CYBERCRIME IN THE DIGITAL AGE: ANALYZING CAUSES AND DEVELOPING PREVENTIVE STRATEGIES

A DISSERTATION

Submitted in partial fulfilment
of the
Requirements for the award of the degree of
BACHELOR OF SCIENCE
in
FORENSIC SCIENCE

by

Ayati Kothari
(TPS2106014)

Under the supervision of
Mr. Akash Chauhan

DEPARTMENT OF FORENSIC SCIENCE

COLLEGE OF PARAMEDICAL SCIENCES

TEERTHANKER MAHAVEER UNIVERSITY MORADABAD

UTTAR PRADESH, INDIA- 244001

2024

DECLARATION

I certify that the dissertation entitled **Cybercrime in the Digital Age: Analyzing Causes and Developing Preventive Strategies** was completed by me at the Department of Forensic Science, Teerthanker Mahaveer University, Moradabad. This is submitted in partial fulfilment of the requirements for the award of the degree of Bachelor of Science in Forensic Science. The work submitted herein is true and original to the best of my knowledge and belief.

TEERTHANKER MAHAVEER UNIVERSITY
TMU
MORADABAD
तीर्थंकर महावीर विश्वविद्यालय
सम्यक् दर्शन • सम्यक् ज्ञान • सम्यक् चारित्र
Accredited with NAAC A Grade
12-B Status from UGC

Date: June 10, 2024
Place: Moradabad

Ayati Kothari

CERTIFICATE

This is to certify that, Ayati Kothari, Bachelor of Science in Forensic Science, the sixth semester has completed her dissertation entitled **Cybercrime in the Digital Age: Analyzing Causes and Developing Preventive Strategies** under my supervision and guidance. The dissertation has been submitted to the Department of Forensic Science, Teerthanker Mahaveer University, Moradabad in partial fulfilment of the requirements for the award of the degree of Bachelor of Science in Forensic Science. The work should not be published even in part without the prior written permission of the undersigned.

Date: June 10, 2024
Place: Moradabad

Mr. Akash Chauhan
Supervisor
Department of Forensic Science
Teerthanker Mahaveer University

TEERTHANKER MAHAVEER UNIVERSITY
TMU
MORADABAD
तीर्थंकर महावीर विश्वविद्यालय
सम्यक् दर्शन • सम्यक् ज्ञान • सम्यक् चारित्र
Accredited with NAAC A Grade
12-B Status from UGC

CERTIFICATE

This is to certify that, Ayati Kothari, Bachelor of Science in Forensic Science, the sixth semester has completed her dissertation entitled **Cybercrime in the Digital Age: Analyzing Causes and Developing Preventive Strategies** and submitted it to the Department of Forensic Science, Teerthanker Mahaveer University, Moradabad in partial fulfilment of the requirements for the award of the degree of Bachelor of Science in Forensic Science. This work is carried out by the student under the supervision of the Faculty of the Department of Forensic Science.

TEERTHANKER MAHAVEER UNIVERSITY
TMU
MORADABAD
तीर्थंकर महावीर विश्वविद्यालय
सम्यक् दर्शन • सम्यक् ज्ञान • सम्यक् चारित्र
Accredited with NAAC A Grade
12-B Status from UGC

Date: June 10, 2024
Place: Moradabad

Mr. Ravi Kumar
Head
Department of Forensic Science
Teerthanker Mahaveer University

ACKNOWLEDGEMENT

I extend my heartful gratitude to my supervisor, Mr. Akash Chauhan, Assistant Professor, Department of Forensic Science for leading me into this fascinating area of research. He supported me throughout the days of my dissertation. I am very thankful to him for his patience and faith in me. He assisted me and gave me better ideas about performing the dissertation. It was his constant inspiration and expert guidance, that led to the successful completion of the task. I am sincerely grateful to the Principal, Prof. (Dr) Navneet Kumar**,** for providing the necessary facilities to complete this dissertation. I thankfully acknowledge our H.O.D., Mr. Ravi Kumar for his moral support and guidance. I am also thankful to other faculty members, Mr. Yogesh Kumar, Mr. Himanshu Yadav, Ms. Anshika Srivastava, and Ms. Sukriti Agarwal, of our department for their valuable guidance throughout the tenure of this dissertation. I am grateful to my friends, Anushka Kunwar, Sammanita Singh, Pratiksha Agarwal, Aman, Drishti Jain, Shatakshi Sharma, and all the classmates who helped me complete my dissertation. I would also like to thank every person who directly or indirectly helped me complete the dissertation. Lastly, I heartily thank my parents for their support and blessings.

TEERTHANKER MAHAVEER UNIVERSITY
TMU
MORADABAD
तीर्थंकर महावीर विश्वविद्यालय
सम्यक् दर्शन • सम्यक् ज्ञान • सम्यक् चारित्र
Accredited with NAAC A Grade
12-B Status from UGC

CONTENTS

TABLE OF FIGURES

ABSTRACT

Cybercrime is a global threat that threatens the safety and security of individuals, and organizations in the digital world. This research aims to explore the factors that drive cybercriminal behavior, identify the vulnerabilities in digital ecosystems, and suggest effective strategies for prevention and mitigation. The study also discusses the legal and ethical perspectives of cybercrime and cybersecurity, providing insights into the measures and policies implemented to safeguard the integrity of our digital society. A total of 200 respondents from various demographic groups completed the survey. The results of this survey highlight how commonplace bogus calls are and how much of an impact they have on people's mental health, financial stability, and privacy. It also focuses on the number of people who have been the victim of cybercrime and their awareness regarding it. The findings of this research can be instrumental in formulating effective strategies to prevent and mitigate the risks associated with cyber threats. This report aims to provide a summary of the survey findings and offer insights into prevailing attitudes toward cybersecurity.

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

INTRODUCTION

Cyber forensics is a meticulous process of extracting electronic data as evidence of a crime while adhering to proper investigation rules to apprehend the culprit. The primary objective of cyber forensics is to maintain a chain of evidence and documentation to identify the perpetrator of the digital crime. This process is beneficial because it can recover deleted files, chat logs, emails, SMS, and phone calls, record audio of phone conversations, determine which user used which system and for how long, and identify which user ran which program[1].

Cybercrime is a broad term used to describe criminal activities carried out using computers and the internet. 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].

In today's digital world, technology has opened a lot of exciting opportunities for growth and innovation. Unfortunately, it has also brought about an increase in cybercrime. Cybercrime includes illegal activities carried out on digital platforms, such as fraud and theft, cyber espionage, and sabotage. These criminals are hard to catch, and they take advantage of the vulnerabilities in networks, systems, and human behavior.

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. Laws and policies are struggling to keep up with the ever-changing technology, making it difficult to combat cybercrime effectively[3].

