ANUSHKA SRIVASTAVA

DR. ARVIND KUMAR SINGH

BBA L.L.B (A8121521012)

17TH FEBRUARY, 2024

CYBERCRIME AND ITS IMPACT ON SOCIETY IN INDIA

ABSTRACT:

Cybercrime has emerged as a threat that is evolving rapidly and giving rise to various challenges to individuals, organizations, and societies across the world. This abstract presents an overview of the multifarious nature of cybercrime and its impact on society in India. The augmentation of new technologies has brought great convenience to individuals but has also created new ways for criminal exploitation. The cybercriminals use numerous techniques to permeate the systems, steal hypersensitive data, and rattle the critical foundation of the organizations which results in an abundance of financial loss, reputational damage, and threat to the privacy of the individuals. This abstract examines the various forms of cybercrime and delves into the scope of cyber threats in India, highlighting the challenges it presents to the government and law enforcement. Teenagers, the elderly, even celebrities, and marginalized communities, are among the vulnerable groups that experience cybercrime exploitation. Governments, corporations, and members of civil society have stepped up their efforts to combat cybercrime through laws, technological advancements, and capacity-building programs in response to the growing threat in the current scenario in India.

KEYWORDS:

Cybercriminals, Cybercrime, Threats, India, Society, Attacks, Cybersecurity, Technology, Victims, Internet, Cyber laws

OBJECTIVES:

1. To provide a comprehensive study of the emerging cyber threats in society.
2. To evaluate the effectiveness of existing cybersecurity strategies and policies in mitigating cyber threats and enhancing societal resilience.
3. To delve into the impact of cybercrime on the society.
4. To make suggestions for improving social, organizational, and individual cybersecurity resilience.

INTRODUCTION:

In the current modern world, where the fabric of society is intricately woven with technology, the concept of cybersecurity has become crucial. The emergence of new technologies is making the lives of people comfortable and convenient but simultaneously it is also giving rise to numerous cyber threats in the current society. Cybersecurity has become a fundamental line of defense against a variety of criminals that creep into the virtual world. Cybercrime is defined as any criminal activity that takes place on or over the medium of computers, the internet, and other technologies and harms individuals and organizations. It is a medium which is infinite and immeasurable. Some of the newly emerged cybercrimes in the current scenario are, cyber-stalking, hacking, cyber-pornography, cyber-defamation, e-mail bombing, identity theft, credit card fraud, unauthorized access, computer vandalism, etc.

The effects of cybersecurity breaches are felt throughout society as a whole, not just on individual computers or business networks. Cyber threats have far-reaching implications that affect all sectors of the economy, including financial organizations, healthcare providers, government agencies, and educational institutions. High-profile cyberattacks in recent years have demonstrated how vulnerable even the most robust systems can be, impairing public confidence and causing key services to be disrupted and sensitive data to be compromised. Cybersecurity breaches have significant social and psychological consequences such as Identity theft, fraud, and harassment can occur when personal information, including social security numbers, credit card numbers, and medical records, is stolen. Cybercrime victims may feel violated, anxious, or helpless, which weakens their sense of security in the digital world. Furthermore, there is a strong risk to national security and public safety from cyberattacks that target key infrastructure, including power grids, transportation networks, and healthcare institutions.

Through the prioritization of cybersecurity knowledge, the implementation of strong defense mechanisms, and the promotion of a cyber-hygiene culture, society can effectively reduce the impact of cyberattacks and protect the digital infrastructure that is essential to contemporary civilization. In addition to endangering personal security and privacy, ignoring cybersecurity threats erodes the confidence and trust that underpin the digital economy and society. To achieve a safer, more secure digital future, cybersecurity must thus continue to be at the forefront of public conversation and group efforts.

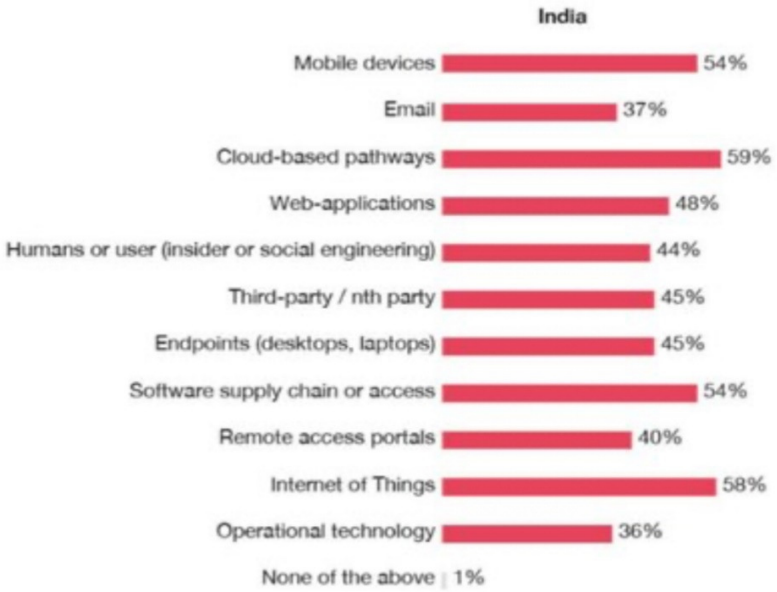
CLASSIFICATION OF CYBERCRIME:

Cybercrime is classified into various types based on the nature of the offense and targets. Here are some classifications of cybercrime-

1. **HACKING**:

It refers to the behavior of an intruder who accesses your computer's data or network without your permission to cause damage, interfere with operations, or steal data. It involves exploiting vulnerabilities in software, hardware, or human behavior to gain access to information or resources that are inaccessible to the hacker. Serious consequences of an attack can include financial loss, data breaches, invasion of privacy, and damage to the company's reputation or operations. Therefore, preventing and controlling hacker attacks is an important part of cybersecurity for individuals, companies, and governments. Conversely, someone's security can be hacked, and their phone numbers, credit cards, addresses, online passwords, etc. It is also known as the theft of personal information.

