforcement cooperation



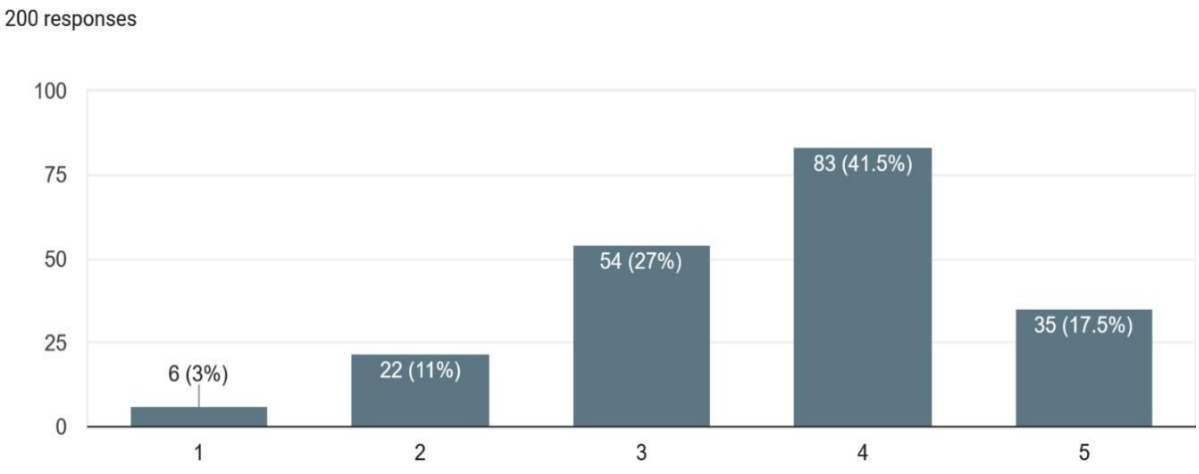
Effectiveness in Cybersecurity Education



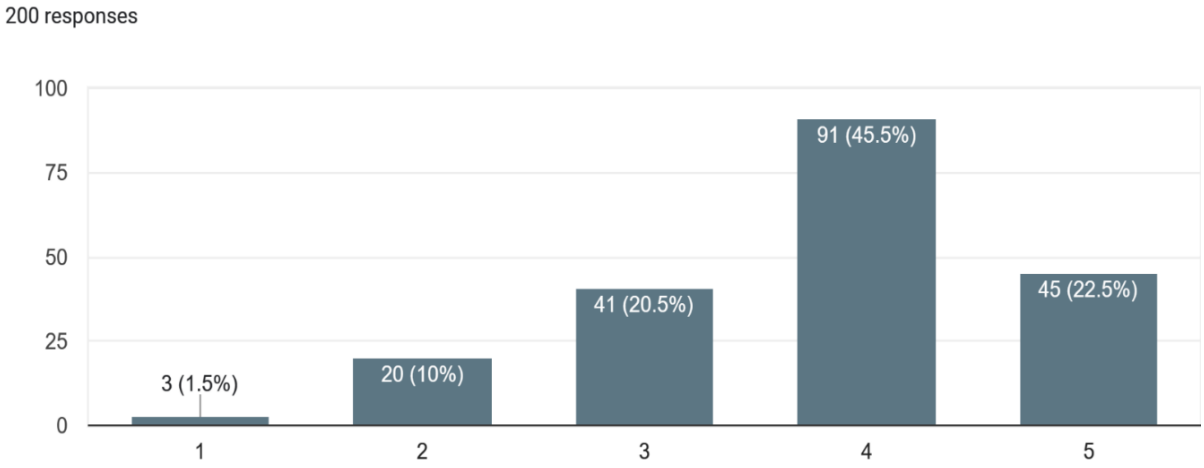
Effective Cybersecurity Measures



Government responsibility in prevention



Fear of cybercrime



DISCUSSION

Our findings suggest that 66% of the respondents have fallen victim to cybercrime, and 36% of them have minimal knowledge about it. Most of the participants believe that the main reason behind cybercrime is the lack of awareness about cybersecurity. Moreover, many respondents think that economic factors can influence people to engage in cybercriminal activities. They also believe that international collaboration and law enforcement efforts are crucial in preventing and combating cybercrime. To prevent cybercrime, the participants suggest that cybersecurity education and training, along with government responsibility, are the most effective measures. According to these findings, the government should take steps to enhance education and training programs in schools, colleges, and workplaces to decrease cybercriminal activities. Additionally, the government should keep cybersecurity as a high priority, implement more cybercrime cell departments in police stations, and introduce stricter laws and penalties to combat cybercrime.