Cybercrime is a significant and growing issue worldwide, affecting a substantial portion of the population in various ways. However, the percentage of individuals affected can vary depending on the source and methodology of the study. Approximately, 30% to 60% of people globally have fallen victim to cybercrime at some point. Nevertheless, these figures may not capture the complete extent of cybercrime since many incidents go undetected or unreported. Several factors contribute to the widespread nature of cyber threats. These include the increasing digitization of personal and financial information, the proliferation of internet-connected devices, and the evolving tactics of cybercriminals. Additionally, as technology advances, new vulnerabilities, and attack vectors emerge, further heightening the risk of cybercrime for individuals and organizations alike[2].

That is why this study is diving into the world of cybercrime, aiming to provide insights into its underlying mechanisms, emerging trends, and societal impacts. This study takes a multidisciplinary approach, including criminology, sociology, computer science, and law. By identifying the motivations driving cybercriminal behavior, finding vulnerabilities in digital ecosystems, and suggesting effective strategies for prevention and mitigation, this research aims to contribute to the ongoing efforts to combat cybercrime and safeguard the integrity of our digital society[1].

A few examples of cybercrime are:

1. **Cyberattacks:** These involve unauthorized access to computer systems or networks for malicious purposes. Examples of cyberattacks include:
   - Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. This includes viruses, worms, Trojans, ransomware, and spyware.
   - Phishing: Deceptive techniques used to trick individuals into providing sensitive information such as passwords, credit card numbers, or personal data. Phishing attacks often involve emails, fake websites, or messages pretending to be from legitimate sources.
   - Denial-of-Service (DoS) attacks: Overloading a network or server with excessive traffic to disrupt its normal functioning and deny service to legitimate users.
   - Man-in-the-middle (MitM) attacks: Intercepting communication between two parties to eavesdrop on or alter the data being transmitted.
2. **Identity Theft:** Cybercriminals steal personal information, such as social security numbers, bank account details, or login credentials, to impersonate individuals or conduct fraudulent transactions.
3. **Financial Fraud:** This involves various schemes to steal money or financial assets. Examples of financial fraud include:
   - Credit card fraud: Unauthorized use of credit or debit card information to make fraudulent purchases.
   - Banking fraud: Illegally accessing bank accounts or conducting fraudulent transactions.
   - Cryptocurrency scams: Fraudulent schemes involving cryptocurrencies, such as Ponzi schemes, fake ICOs (Initial Coin Offerings), or phishing attacks targeting cryptocurrency holders.
4. **Data Breaches:** Unauthorized access to sensitive information stored in databases or systems. This may involve personal data, intellectual property, or financial records. Data breaches can lead to financial losses, reputational damage, and legal consequences.
5. **Cyberbullying and Online Harassment:** Using digital platforms to harass, intimidate, or threaten individuals. This includes cyberstalking, online defamation, and spreading malicious rumors or false information.
6. **Cyber Espionage:** State-sponsored or corporate espionage activities aimed at stealing sensitive information, intellectual property, or trade secrets. Cyber espionage can have significant geopolitical and economic implications.
7. **Child Exploitation:** The use of the internet to exploit children for sexual purposes, trafficking, or grooming. This includes activities such as child pornography, online grooming, and sextortion.
8. **Cyber Warfare:** Coordinated attacks against the infrastructure, networks, or systems of other nations or organizations for strategic or political purposes. Cyber warfare can involve disrupting critical services, stealing sensitive information, or causing widespread chaos. Combatting cybercrime requires a multi-faceted approach

involving technical solutions, cybersecurity measures, legislation, international cooperation, and public awareness campaigns. Cybercrime poses significant challenges for law enforcement agencies, governments, businesses, and individuals[3].

To protect oneself, their devices, and their data from online threats, it is important to take proactive steps to prevent cybercrime.

Here are some essential tips to help stay safe online:

1. **Use strong, unique passwords:** Create strong passwords for all accounts and avoid using the same password for multiple accounts. Use a reputable password manager to securely store and generate complex passwords.
2. **Enable multi-factor authentication (2FA):** Enable multi-factor authentication wherever possible, as it adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone, and your password.
3. **Keep software updated:** Regularly update the operating system, antivirus software, web browsers, and other applications to patch security vulnerabilities and protect against known threats.
4. **Beware of phishing attempts:** Be cautious of unsolicited emails, messages, or calls asking for personal or financial information. Phishing attempts often masquerade as legitimate entities to trick you into revealing sensitive data. Verify the authenticity of requests before responding or clicking on any links.
5. **Secure the Wi-Fi network:** Use strong encryption, such as WPA2 or WPA3, and a unique password for your Wi-Fi network to prevent unauthorized access. Avoid using default or easily guessable passwords.
6. **Beware of public Wi-Fi:** Exercise caution when using public Wi-Fi networks, as they may be insecure and vulnerable to eavesdropping. Consider using a virtual private network (VPN) to encrypt your internet connection and protect your data when connecting to public Wi-Fi.
7. **Backup your data regularly:** Backup important files and data regularly to an external hard drive, cloud storage service, or both. In the event of a ransomware attack or data loss, having backups can help restore the files without paying a ransom.
8. **Educate yourself:** Stay informed about the latest cybersecurity threats and best practices for staying safe online. Educate yourself and your family members about common scams, phishing techniques, and ways to protect personal information.
9. **Use secure websites:** When making online transactions or sharing sensitive information, ensure that the website's URL begins with https:// and displays a padlock icon in the address bar. This indicates that the website is using encryption to protect your data.
10. **Monitor your accounts:** Regularly review your bank statements, credit reports, and online accounts for any suspicious activity. Report any unauthorized transactions or unusual behavior to the relevant authorities immediately.

By following these cybersecurity best practices, you can significantly reduce the risk of falling victim to cybercrime and safeguard your digital identity and assets[4].

International cooperation is crucial in effectively combating cybercrime due to the borderless nature of cyber threats and the interconnectedness of digital networks.

There are several ways in which countries can work together to address cybercrime:

1. **Information sharing:** Countries exchange information and intelligence on cyber threats, trends, and incidents to enhance situational awareness and improve their ability to detect and respond to cyber-attacks. This sharing of information may occur bilaterally between countries or through multilateral forums and organizations.
2. **Mutual Legal Assistance Treaties (MLATs):** MLATs are agreements between countries that facilitate cooperation in criminal investigations and proceedings. These treaties enable the exchange of evidence, witness testimony, and other legal assistance between law enforcement agencies in different jurisdictions, aiding in the investigation and prosecution of cybercriminals.
3. **International law enforcement cooperation:** Law enforcement agencies collaborate across borders to investigate cybercrimes that have transnational implications. This cooperation may involve joint operations, task forces, or coordinated efforts to apprehend cybercriminals and disrupt cybercrime networks operating across multiple countries.
4. **Capacity building and technical assistance:** Developed countries provide technical assistance and capacity-building support to developing nations to strengthen their cybersecurity capabilities and enhance their ability to combat cybercrime. This assistance may include training programs, technology transfers, and the provision of tools and resources to improve cybercrime investigation and response capabilities.
5. **International organizations and initiatives:** International organizations such as Interpol, the United Nations Office on Drugs and Crime (UNODC), and the Council of Europe's Cybercrime Convention (also known as the Budapest Convention) facilitate cooperation and coordination among member states to combat cybercrime. These organizations provide platforms for sharing best practices, developing common standards and protocols, and fostering collaboration among law enforcement agencies and other stakeholders.
6. **Public-private partnerships:** Governments collaborate with private sector entities, academia, and civil society organizations to address cyber threats collaboratively. Public-private partnerships promote information sharing, facilitate joint initiatives for cyber risk management, and leverage the expertise and resources of both sectors to enhance cybersecurity and combat cybercrime.
7. **Cybersecurity Capacity Maturity Model (CMM):** Some initiatives, such as the CMM developed by the Organization of American States (OAS), provide a framework for assessing and enhancing the cybersecurity capabilities of countries. This framework enables countries to identify areas for improvement, prioritize capacity-building efforts, and benchmark their progress in addressing cyber threats.