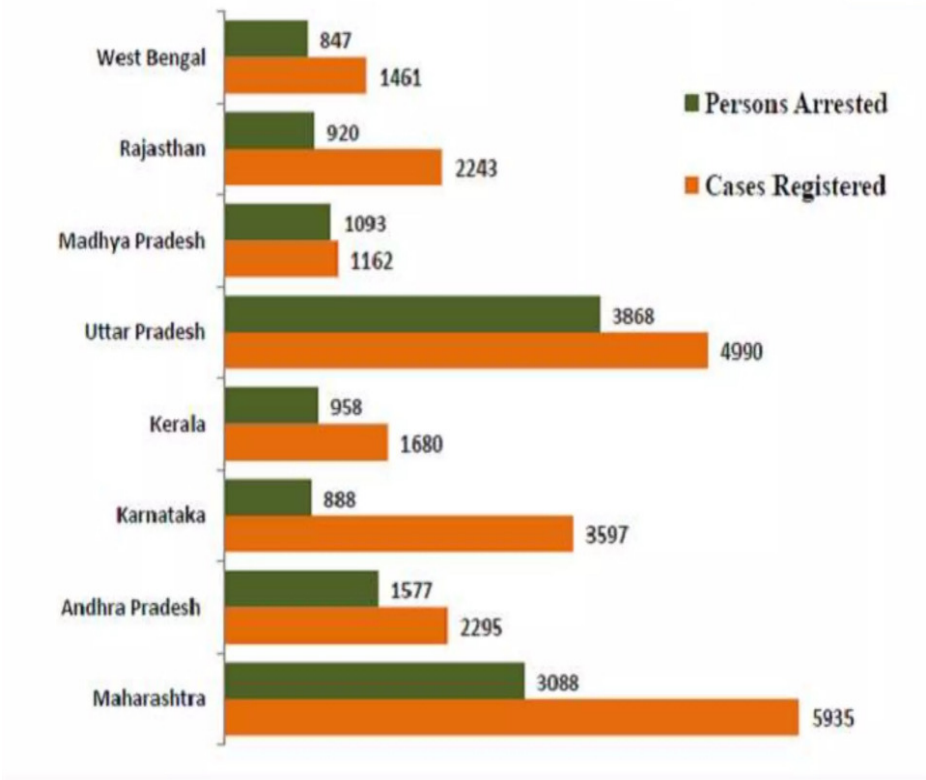
Here's the percentage data of people hacked through various online platforms in the year 2023.



2. **CYBER-FRAUD**:

It refers to fraud committed over the internet or using digital technology to deceive the victim for financial or other benefits. It covers a wide range of crimes, often involving fraud, manipulation, or exploitation of people, organizations, or processes. Some common types of cyber fraud include phishing, identity theft, online scams, credit card fraud, account takeover, etc. The fact that online fraud poses a major risk to individuals, businesses, and society underscores the importance of cybersecurity measures, know-how, and defensive anti-fraud measures in the digital economy.

Below is a statistic that shows the number of cases registered in the leading states and the people arrested for cyber fraud in the year 2023.



3. **CYBER-PORNOGRAPHY**:

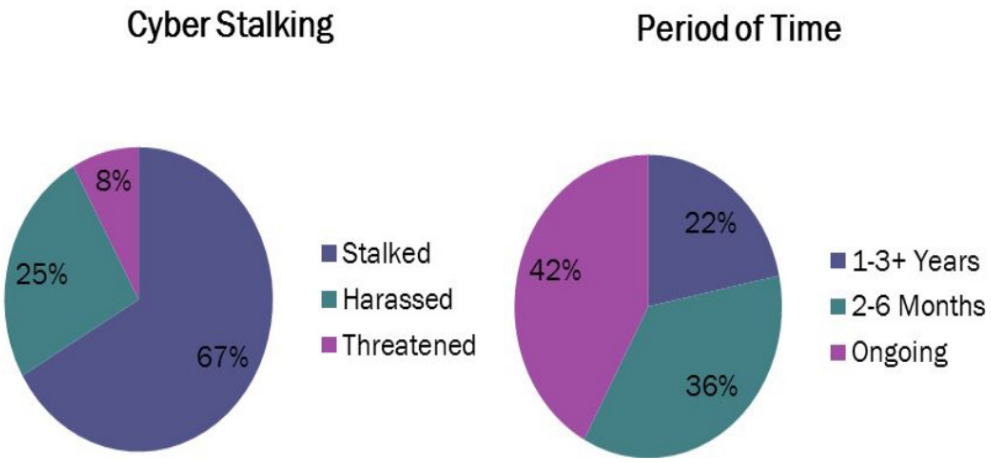
It is also known as Internet nudity or Internet nudity, which refers to the posting, use, or creation of sexual content through platforms and on the Internet. Solving the crucial problem of viewing online pornography requires a multifaceted approach that includes education, prevention, control, management, psychological support, and laughter. There are currently more than 420 million private pages. Child porn is very popular on the internet. It brings shame to the future of children and describes and distributes them negatively on social networking sites. Therefore, in a country like India, where there are a large number of women and girls in the population, the laws on this subject must be strictly followed and at the same time adapted to social and cultural differences.

Below is a table that represents the leading states and the number of cyberpornography cases committed in the year 2023.

Karnataka	235
Madhya Pradesh	137
Delhi	116
Chhattisgarh	112
Rajasthan	106
Kerala	104
Andhra Pradesh	99
Maharashtra	54
Odisha	47
Uttar Pradesh	38
Gujarat	32
Assam	24
Tamil Nadu	19
Punjab	15
Jharkhand	6
Telangana	6
Haryana	5
Andaman and Nicobar	3
Himachal Pradesh	2
Uttarakhand	2
West Bengal	1
Goa	1
Meghalaya	1

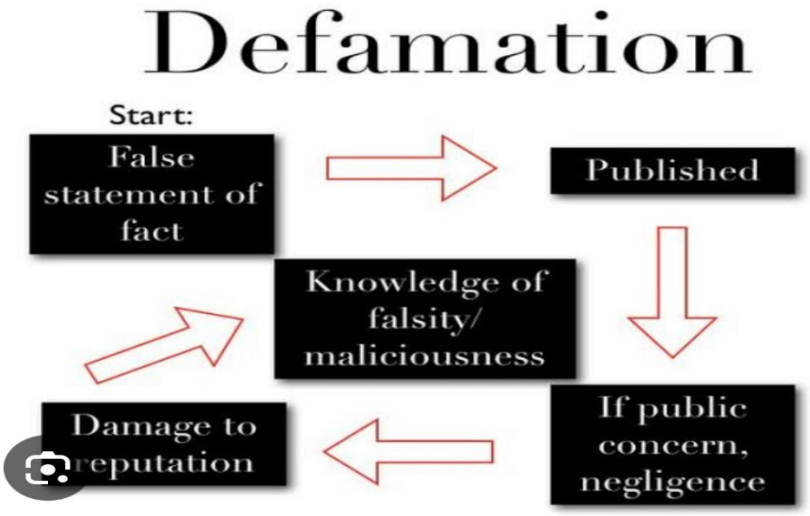
4. **CYBERSTALKING**:

Cyberstalking is the use of electronic communications or digital technology to harass, intimidate, stalk, or threaten someone, often persistently and destructively. Engages in inappropriate and repetitive online chats that create fear, anxiety, or distress in the victim. Most victims are women pursued by men and children pursued by adult predators. Cyberstalking can have serious consequences for victims, including psychological harm, isolation, loss of privacy, financial loss, and security risks. People need to take steps to protect their online privacy and security, such as using strong passwords, protecting privacy settings, being careful about sharing their personal information online, and reporting cyber incidents to authorities or online platforms. Additionally, raising awareness about cyberstalking and providing support services to victims is crucial in combating this type of online harassment.