Our research has revealed that economic factors can play a significant role in encouraging people to engage in cybercriminal activities. Additionally, we have found that inadequate law enforcement efforts and limited awareness of cybersecurity can also contribute to the growth of cybercrime. Our findings are consistent with the research conducted by Nir Kshetri (2016), which suggests that low conviction rates in cybercrime cases in India are due to technological illiteracy among law enforcement and a lack of awareness of cybercrime. Moreover, India's low wages and weak formal and informal institutions make it a desirable destination for cybercriminals.

Certainly, the difference in the specific criteria of the research conducted by Nir Kshetri (2016) was that it does not discuss the role of international cooperation in combating cybercrime in India. The objective of this study is to comprehend the underlying reasons, recognize weaknesses, and create strategies to counter them. We only used 200 respondents without the involvement of any cybercrime cell officer or law enforcement personnel. Future research should include a larger number of respondents, as well as officers in this field. One aspect that lacks in-depth analysis is the specific cybersecurity measures and technologies implemented in India, and the paper does not provide a detailed examination of the cultural factors influencing cybersecurity awareness in India.

CONCLUSION

The survey results provided valuable insights into the target audience's opinions, preferences, and behaviours. These findings can be utilized for decision-making processes, refining preventive strategies, and improving the overall offering to better meet the needs and expectations of people.

The survey results provide valuable insights into the respondents' demographics and characteristics.

- Specifically, 39.5% of the participants were aged between 18-24 years, while 37.5% were between 45-54 years.
- Male respondents constituted the majority, accounting for 59% of the total, while female respondents comprised 40%.
- Urban areas were home to most of the respondents (67%), while suburban and rural areas were home to 27.5% and 5.5% of the respondents, respectively.
- It is noteworthy that educational attainment was relatively high, with 60.5% of the respondents holding a bachelor's degree and 32% holding a master's degree.
- Most respondents (38.5%) worked in Business/Management roles, followed by education (21%) and IT/Technology (20%).
- Furthermore, 94.5% of the respondents used smartphones regularly, 77.5% used desktops/laptops, and 23% used tablets.
- More than half of the respondents (55%) spent more than 6 hours daily on electronic devices.

Please find below a summary of the survey results on Cybercrime Awareness and Experience:

- 45.5% of the respondents always use the same password across multiple devices.
- Among all the respondents, 31.5% never change their passwords, while 35% occasionally change them.
- A significant majority of the respondents (73%) synchronize all their electronic devices.
- Regarding computer usage, 59.5% of the respondents regularly use their devices for online social networks, while 61.5% use them for email communication, among others.
- According to the respondents, safe computer use for work, online banking, and business data exchange are considered topmost, while unsafe use, including random free program use, explicit web browsing, and online gaming, is also considered topmost.
- 38.5% of the respondents never go through the terms and conditions of a software/application before signing in.
- The survey found that 52.5% of the respondents received a fake/spam call but did not fall for it, while 39% fell for it.
- The majority of the respondents (66%) have been victims of financial cyberattacks, while 51.5% have experienced both electronic harassment and asset endangerment.
- The survey reveals that 36% of the total respondents have low awareness/knowledge of cybercrime and cybersecurity issues.

According to a survey conducted on the subject of Cybercrime Causes, the following results were obtained:

- The majority of respondents (68%) believe that the primary motivation behind individuals engaging in cybercriminal activities is the lack of cybersecurity awareness. A further 55% of respondents contend that economic factors are a significant contributing factor to these activities.

- Interestingly, a sizeable number of respondents (35%) strongly believe that socio-economic factors, such as income inequality and unemployment, can also motivate individuals to engage in cybercrime.

In the realm of Cybercrime Prevention and Strategies, a survey was conducted among the respondents to gauge their confidence level in the current cybersecurity measures.