By fostering collaboration and coordination among countries, international cooperation plays a vital role in addressing the global challenge of cybercrime and promoting a safer and more secure cyberspace for all[4].

India has implemented several laws and regulations to tackle cybercrime and enhance cybersecurity.

Some of the significant legislations related to cybercrime in India include:

1. **Information Technology Act, 2000 (IT Act):** This legislation is the primary governing law for cyber activities and electronic commerce in India. It provides legal recognition for electronic records and digital signatures. Additionally, it outlines offenses related to unauthorized access, hacking, data theft, cyber terrorism, and the distribution of obscene materials online. The IT Act was amended in 2008 to strengthen provisions related to cybercrime and introduce new offenses and penalties[5].
2. **Indian Penal Code (IPC):** Certain provisions of the IPC, such as Sections 65, 66, 66A, 66B, 66C, and 66D, are relevant to cybercrime and prescribe penalties for offenses such as hacking, identity theft, cyberstalking, and online defamation[5].
3. **Information Technology (Amendment) Act, 2008:** This amendment to the IT Act introduced several new provisions to address emerging cyber threats and enhance cybersecurity measures. It criminalized activities such as cyber terrorism, the publication or transmission of sexually explicit material in electronic form, and the unauthorized interception of electronic communications[5].
4. **National Cyber Security Policy, 2013:** This policy framework outlines the government's vision and strategy to enhance cybersecurity and protect critical information infrastructure in India. It emphasizes the importance of collaboration between government agencies, private sector entities, and other stakeholders to address cyber threats effectively[5].
5. **Rules and Regulations under the IT Act:** The government has issued various rules and regulations under the IT Act to regulate specific aspects of cyber activities, such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which govern the regulation of online content and social media platforms[5].
6. **Cybercrime Investigation Cells:** Several states in India have established specialized cybercrime investigation cells or cyber police stations to investigate and prosecute cyber offenses effectively. These units typically collaborate with other law enforcement agencies and cybersecurity experts to combat cybercrime[5].

It is important to note that the legal landscape surrounding cybercrime in India continues to evolve, with amendments and updates being made to existing laws and regulations to address emerging threats and challenges in cyberspace. Additionally, international cooperation and collaboration play a crucial role in addressing transnational cybercrimes and ensuring effective enforcement of cyber laws[5].

Research in cybercrime prevention and causes is of utmost importance for various reasons[6]:

1. It helps in understanding the ever-evolving nature of cyber threats, including the tactics, techniques, and procedures used by cybercriminals, which is crucial for devising effective countermeasures.
2. Through research, vulnerabilities in systems, networks, and software can be identified, which provides essential information to develop patches and updates to mitigate these vulnerabilities and enhance cybersecurity.
3. Research findings can also inform policymakers and legislators about the nature and extent of cyber threats, leading to the development of appropriate laws, regulations, and policies aimed at combating cybercrime and enhancing cybersecurity at national and international levels.
4. Research contributes to the development of advanced cybersecurity technologies, tools, and strategies for preventing, detecting, and responding to cyber threats effectively.
5. The outcomes of research can be used to educate individuals, organizations, and communities about cyber threats, thereby raising awareness and promoting best practices for cybersecurity hygiene.
6. Research helps law enforcement agencies understand cybercriminal behavior patterns, gather digital evidence, and develop investigative techniques to prosecute cybercriminals successfully.
7. Cybercrime has significant economic ramifications, including financial losses, disruption of business operations, and loss of intellectual property. Research helps in quantifying these impacts and developing cost-effective strategies for mitigating them.
8. Effective cybercrime prevention measures must balance security with privacy and civil liberties. Research can contribute to the development of solutions that prioritize individual rights while combating cyber threats.

Overall, research in cybercrime prevention and its causes plays a crucial role in safeguarding individuals, organizations, and societies against the growing menace of cyber threats. It enables proactive measures to mitigate risks, protect critical infrastructure, and uphold cybersecurity principles in an increasingly digital world.

AIM:

The aim of this study is to explore the various factors contributing to the rise of cybercrime and to develop effective strategies to prevent and combat it.

OBJECTIVES:

- Investigate best practices for preventing cybercrime, including encryption, multi-factor authentication, intrusion detection systems, and employee training programs.
- To conduct a thorough analysis to calculate the number of individuals affected by cybercrime.
- To determine the number of individuals who are knowledgeable and aware of cybercrime, as well as the necessary precautions and measures to prevent cyberattacks.

REVIEW OF LITERATURE

1. **Das and Nayak (2013) -** As per this research study, the role of the government is of utmost importance in preventing cybercrime. However, the onus of responsibility lies significantly on commercial entities creating software and those capable of stopping fraud. Consumer outreach campaigns may have limited efficacy, and only a small percentage of potential victims can be assisted through such endeavors. Therefore, to combat cybercrime effectively, non-intrusive interventions that require substantial involvement are necessary. It is essential to keep security measures simple and efficient to ensure their effectiveness. While it is impossible to predict the future, we can safely assume that the Internet will continue to exist. However, it is uncertain whether cybercrime will remain a significant problem in the long run[7].

2. **Bele et.al (2014) -** As per this research, it has been identified that there is a significant need for additional education regarding the hazards of cybercrime and the significance of information safety for all target groups. Consequently, it has been concluded that ongoing education is imperative in raising consumer awareness and motivating them to utilize preventive strategies in their daily lives. Considering this, an assessment will be conducted following the completion of each educational module to evaluate the effectiveness of its implementation. By implementing these educational modules that specifically target younger Internet users, we will be taking the first step toward creating a culture of information security[8].

3. **Esther Ramdinmawii et.al (2015) -** The study on cybercrime reveals that a significant number of countries are still grappling with this issue, even in today's digital age. Among them, the United States of America has borne the brunt of cyberattacks, suffering the highest damage in terms of financial loss, data breaches, and other forms of cybercrime. The study notes that cybercrime is rampant in common areas such as online banking and e-commerce, social media, and email phishing scams. With the increasing sophistication of cybercriminals, new forms of cybercrime continue to emerge, including ransomware attacks, identity theft, and hacking. The study highlights the need for stronger cybersecurity measures and greater awareness among individuals and organizations to combat cybercrime effectively[9].