5. CYBER DEFAMATION:

It is also known as online defamation or online defamation, which refers to inappropriate and malicious behavior towards individuals or organizations through digital communications such as social media, websites, forums, blogs, or online comments. These statements are called libel and can harm the victim's reputation, credibility, or livelihood. The problem that posting negative comments on the internet causes people is huge and cannot be corrected because the information is broadcast to the whole world. Online fraud affects the health of not only the victim but also the entire society. To prevent online fraud, individuals and organizations can take important steps such as monitoring their online presence, responding quickly to false or negative messages, providing legal advice when necessary, and promoting good and accurate information about themselves online. Additionally, promoting digital awareness and online behavior can help prevent the spread of negative content and reduce its impact.



CYBER LAWS IN INDIA:

To combat the threat posed by cybercriminals, the government created the Information Technology Act of 2000, the primary goal of which is to provide an enabling environment for successful internet use as well as to report cybercrime in India. The main goal of this Act is to provide eCommerce with trustworthy legal protection by making it easier to register real-time information with the government. However, as cyber attackers became more cunning, coupled with the human predisposition to manipulate technology, several adjustments were made.

The IT Act is the most important because it instructs all Indian laws to strictly control cybercrimes:

Section 43 - This section applies to those who damage the computer without permission from the owner. In this case, the owner is entitled to full compensation for all losses.

Section 66 - This section applies if a person is found to have done something dishonestly or fraudulently within section 43. In this case, the penalty may be imprisonment for up to three years or a judicial fine of up to one thousand liras. 5 Lakhs.

Section 66B - Includes penalties for the offense of obtaining stolen communications equipment or computers by fraud, including a three-year prison sentence. Depending on its severity, the action may also attract a fine of Rs. 100,000.

Section 66C – This section focuses on identity theft, including forging digital signatures, and stealing passwords and other unique identifiers. If found guilty, the penalty for the crime will be three years imprisonment and a fine of Rs 1 lakh.

Section 66 D - This section was added to punish fraudsters who impersonate others using computer technology. Theft and similar crimes are committed via the Internet or electronic media.

In addition to criminal penalties, the Information Technology Law also allows an agent of the central government to restrict public access to information or computer resources if it deems it necessary in the interests of the country. It can in. fluence, make decisions and monitor this information.

LITERATURE REVIEW:

Cybercrime is defined as a "crime committed with criminal intent against an individual or group for the purpose of defaming the victim or causing direct or indirect physical or mental harm to the victim" by Debarati Halder and K. Jaishankar. Use of modern means of communication such as mobile phones and the Internet (chat rooms, emails, newsletters, cybercrime, and its distribution). The Oxford Dictionary defines cybercrime as a criminal activity using a computer or the internet. Criminal or other unlawful use of electronic communications or information, including by any device, internet, or any combination, is considered a cybercrime. It includes everything from power outages to denial-of-service attacks and generally refers to crimes that use a computer or computer as a tool, target, or crime scene. It can also refer to more serious crimes where the crimes are committed through the use of computers or the internet. Cybercriminals anywhere can disrupt trains, jam planes with false signals, and leak important military information.

RESEARCH METHODOLOGY:

To gain a better understanding of how much information people have regarding cybercrime in India, this study relies on surveys as its primary research method. This approach allows for the efficient collection of data from a diverse population, ensuring that the sample accurately reflects India's cybercrime demographics. By following this process, we can provide a clear and detailed overview of the research used to gather information regarding cybercrime investigations, ensuring the research is open and reliable. The survey shows people's knowledge of Cybercrime, how they handle the case of security breaches, laws regarding cybercrime, etc. This survey helped us better understand the people and their understanding of cybercrime. By exploring people's views regarding cybercrime, the research aims to provide better alternatives to society to combat the threats of cybercrime in today's world.

DATA ANALYSIS:

Analyzing the impact of cybercrime on Indian society requires a multifaceted approach that takes into account various factors such as the type of cybercrime, prevalence, financial impact, social impact energy, and prevention and mitigation**.** Here's the structure of the data analysis for this research paper-

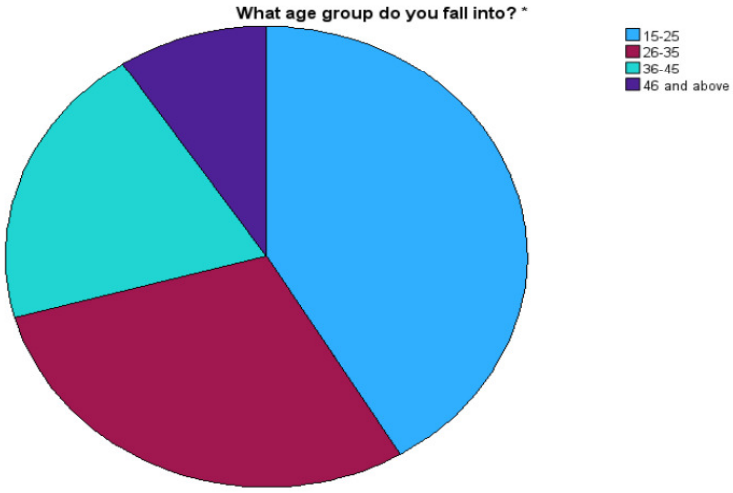
- **Understand the types and common types of cybercrime**: Cyber fraud, theft Hacking, hacking, cyberbullying, etc. present in India. Publish information about different types of cybercrimes such as. Research trends over time to see whether specific types of cybercrime are increasing or decreasing. Indicate hotspots or areas of cybercrime.
- **Social impact assessment**: Look at the literature on the social impacts of cybercrime, such as psychological harm to victims, destruction of trust in online platforms, and damage to personal and professional life. Publish

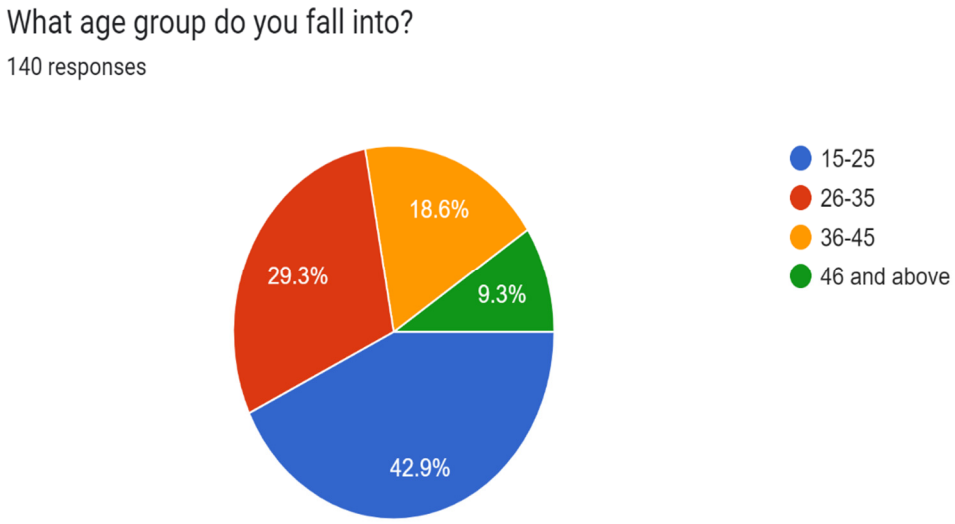
scientific data or positive responses to understand the emotional and psychological impact of cybercrime on individuals and communities.