- According to the survey, 44% of the respondents expressed moderate confidence in the efficacy of the current cybersecurity measures.
- 50% of the respondents believed that international collaboration and law enforcement efforts are essential in preventing and combating cybercrime.
- The survey revealed that the majority of the respondents, i.e., 63.5%, felt that cybersecurity education programs could significantly reduce the risk of individuals and organizations falling victim to cybercrime.
- When asked about the most effective measures to prevent cybercrime, the respondents opined that cybersecurity education and training were the most effective, followed by strong passwords (68%) and multi-factor authentication (66.5%).
- Another interesting survey finding was that 41.5% of the respondents believed that the government has a considerable responsibility in preventing cybercrime.
- Finally, the survey showed that 45.5% of the respondents have a high fear of cybercrime.

Table 1: Demographic distribution of respondents (N = 200)

Attribute	**Category**	**Percentage (%)**
Age	18-24 years	39.5
	25-34 years	11.0
	35-44 years	9.0
	45-54 years	37.5
Gender	Male	59.0
	Female	40.0
	Others	1.0
Area	Urban	67.0
	Suburban	27.5
	Rural	5.5
Device Usage	Smartphone	94.5
	Desktop/Laptop	77.5
	Tablet	23.0
Screen Time	>6 hours/day	55.0

Table 2: Cyber Awareness and Usage Behaviour

Indicator	Response Category	Percentage (%)
Password usage pattern	Always the same password on multiple devices	45.5
	Never change passwords	31.5
	Occasionally change passwords	35.0
Device synchronization	Synchronize all devices	73.0
Reading Terms & Conditions	Never read the terms and conditions	38.5
Received a fake/spam call	Yes	91.5
Fell for a spam call	Yes	39.0
Victim of financial cyberattack	Yes	66.0
Victim of harassment or asset endangerment	Yes	51.5
Awareness level about cybercrime	Low	36.0

Table 3: Perceived Causes of Cybercrime

Lack of cybersecurity awareness	68.0
Economic factors (unemployment, etc.)	55.0
Socio-economic inequality	Moderate-High (rating scale)

Table 4: Trust in Cybersecurity and Preventive Measures

Measure/Opinion	Agreement (%)
Confidence in current cybersecurity (Moderate)	44.0
Trust in international law enforcement cooperation	50.0
Cybersecurity education effectiveness	63.5
Strong passwords as a prevention strategy	68.0
Multi-factor authentication	66.5
The government has a major responsibility	41.5
High fear of cybercrime	45.5

REFERENCES

1. Lapuh Bele, J., Dimc, M., Rozman, D. & Sladoje Jemec, A. *Raising Awareness of Cybercrime-The Use of Education as a Means of Prevention and Protection*. https://www.researchgate.net/publication/291317388 (2014).
2. Park, H., Cho, S. & Kwon, H.-C. *Cyber Forensics Ontology for Cyber Criminal Investigation*. vol. 8 http://www.netan.go. (2009).
3. Datta, P., Panda, S. N., Tanwar, S. & Kaushal, R. K. A Technical Review Report on Cyber Crimes in India. in *2020 International Conference on Emerging Smart Computing and Informatics, ESCI 2020* 269–275 (Institute of Electrical and Electronics Engineers Inc., 2020). doi:10.1109/ESCI48226.2020.9167567.
4. PREVENTION OF COMPUTER CRIME THROUGH KNOWLEDGE OF THE CONCEPT OF CYBER SECURITY.
5. Mohd Ali, M. Determinants of Preventing Cyber Crime: a Survey Research. *International Journal of Management Science and Business Administration* **2**, 16–24 (2015).
6. Gordon, S. & Ford, R. On the definition and classification of cybercrime. in *Journal in Computer Virology* vol. 2 13–20 (2006).
7. Umar, I. N. & Ghazal, S. Computer-supported collaborative learning: Factors affecting students' participation and interaction in a knowledge building environment. *WSEAS Transactions on Environment and Development* **17**, 546–555 (2021).
8. Bhagwani, V. & Balasinorwala, S. CYBER SECURITY. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT* **07**, (2023).
9. Combating Cybercrime: A Study on Problems, Preventions and Cyber Laws of India. *European Economic Letters* (2024) doi:10.52783/eel.v14i1.1220.