4. **M Lakshmi Prasanthi (2015)** - The paper delves into the critical topics of cybercrime and cybersecurity and explores different types of cybercrime that the authors have encountered. It also discusses various techniques to prevent and detect cyberattacks. The prevention techniques discussed in the paper include Tripwires, configuration-checking tools, Honey Pots, and anomaly detection systems. These tools help to prevent cyberattacks by detecting unusual activity and alerting the relevant authorities. The paper also discusses the importance of operating system

commands in identifying and preventing cyber threats. In addition, the paper highlights the significance of cybersecurity in today's world, where cybercrime has become a significant threat to individuals and organizations alike. The authors emphasize the need for individuals and businesses to take measures to protect their data and systems from cyber-attacks. The paper also discusses the legal and ethical perspectives of cybercrime and cybersecurity, providing insights into the measures and policies that can be implemented to ensure the safety and security of individuals and organizations in the digital world[10].

5. **Jigar Shah (2016) -** This survey-based study found that many internet users are unaware that cybercrimes can also target individuals. Besides hacking, users are unaware of cyber-stalking, TOR and Deep web crimes, copyright infringement, cyberbullying, phishing, child soliciting, and sharing of disturbing content. Half of the respondents have already become victims of various viruses and have not been adequately securing their PCs and laptops. The study urges the government to take necessary measures to enforce rules and regulations to prevent cybercrimes and educate citizens about cybersecurity[11].

6. **Maziah Mohd Ali (2016) -** This article provides an in-depth analysis of the research conducted by the researcher on the key determinants that can help prevent cybercrimes among Bumiputera entrepreneurs operating in the online business sector in Malaysia and Perak. The study aims to identify the crucial factors that can mitigate the risks of cyber-attacks and safeguard the interests of online businesses. Through rigorous research and data analysis, the authors have identified various factors that can help businesses protect themselves against cyber threats. The findings of this research can be instrumental in formulating effective strategies to prevent cybercrime and improve the overall cybersecurity posture of online businesses in Malaysia and Perak[12].

7. **Nir Kshetri (2016) -** This article delves into the issue of cybercrime and cybersecurity in India. It highlights that around 30 million Indians have fallen prey to cybercrime, which has cost the Indian economy a staggering $7.6 billion per year. India has also become a target of high-profile international cyberattacks. Additionally, the article discusses the measures taken by the government of India, such as UIDAI and NCPS, to tackle this menace[13].

8. **Anisha (2017) -** This study concluded that technology-based crimes are increasing daily and require our utmost attention. Due to their diverse nature, it is challenging to identify cybersecurity problems, which leads to a lack of knowledge about security risks. To address this issue, we can arrange workshops and free advertisements with the help of government and non-governmental organizations. We must begin raising awareness about cybercrimes and cyber illiteracy at the grassroots level, including institutes, schools, computer centers, and individuals[14].

9. **N. Jyoti (2017) -** In the paper, the author provides information related to cybercrime, the right to privacy, and the importance of securing individuals' private data, as stated in the National Cyber Security Policy. The paper discusses various types of cybercrimes, such as Hacking, Cyber Stalking, Spamming, Cyber Phishing, and Cyber terrorism[14].

10. **Sreehari A et.al (2018) -** This research showed that most students are just aware of cybercrime but do not know much about it. The study also revealed that most students had received spam messages or calls, yet none of them had reported it to the cybercrime cell for prevention. It was also observed that even though the students were aware of cybercrime, they still downloaded various content such as movies and games, which are categorized as cybercrime[15].

11. **Manishaben Jaiswal (2019) -** This article provides a comprehensive analysis of the types of cybercriminals and their motives, along with measures to prevent cybercrime. The article categorizes cybercrime into four different types: against individuals, against property, against organizations, and against society. It further delves into the factors that motivate cybercriminals, such as financial gain, personal vendettas, or ideology. Additionally, the article discusses various network security measures that can help prevent cybercrime, such as biometric control, satellite offices, and firewalls. It also highlights industry standards such as NIST (National Institute of Standards and Technology) that provide a framework for organizations to develop robust cybersecurity policies[16].

12. **Muhammad Suleiman et.al (2020) -** This article concluded that there are numerous approaches to identifying and avoiding cybercrime attacks that can be implemented effectively within our community. This is facilitated by utilizing various ICT-based resources such as social media platforms, social networking sites, electronic transactions, computer collaborations, and more. These resources can play a significant role in combating cybercrime since they enable individuals and organizations to share information, collaborate, and make informed decisions. For example, social media platforms can be used to spread awareness about cyber threats, while electronic transactions can be secured using encryption technologies to prevent unauthorized access. Additionally, computer collaborations can enable organizations to share intelligence and coordinate their efforts in responding to cyber-attacks. Overall, these ICT-based resources can be leveraged effectively to mitigate the risks of cybercrime and enhance the safety and security of our communities[17].

13. **Olena Sviatun (2021) -** This paper discussed the level of cybercrime that had a direct impact on cybersecurity and the legal methods used to counteract it, which varies from country to country. The interrelationship between these factors has been extensively studied and it has been proven that there is a need for international cooperation to develop global strategies and other measures to combat cybercrime.

The development of such strategies and measures is essential to ensure that cybercrime is effectively countered and that the safety and security of individuals, businesses, and governments are protected. Therefore, countries must work together to address the challenges posed by cybercrime and to strengthen their cybersecurity measures[18].

14. **Andrei POP (2022) -** The article aims to raise awareness of cyber security and the significance of implementing cyber data protection systems. Cyber-attacks have surged in recent years, targeting personal computer systems, company computer systems, as well as those managed by state institutions[19].

15. **K Manasa Veena (2022)** - This article discusses how cybercrime is becoming increasingly prevalent in the digital age. To combat this, the use of advanced techniques is necessary to identify criminals. One such technique is the unsupervised method of using Gaussian mixture models, which shows improved performance in detecting cyber criminals[20].

16. **Md. Golam Rabbani Sarker (2022)** - The paper under consideration delves into the intricate subject of the effects of digital media on young individuals, and the numerous reasons that have contributed to the surge in cybercrime on social media. The researcher provides a detailed analysis of the various ways in which digital media has influenced the behavior of young people, as well as its long-term effects on their mental and emotional well-being. Additionally, the paper identifies the different types of cybercrimes committed on social media platforms and their impact on individuals and society as a whole. Finally, the researcher presents a comprehensive set of recommendations aimed at educating children about the dangers of cybercriminals, and how to stay safe online. The paper concludes by emphasizing the need for a proactive approach to addressing cybercrime and safeguarding the next generation[21].

17. **Nguyen The Sang (2022) -** The paper delves into the topic of cybercrime and presents a detailed analysis of its various viewpoints. It discusses how cybercrime affects individuals, organizations, and society as a whole, and highlights the various ways in which it can impact them negatively. The paper also proposes a comprehensive prevention strategy that can help individuals and organizations protect themselves from cyber threats. The strategy takes into account the latest trends and best practices in cybersecurity and aims to provide a robust defense against cybercrime. Overall, the paper serves as a valuable resource for anyone interested in understanding the complex world of cybercrime and how to protect themselves against it[22].