- **Research on Sociodemographic Factors**: Examine whether there are specific factors (such as age, gender, education, or income) that affect health and are related to vulnerability to cybercrime or its effects.
- **See legal and regulatory response**: Indicate barriers to reporting cybercrime, such as fear of retaliation or lack of knowledge about reporting procedures.
- **Policy implications and recommendations**: Based on the analysis of the results, recommendations are given to policymakers, law enforcement, and other stakeholders to strengthen cybersecurity measures and reduce the impact of cybercrimes on Indian society. Advocate for investment in cybersecurity infrastructure, regulatory reform, and coordinated efforts to address cyber threats.

DATA INTERPRETATION –

What age group do you fall into? *					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	15-25	58	41.4	41.4	41.4
	26-35	41	29.3	29.3	70.7
	36-45	28	20.0	20.0	90.7
	46 and above	13	9.3	9.3	100.0
	Total	140	100.0	100.0	



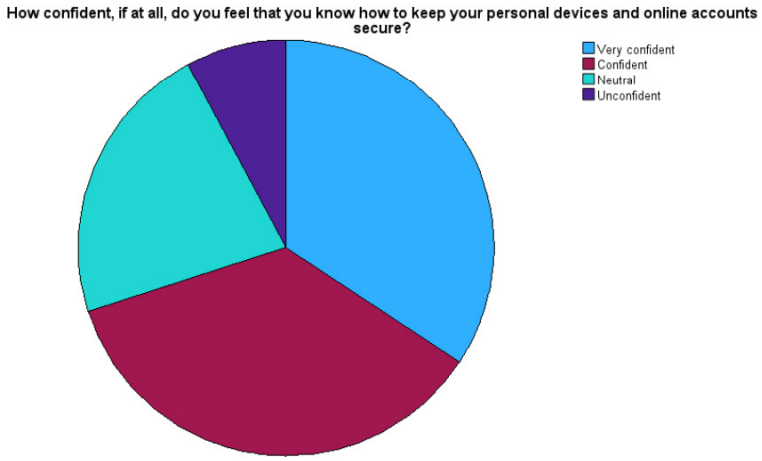


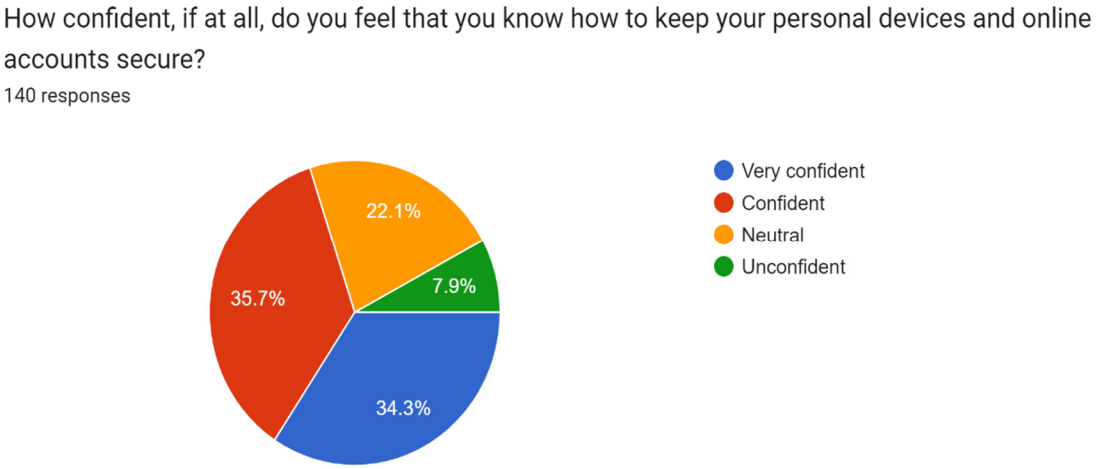
Interpretation:

This pie chart shows the age groups of the people who gave their responses to the questionnaire on cybercrime. Majorly, 42.9% of the people, who gave responses are aged between 15 to 25 years. Then 29.3% of people who answered the questionnaire were aged between 26 to 35 years, 18.6% people were aged between 36 to 45 years, and 9.3% of people who answered were aged 46 years and above. Thus it shows that the young generation is mostly interested and involved in the questionnaire and equally enthusiastic to participate in surveys and questionnaires.

How confident, if at all, do you feel that you know how to keep your personal devices and online accounts secure?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very confident	48	34.3	34.3	34.3
	Confident	50	35.7	35.7	70.0
	Neutral	31	22.1	22.1	92.1
	Unconfident	11	7.9	7.9	100.0
	Total	140	100.0	100.0	



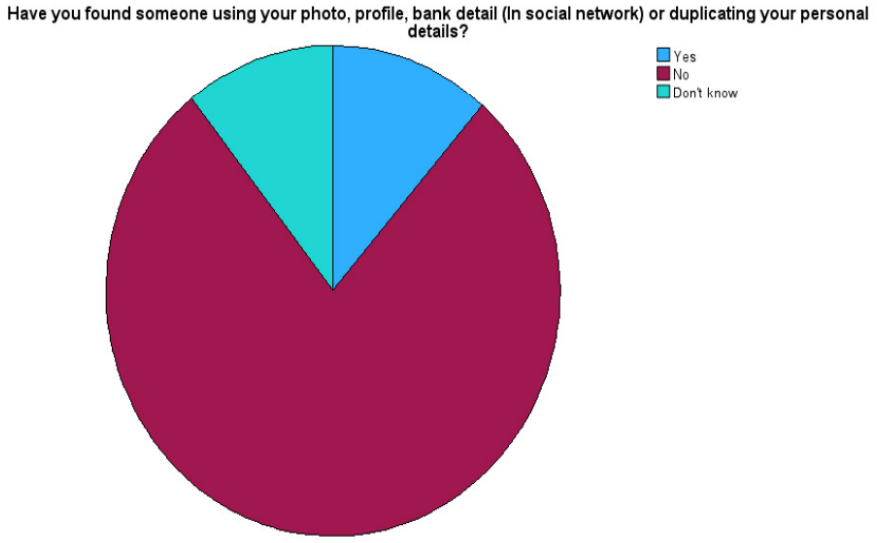


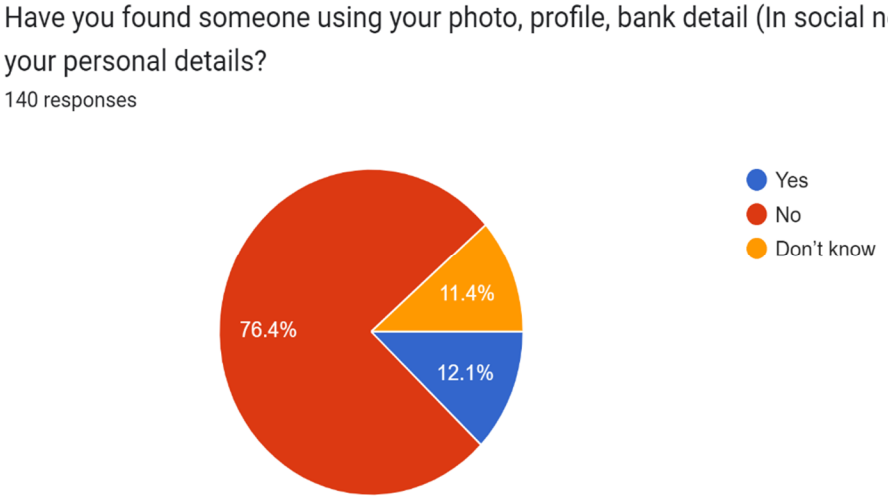
Interpretation:

This analysis paints a picture of the people who feel positive about keeping their personal devices and online accounts safe and secure. Approximately, 35.7% of the people feel very confident about keeping their accounts and devices secure, 34.3% of the people feel confident, 7.9% people feel neutral or maybe not sure about their security and 7.9% of people feel unconfident. As per this analysis, the people who feel neutral and unconfident about the security of their personal devices and online accounts must be guided and should be provided knowledge regarding the same otherwise they could be exposed to cyber threats.

Have you found someone using your photo, profile, bank detail (In social network) or duplicating your personal details?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	16	11.4	11.4	11.4
	No	109	77.9	77.9	89.3
	Don't know	15	10.7	10.7	100.0
	Total	140	100.0	100.0	



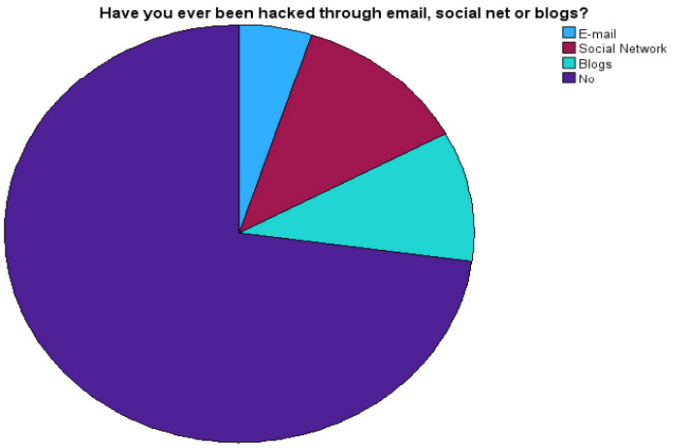


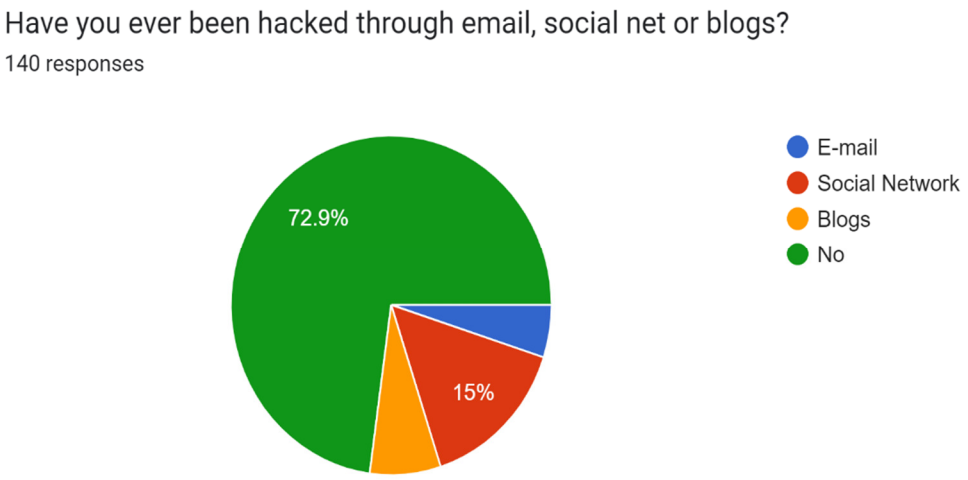
Interpretation:

The above analysis represents the data of people whose personal details such as photos, profiles, bank details, etc, have been used by someone else. The analysis shows that 76.4% of the people did not experience any such thing, whereas 11.4% of the people are completely unaware whether their details are being used by someone else or not. Also, 12.1% of the people have experienced it and are aware that someone else has been using their details. The people who are aware and are not aware of it are at risk of cyber threats and cyberattacks. The people who are completely unaware should check for the same to reduce their chances of cyber threats.

Have you ever been hacked through email, social net or blogs?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	E-mail	7	5.0	5.0	5.0
	Social Network	17	12.1	12.1	17.1
	Blogs	14	10.0	10.0	27.1
	No	102	72.9	72.9	100.0
	Total	140	100.0	100.0	