18. **Sardor A. Turaev (2022)** -The article underlines the significance of having a thorough understanding of the criminological description of internet crimes, along with the study of its underlying causes, conditions, and preventive measures, to

effectively combat such offenses. With the prevalence of internet-based crimes, it is essential to comprehend the nature of the crime and its underlying factors to develop effective strategies to prevent and tackle them. The study of criminological aspects of internet-based crimes can provide valuable insights into the criminal behavior, modus operandi, and patterns of such crimes. Further, identifying the root cause and conditions that lead to these crimes can help in taking preventive measures and developing strategies to reduce their occurrence. Therefore, it is crucial to have a comprehensive understanding of the criminological aspects of internet-based crimes to ensure a safer online environment for individuals and businesses[23].

19. **Vinisha Bhagwani (2023) -** The researchers have analyzed the present condition of cyber security and the most widespread types of cyber threats, including phishing, malware, and ransomware. They emphasized the significance of continuous investment in the research and development of cyber security to keep up with the constantly evolving threat landscape[24].

20. **Wang et.al (2023) -** He conducted an in-depth study on the behavior of both victims and abusers, with a specific focus on cyber violence. The study aimed to identify the root causes of cyber violence and to analyze the behavior of both the victim and the abuser to gain a better understanding of the issue. The author further analyzed the findings to identify effective methods to prevent cyber violence. The study concluded that the causes of cyber violence are often multifaceted, with factors such as anonymity, lack of empathy, and social norms playing significant roles. The author suggests that effective prevention methods should address these underlying causes. For instance, measures such as promoting digital literacy, encouraging empathy, and creating awareness of the negative impacts of cyber violence can go a long way in preventing such incidents[25].

METHODOLOGY

A thorough investigation was conducted on **Cybercrime in the Digital Age: Analyzing Causes and Developing Preventive Strategies**. This inquiry involves a multi-disciplinary approach encompassing different fields such as criminology, psychology, and law. It comprises several sections that cover various aspects, such as demographics, cybercrime awareness and experience, cybercrime causes, and cybercrime prevention strategies.

1. RESEARCH METHODOLOGY

a) Research Approach

Quantitative Approach - A structured survey was conducted online to collect quantitative data from social media users.

b) Sampling Design

- Sampling Technique: Stratified Random Sampling
- Population: Urban, Suburban, and Rural areas
- Sample Size: Altogether 200 responses were received in response to 25 questions including demographic data.

c) Data collection

- Instrument: Online Questionnaire
- Platform: Google Forms
- Procedure: The questionnaire was distributed through multiple networks to achieve a more comprehensive audience range. Participants were encouraged to share the survey link with their contacts to expand the survey's reach.
- Questionnaire Structure:

i. Demographic Information: It includes the age, gender, geographic area, educational background, occupation, etc. of the participants.

ii. Cybercrime awareness and experience: The assessment methodology utilizes multiple-choice and linear-scale questions to evaluate one's awareness, knowledge, and understanding of cybercrime. Additionally, it aims to gauge one's susceptibility to falling victim to cyberattacks.

iii. Cybercrime Causes: This section entails gathering the participants' viewpoints concerning cybercriminal activities.

iv. Cybercrime Prevention Strategies: The survey seeks to gather participants' insights regarding their confidence levels in cybersecurity measures, international collaboration, and law enforcement efforts. It also aims to understand their perspectives on cybersecurity education programs and their beliefs about cybercrime prevention. Moreover, the survey delves into the government's responsibility in addressing cybercrime and the fear it instills in the public.

- Collection Method: The data collection process involved distributing a Google form through social media platforms to gather responses from the participants.

d) Data Analysis

The collected responses were subjected to analysis using Microsoft Excel sheets. This approach was taken to ensure that the data was thoroughly and accurately analyzed.

2. ETHICAL CONSIDERATIONS

The following were observed to ensure that moral principles were followed while conducting the survey:

- **Informed Consent:** Before participating in the survey, all the participants were thoroughly informed about the purpose and procedures of the survey. They had provided their consent voluntarily and without any kind of coercion.
- **Confidentiality:** The participants' responses were kept confidential to ensure their privacy. This included protecting their identity.
- **Voluntary Participation:** Participation in the survey was purely voluntary. Participants were free to withdraw their participation at any point in time without facing any negative consequences.
- **Respect for Diversity:** The diversity of the participants, including their cultural backgrounds, beliefs, and values, was respected.
- **Data Security:** The participants' data was stored securely, and all necessary steps were taken to protect it from unauthorized access or disclosure.

3. QUESTIONS INCLUDED IN THE QUESTIONNAIRE

Demographics

1. Name
2. Age
   - Under 18
   - 18-24
   - 25-34
   - 35-44
   - 45-54
   - 55-64
   - 65 or older
3. Gender
   - Male
   - Female
   - Non-binary
   - Prefer not to say
4. What type of area do you primarily reside in?
   - Urban
   - Suburban
   - Rural

5. Educational background
    - Bachelor's Degree
    - Master's Degree
    - PhD or other advanced degrees
6. Occupation
    - Education
    - IT/Technology
    - Business/Management
    - Government/Defense
    - Healthcare
7. Please indicate the types of electronic device(s) you regularly use. (Select all that apply)
    - Desktop / Laptop
    - Smartphone
    - Tablet
8. On average, how many hours per day do you spend using electronic devices for personal or professional activities?
    - Less than 1 hour
    - 1-2 hours
    - 2-4 hours
    - 4-6 hours
    - More than 6 hours

Cybercrime Awareness and Experience

9. Do you use the same password across multiple devices?
    - Always
    - Rarely
    - Never
10. How often do you change your passwords?
    - Regularly
    - Occasionally
    - Rarely
    - Never
11. Are all your electronic devices synchronized?
    - Yes
    - No

12. In which areas of your work do you regularly use a computer? Please select all that apply.
    - Office/Productivity Tasks (e.g., word processing, spreadsheets)
    - Email Communication
    - Random internet browsing
    - Education
    - Online social network
13. Safe/Unsafe use of computer according to you.
    - Work
    - Random web browsing
    - Random free programs use
    - Explicit web browsing
    - Music/movie transfer
    - Online playing games
    - Online banking Email exchange
    - Online shopping
    - Internet data exchange
    - Business Data Exchange
14. Do you go through the terms & conditions of a software/application before signing in?
    - Always
    - Often
    - Occasionally
    - Rarely
    - Never
15. How often do you receive a fake / spam call? Did you ever fall for it?
    - Received, but NEVER fell for it.
    - Received, and fell for it.
    - Never received.
16. Have you or someone you know ever been a victim of cybercrime?
    - Electronic Harassment - Email / Cyber harassment; Cyber blackmailing.
    - Asset Endangerment - Hacking; Computer Virus; Identity Theft; Computer Vandalism; Unauthorized access.
    - Indecent Behavior - Exposure to Indecent Materials, Child Pornography, Hate Speech, Rumor Spreading.
    - Financial Cyber Attacks - Email notification; Bank/financial institution notification; Monitoring of accounts; Unusual activity noticed.
17. How would you rate your awareness/knowledge of cybercrime and cybersecurity issues?
    - Linear Scale (1-5)

Cybercrime Causes

18. What, in your opinion, are the main motivations behind individuals engaging in cybercriminal activities?
    - Lack of cybersecurity awareness
    - Economic factors (unemployment, financial motivation)
    - Anonymity provided by the internet
    - Insufficient law enforcement measures
    - Technological advancements and evolving attack surfaces.
19. How do you think socio-economic factors, such as income inequality and unemployment, may influence individuals to engage in cybercriminal activities?
    - Linear Scale (1-5)

Cybercrime Prevention Strategies

20. How confident are you in the effectiveness of current cybersecurity measures (e.g., firewalls, antivirus software) in preventing cybercrimes?
    - Linear Scale (1-5)
21. Do you think international collaboration and law enforcement efforts are essential in preventing and combating cybercrime?
    - Strongly disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly agree
22. To what extent do you believe cybersecurity education programs can reduce the risk of individuals and organizations falling victim to cybercrime?
    - Not effective
    - Slightly effective
    - Moderately effective
    - Very effective
    - Extremely effective
23. What cybersecurity measures do you believe are most effective in preventing cybercrime? (Select all that apply)
    - Strong passwords
    - Multi-factor authentication
    - Regular software updates
    - Cybersecurity education and training
    - Ethical hacking practices
24. How much responsibility do you believe governments have in preventing cybercrime?
    - Linear Scale (1-5)
25. Fear of cybercrime.
    - Linear Scale (1-5)

RESULT AND ANALYSIS

QUESTIONNAIRE ANALYSIS REPORT

INTRODUCTION

The following report presents the findings of a survey conducted to gather insights on **Cybercrime in the Digital Age: Analyzing Causes and Developing Preventive Strategies**. The survey questionnaire was designed to collect the target audience's opinions, preferences, and demographics.

METHODOLOGY

- Survey Type: Questionnaire
- Sample Size: 200 respondents
- Demographics: Respondents were from varied backgrounds, including various age groups, genders, occupations, educational backgrounds, and geographic locations.

KEY FINDINGS

- ❖ **DEMOGRAPHICS**

Q1. AGE:

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

Q2. GENDER:

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

Q3. 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

Q4. Please indicate the type of electronic device(s) you regularly use. (Select all that apply).

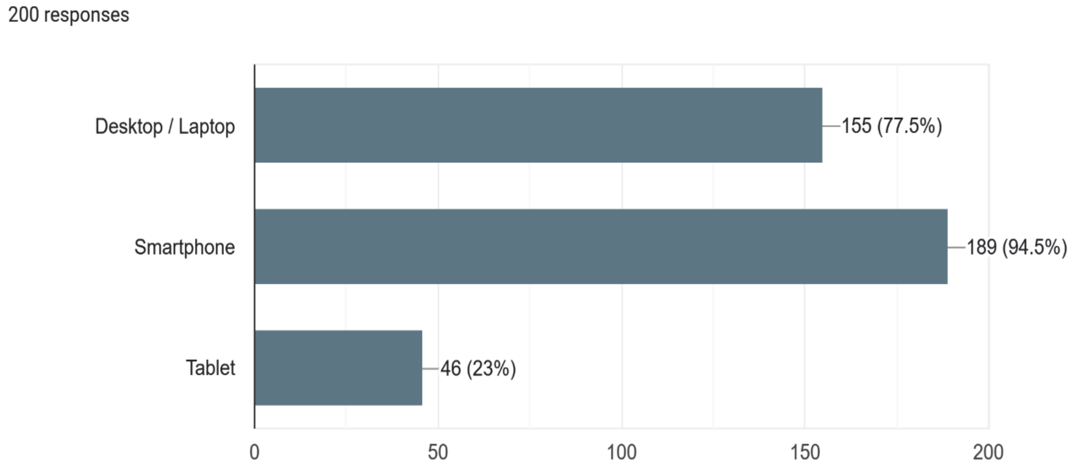

Figure 1

Electronic gadgets have permeated every aspect of modern life, impacting our work, communication, and leisure activities. This research aims to shed light on the various kinds of e-devices that the population uses daily.

According to survey replies, the following technological gadgets were found to be frequently used:

- **Smartphones:** According to reports, smartphones are the electronic gadgets that **94.5%** of people use the most frequently. Smartphones have become incredibly useful tools for many people due to their multipurpose features, which include productivity apps, social media involvement, internet browsing, and communication.
- **Desktops and laptops:** For jobs needing more intensive processing power and productivity, like content production, work-related activities, and sophisticated software usage, desktops and laptops are still necessary.
- **Tablets:** Although not as common as desktops/laptops or smartphones, tablets are very much used **(23%)**. They are beneficial for reading e-books, viewing movies, playing light productivity games, and casual gaming.

Electronic devices are now considered essential tools in modern life, serving various purposes- from entertainment and health monitoring to communication and work. One notable trend is the widespread use of smartphones, which PCs and tablets closely follow. Moreover, e-readers, game consoles, wearable technology, and smart home appliances add to the varied landscape of electronic device usage. Comprehending the prevalent device kinds can facilitate the creation of customized technologies and services to fulfill changing consumer needs.

Q5. On average, how many hours per day do you spend using electronic devices for personal or professional activities?

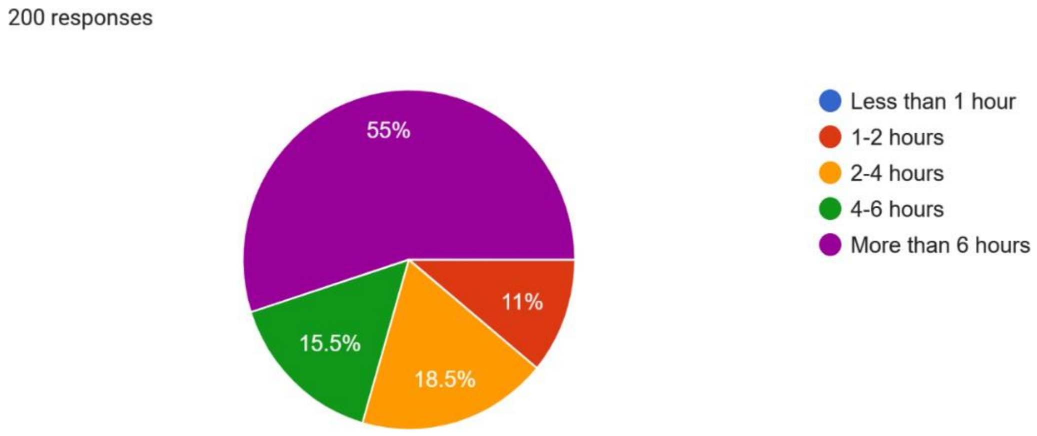

Figure 2

Electronic gadgets are becoming a necessary component of our day-to-day life, being used for both work and personal needs. Knowing how many hours a day on average people spend using electronics can shed light on modern lifestyle choices and technology dependence.