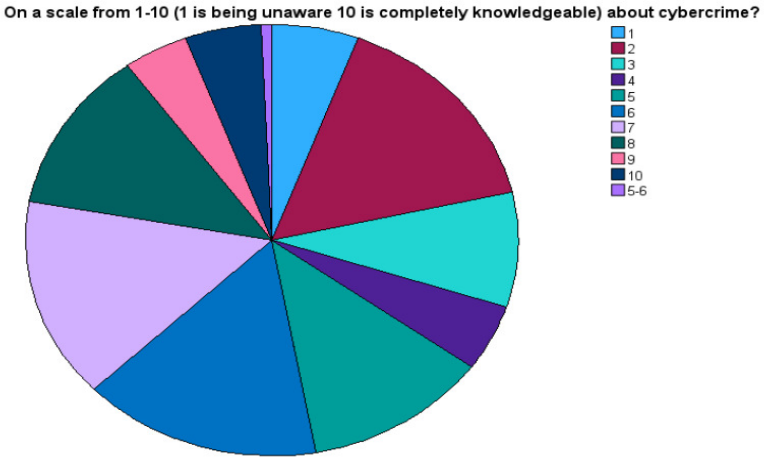


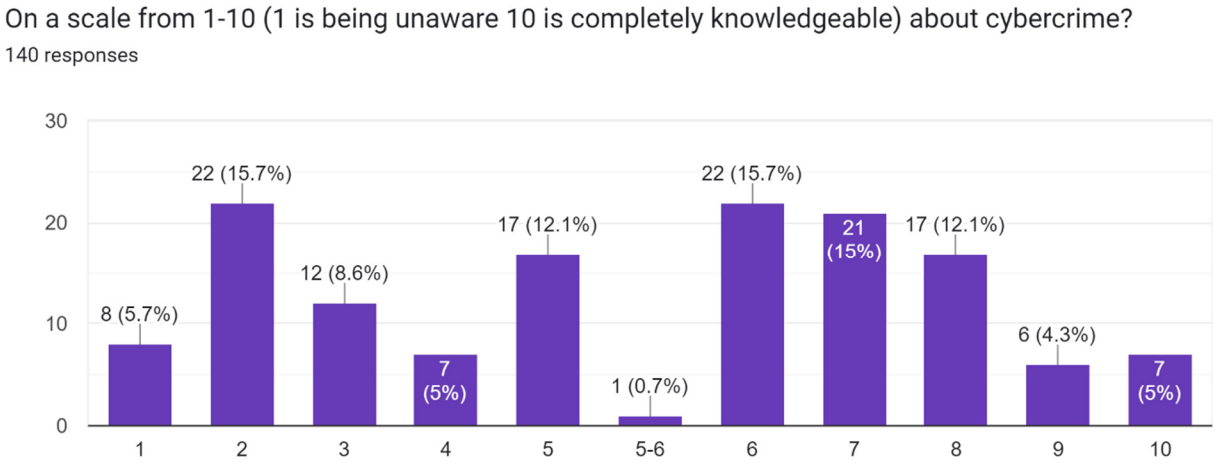


Interpretation:

The given analysis presents the data of people who have been hacked through social networking sites, e-mails, and blogs. According to the analysis, 72.9% of the people have not been hacked through any of the platforms whereas 15% of the people have been hacked through social networking sites. In today's world, hacking through social networking sites is increasing at a greater pace and increasing cyberattacks and losses. It also leads to cyberpornography and cyberdefamation which leave people depressed and have a great impact on their reputation.

On a scale from 1-10 (1 is being unaware 10 is completely knowledgeable) about cybercrime?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	8	5.7	5.7	5.7
	2	22	15.7	15.7	21.4
	3	12	8.6	8.6	30.0
	4	7	5.0	5.0	35.0
	5	17	12.1	12.1	47.1
	6	22	15.7	15.7	62.9
	7	21	15.0	15.0	77.9
	8	17	12.1	12.1	90.0
	9	6	4.3	4.3	94.3
	10	7	5.0	5.0	99.3
	5-6	1	.7	.7	100.0
	Total	140	100.0	100.0	

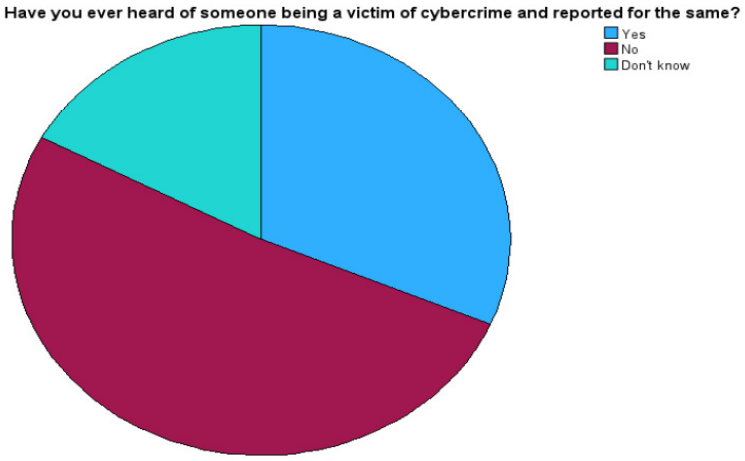


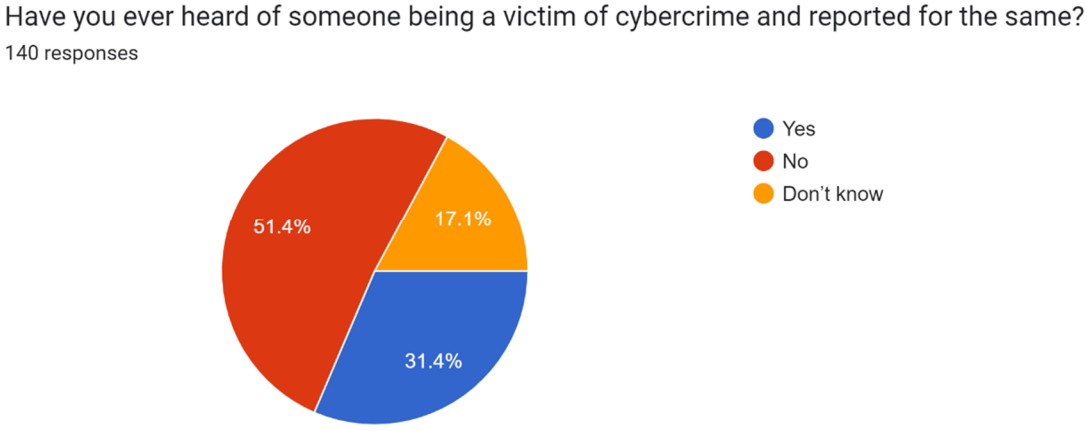


Interpretation:

The given statistic represents the data of people's knowledge about cybercrime. From the statistics, we can see that a total of 52.1% of the people are knowledgeable about cybercrime among which only 5% of people are completely knowledgeable about it whereas a total of 47.8% of people are completely unaware about cybercrime. The main objective of this research is to provide knowledge about cybercrime to the people so that they can prevent themselves from cyber threats and cyberattacks. In today's world where the cybercrime rate is increasing at a greater pace, people must have a good knowledge about cybercrime so that they don't experience it. The institutions should provide special programs to impart knowledge on cybercrime. The ones who have a piece of good knowledge about cybercrime should help other people in society and guide them for the same.