A total of 200 respondents from various demographic groups completed the study. The findings revealed that the majority of the respondents, **55%** stated using electronic devices for around **more than six hours** a day when combining their personal and professional use.

The results highlight how commonplace electronic device use is in contemporary culture. The amalgamation of personal and professional pursuits on digital platforms has resulted in a rise in screen time for people belonging to diverse demographic groups. Even though using electronics excessively can lead to digital fatigue, eye strain, and sedentary lives, they can also be efficient and convenient. Furthermore, the blending of personal and professional gadget usage emphasizes how critical it is to develop appropriate screen-time routines and put digital wellness ideas into practice.

The results of this study indicate that individuals often use electronic gadgets for work or personal purposes for eight hours a day on average. Maintaining a positive connection with digital gadgets requires finding a balance between making use of the positive aspects of technology and minimizing any negative effects as it develops. To ensure people's well-being in an increasingly digitalized society, and to encourage appropriate usage patterns, more research and awareness efforts are necessary.

❖ CYBER AWARENESS AND EXPERIENCE

Q6. Do you use the same password across multiple devices?

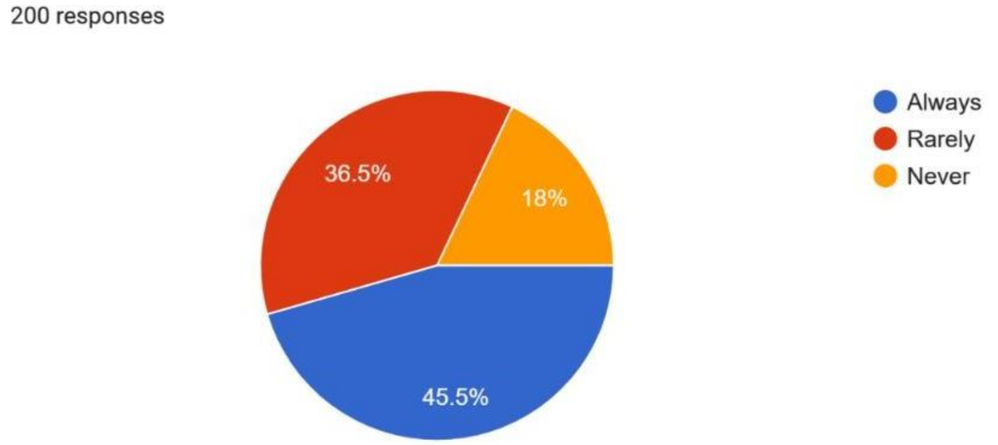

Figure 3

Password security is crucial in the era of digitalization for protecting sensitive and private data. The increasing number of devices including computers, tablets, smartphones, and more means that users frequently struggle to keep track of their passwords on several platforms. The prevalence of using the same password on many devices is examined in this paper, along with its repercussions.

THE FREQUENCY OF PASSWORD REUSE:
45.5% of the total of those surveyed acknowledged using the same password across several devices.

Motivations for Password Reuse:

I. Convenience:
Convenience is the main justification for password reuse. Keeping track of multiple passwords can be difficult, so people choose to keep things simple.

II. Memory:
They have trouble remembering different passwords; therefore, they utilize the same one on all their devices.

III. Lack of Awareness:
Failing to recognize that entering the same password twice poses security issues.

Implications for Security:

- Vulnerability to Breach: Using the same password on several devices raises the possibility that several accounts could be compromised by a single breach.
- Increased Effects of Data Breach: Personal data kept on several platforms is more susceptible in the case of a data breach.
- Cybercriminals use password reuse patterns as a target to carry out credential stuffing attacks, which allow them to access accounts without authorization.

Strategies for Mitigation:

- Password managers: Promoting its use can help lessen the stress of remembering several passwords while guaranteeing strong security thanks to encryption and randomized password creation.
- Two-Factor Authentication (2FA): Using 2FA requires users to authenticate their identity during login using a secondary method (such as an SMS code or biometrics), which adds an extra layer of security.
- Education and Awareness: Creating a culture of cybersecurity hygiene requires raising public awareness of password security procedures and the dangers of reusing passwords.

Although it makes sense to be tempted to reuse passwords for convenience, doing so puts users at serious risk for security breaches. To reduce these dangers, it is essential to implement strong password management techniques like employing password managers and turning on two-factor authentication. Users can strengthen their digital security across numerous devices by adopting safer password practices through education and awareness campaigns.

Q7. How often do you change your password?

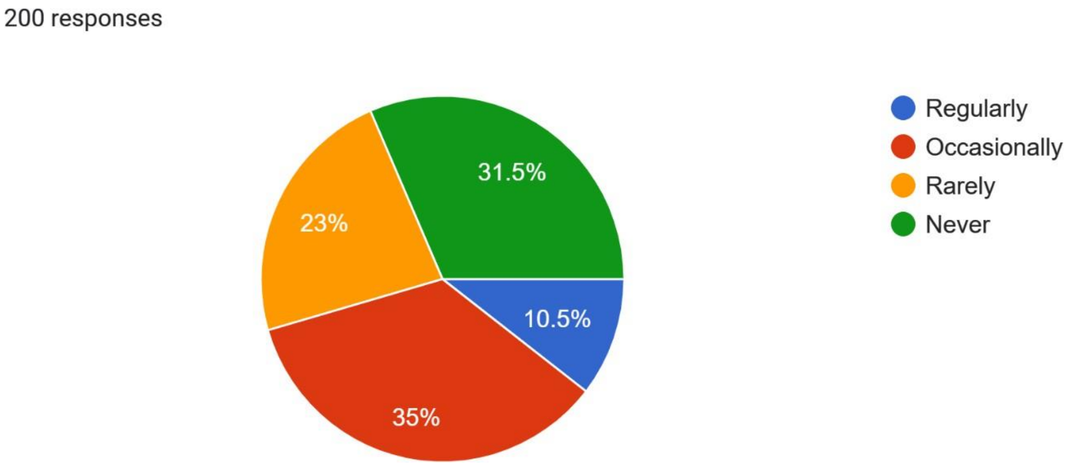

Figure 4

An essential component of both individual and corporate cybersecurity is password security. Changing passwords regularly is generally advised as a safeguard against data breaches and illegal access. The ideal frequency of password changes, which strikes a balance between user convenience and security requirements, is still up for discussion. This research aims to investigate how people and organizations now go about changing their passwords and what their thoughts are on the subject.

Frequency of Changing Passwords:

- **35%** of participants stated they **occasionally** change their passwords.
- **31.5%** of users **never** update their passwords.
- **23% seldom** update their passwords.
- **10.5%** of users **regularly** update their passwords.

The frequency with which people and organizations change their passwords varies greatly. Some combine security requirements with user convenience and practicality, while others favor frequent updates for increased security. Effective password security techniques must address issues like memorability and managing various passwords, as well as comprehend the motivations behind password changes. For organizations to maintain strong cybersecurity procedures without placing an undue burden on users, password policies should be customized based on risk assessments, industry norms, and user requirements.

Q8. Are all your electronic devices synchronized?