Have you ever heard of someone being a victim of cybercrime and reported for the same?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	44	31.4	31.4	31.4
	No	72	51.4	51.4	82.9
	Don't know	24	17.1	17.1	100.0
	Total	140	100.0	100.0	



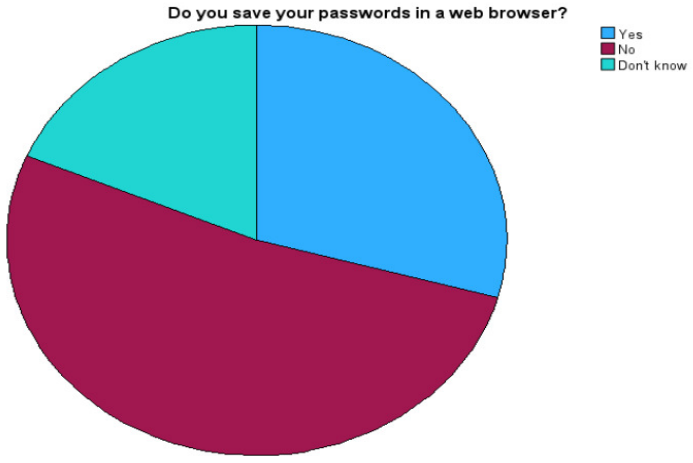


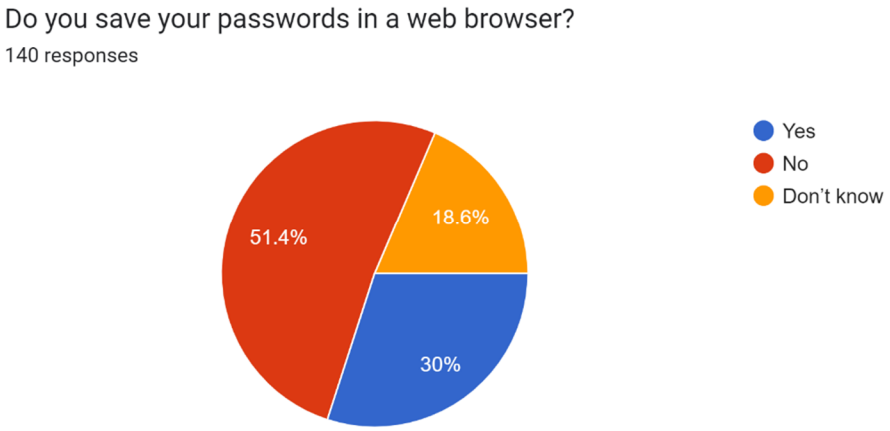
Interpretation:

The given analysis presents the data of people who heard of someone being a victim of cybercrime and reported the same. It depicts that 51.4% of the people were completely unaware of any cybercrime victim and did not report if they knew also. 31.4% of the people who heard of cybercrime victims also reported for it whereas 17.1% of people did not know whether they have heard of any cybercrime victim or not. There are people who if heard about any cybercrime victim, did not report it which harms society. It's important to report the cybercrime victims to reduce cyberattacks in society and prevent more such cases. The people who reported it show their active participation in helping society and making people aware of it.

Do you save your passwords in a web browser?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	41	29.3	29.3	29.3
	No	73	52.1	52.1	81.4
	Don't know	26	18.6	18.6	100.0
	Total	140	100.0	100.0	

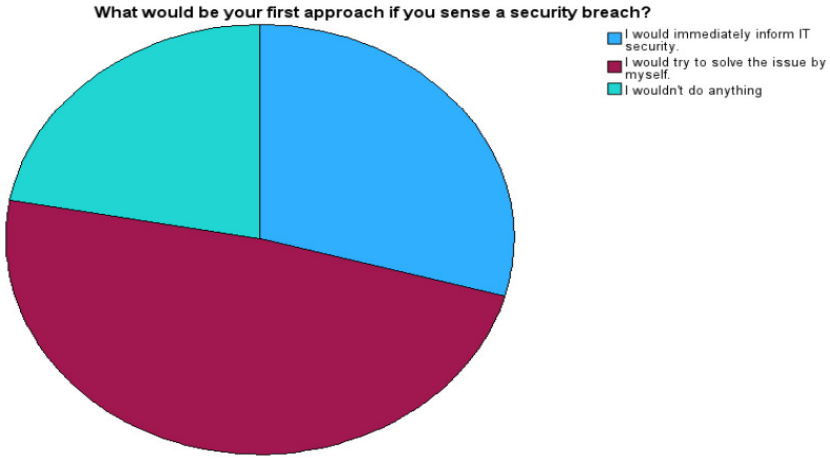


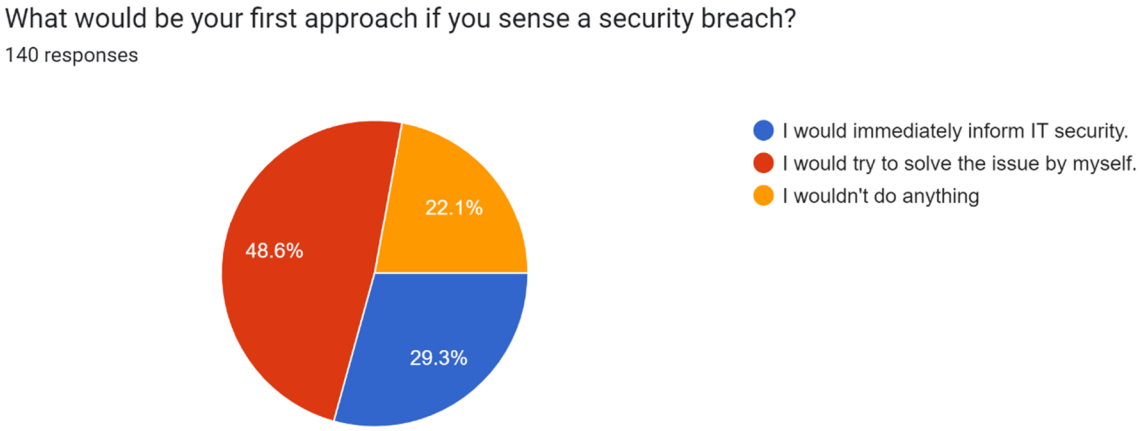


Interpretation:

The analysis presents the data of people who save their important passwords in web browsers. As per the given data, 51.4% of people do not save their passwords in web browsers, 30% of people do save their passwords in web browsers, and 18.6% of people are unaware of whether they save their passwords or not in web browsers. People should not save their passwords in web browsers as they are at higher risk of cyber threats. If their accounts get hacked then they might suffer huge losses and reputational damage.

What would be your first approach if you sense a security breach?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I would immediately inform IT security.	41	29.3	29.3	29.3
	I would try to solve the issue by myself.	68	48.6	48.6	77.9
	I wouldn't do anything	31	22.1	22.1	100.0
	Total	140	100.0	100.0	





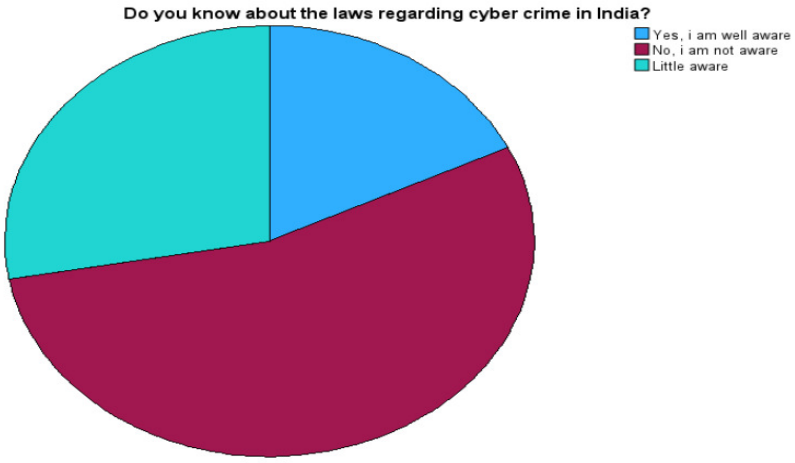
Interpretation:

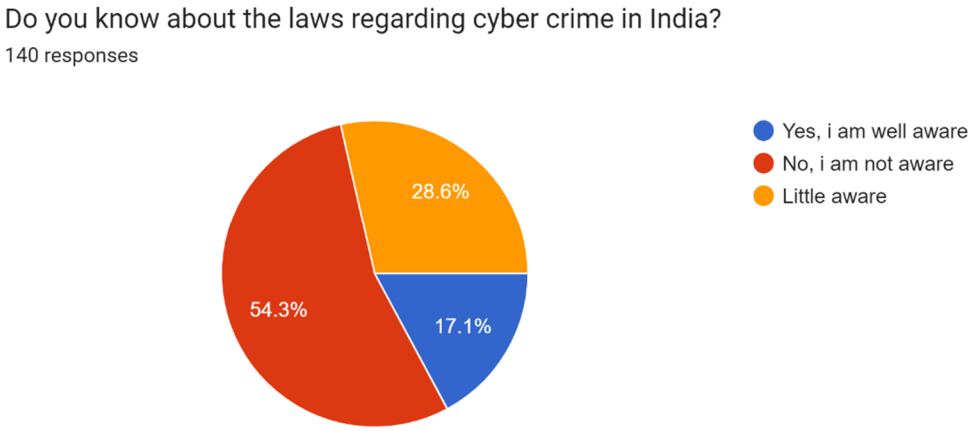
When asked about the first approach by the people if they sense a security breach, 29.3% of people responded that they would inform IT security immediately, 48.6% of people

would try to solve the issue by themselves, and 22.1% of people would not do anything. We can see that the majority of the people would try to solve the issue by themselves as they are unaware of IT security and less knowledgeable about cybercrime. Therefore, it's important to provide knowledge to the people regarding cybercrime and ways to tackle security breaches. It will result in decreasing cybercrime rates in the society.

Do you know about the laws regarding cyber crime in India?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, i am well aware	25	17.9	17.9	17.9
	No, i am not aware	76	54.3	54.3	72.1
	Little aware	39	27.9	27.9	100.0
	Total	140	100.0	100.0	





Interpretation:

This analysis presents the data on people's knowledge about the cyber laws in India. As per the data, 54.3% of people are completely unaware of the cyber laws in the country, 28.6% of people are little aware of the cyber laws, and 17.1% of people are only aware of the prevalent cyber laws in the country. The analysis depicts that the majority of people are unaware of the cyber laws in the country due to a lack of knowledge on cybercrime and that is the result of the increasing cybercrime rate in the country. It's high time that society should be provided with good knowledge of cybercrime, cyber laws, its threats, etc. Since the majority of people are unaware of the cyber laws and the remedies provided for cybercrime, the majority of people try to solve their issues by themselves in cases of security breaches.

CONCLUSION:

In conclusion, cybercrime poses significant challenges to society, impacting individuals, businesses, governments, and overall societal trust in online systems. The proliferation of cyber threats such as hacking, phishing, identity theft, and ransomware attacks has resulted

in financial losses, data breaches, and erosion of privacy. Additionally, cybercrime can facilitate other forms of criminal activity, including fraud, terrorism, and espionage.

Here are some remedies that can be followed to overcome these challenges-

- **Strengthening cybersecurity measures**: Businesses, governments, and individuals must invest in robust cybersecurity infrastructure and practices to protect against cyber threats. This includes regular software updates, strong password policies, encryption, and security awareness training.
- **Enhanced law enforcement efforts**: Law enforcement agencies need adequate resources and training to investigate and prosecute cybercriminals. International cooperation is also crucial to combat cybercrime, given its transnational nature.
- **Public awareness and education**: Increasing public awareness about cyber threats and best practices for cybersecurity is essential. Education initiatives can help individuals and organizations recognize potential risks and take appropriate precautions.
- **Technological innovation**: Continued innovation in cybersecurity technologies, such as artificial intelligence, machine learning, and blockchain, can help in detecting and preventing cyber threats more effectively.
- **Collaboration between public and private sectors**: Collaboration between governments, businesses, academia, and civil society is vital to addressing cybersecurity challenges collectively. Information sharing and coordination efforts can enhance cybersecurity resilience across various sectors.

Cybercrime is a pervasive and evolving threat that undermines the fabric of society. Its impact extends beyond financial losses to encompass privacy violations, disruption of critical infrastructure, erosion of trust, and challenges to national security. Addressing cybercrime requires a multifaceted approach involving technological innovation, regulatory frameworks, international collaboration, and public awareness efforts to mitigate its detrimental effects on society.

REFERENCES:

Research paper-

i. Saini, Hemraj, Yerra Shankar Rao, and Tarini Charan Panda. "Cyber-crimes and their impacts: A review." *International Journal of Engineering Research and Applications* 2.2 (2012): 202-209.

ii. Das, Sumanjit, and Tapaswini Nayak. "Impact of cybercrime: Issues and challenges." *International journal of engineering sciences & Emerging Technologies* 6.2 (2013): 142-153.

iii. Singh, Devika. "Emerging Trends in Cyber Crimes." *Sustainable Business and IT* (2023): 39-45.

iv. Javkhedkar, Sarang, Anjali Shrungarkar, and Atul P. Kulkarni. "An Ethical Angle of Cyber Crime Issues and Challenges in India."

v. Chawla, Rakesh Kumar, J. S. Sodhi, and Triveni Singh. "Study of the Need for Effective Cyber Security Trainings in India." *International Conference on Data Management, Analytics & Innovation*. Singapore: Springer Nature Singapore, 2023.

Websites-

https://www.ijcrt.org/papers/IJCRT2307276.pdf

https://lexpeeps.in/the-impact-of-cybercrime-on-the-indian-economy-and-society/

https://thefinancialexpress.com.bd/views/reviews/cyber-crime-affects-society-in-different-ways

https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Cybercrime_2016.pdf

https://ignited.in/I/a/293193

https://www.irjmets.com/uploadedfiles/paper//issue_4_april_2023/36239/final/fin_irjmets1681872361.pdf
https://www.legalserviceindia.com/legal/article-10864-cybercrimes-affecting-the-society.html
https://www.bbau.ac.in/dept/Law/TM/1.pdf
https://www.drishtiias.com/daily-updates/daily-news-analysis/cyber-crime-4
https://i4c.mha.gov.in/cyber-crime-categories.aspx
https://en.wikipedia.org/wiki/Cybercrime
https://blog.ipleaders.in/cyber-crime-types-consequences-laws-protection-and-prevention/