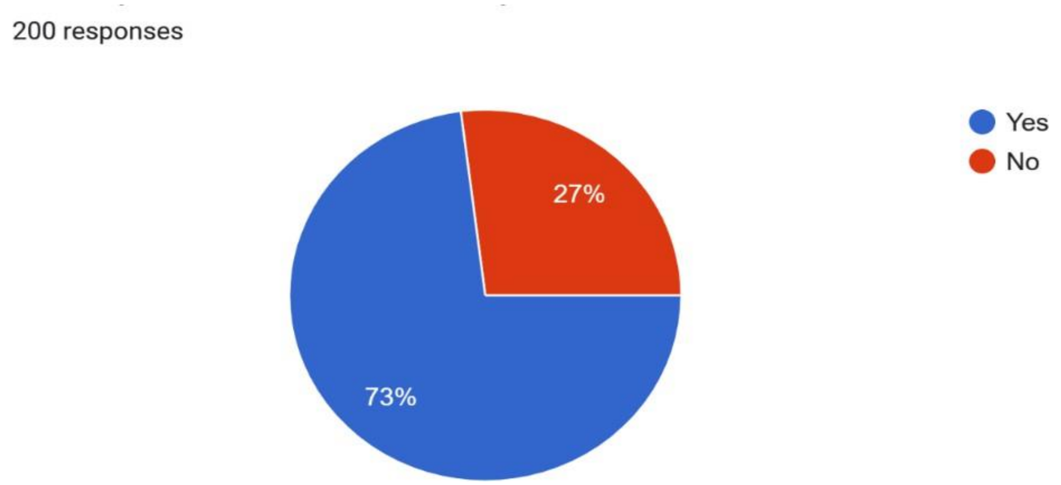

Figure 5

As per the report, it has been indicated that **73%** of individuals have synchronized all their electronic devices.

Synchronizing electronic devices has become progressively popular in modern society. With the proliferation of smartphones, tablets, laptops, and smartwatches, users often desire seamless integration and synchronization across their devices. This report explores the various hurdles encountered by users when attempting to synchronize their electronic devices.

Compatibility Issues:

The main challenges user faces is unity issues between different devices and operating systems. Not all devices are designed to work smoothly with each other, leading to frustrations when attempting to synchronize data, such as contacts, calendars, and files.

Complexity of Setup:

Setting up synchronization between multiple devices can be a daunting task, particularly for users who are not tech-savvy. Configuring settings, installing software, and troubleshooting connectivity problems require a certain level of technical knowledge, which many users may lack.

Data Security Concerns:

Synchronizing electronic devices raises concerns about data security and privacy. Users may worry about the security of their personal information when transferring it between devices, especially if the synchronization process involves storing data on third-party servers or cloud services.

Data Loss Risks:

Despite the convenience of synchronization, there is always a risk of data loss during the process. Technical glitches, software errors, or accidental deletions can result in the loss of important data, such as documents, photos, or messages if proper backup measures are not in place.

Syncing Delays and Inconsistencies:

Users may experience delays or inconsistencies when synchronizing data between their devices. Changes made on one device may not immediately reflect on another, leading to confusion and inefficiencies, particularly in collaborative work environments where real-time updates are crucial.

Dependency on Internet Connectivity:

Synchronization often relies on internet connectivity, which can be unreliable in certain situations. Users may encounter difficulties synchronizing their devices when experiencing poor network coverage or when offline, limiting their ability to access and update synchronized data.

Cross-Platform Limitations:

Users who own devices running different operating systems, such as iOS, Android, Windows, or macOS, may encounter challenges when attempting to synchronize them. Some synchronization solutions are platform-specific, making it difficult to achieve seamless integration across diverse device ecosystems.

Limited Integration Options:

While many electronic devices offer built-in synchronization features, they may have limited integration options with third-party services or applications. Users may find synchronizing data between their devices and preferred productivity tools or software solutions challenging, leading to workflow inefficiencies.

Synchronizing electronic devices offers numerous benefits in terms of convenience, accessibility, and productivity. However, users must navigate various challenges, including compatibility issues, setup complexity, data security concerns, and synchronization delays. Addressing these threats requires ongoing technological advancements, improved interoperability standards, and user-friendly synchronization solutions to establish a seamless and secure user experience across all electronic devices.

Q9. In which areas of your work do you regularly use a computer? Please select all that apply.

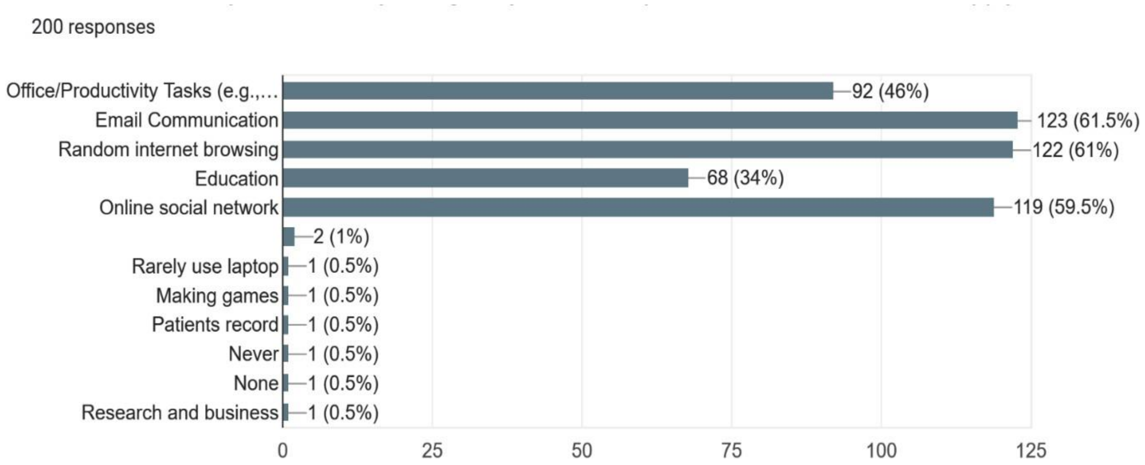

Figure 6

Computers have become an indispensable tool in the modern workplace, facilitating numerous tasks across different domains. This examines the prevalent usage of computers in various work areas, including office productivity tasks, email communication, random internet browsing, education, online social networking, etc. Understanding the handling of computer usage across these domains provides judgment into how technology influences work practices and communication patterns.

- Office Productivity Tasks: Computers are widely used in this field, with software packages such as Microsoft Office, Google Workspace, and specialized applications tailored to specific industries. About **46%** of respondents regularly use computers.
- Email communication: Email communication remains a fundamental aspect of modern business correspondence, facilitating internal communication among colleagues, external communication with clients and partners, and the dissemination of information. **61.5%** of respondents regularly use computers for email communication.

Computers are an integral part of various work fields, facilitating office tasks, email communication, leisure surfing, education, online social networking, and more. The maximum interview rate is H. Nearly **61.5%** and **61%** of respondents regularly use computers for email communication and casual surfing, respectively, while **59.5%** frequently use computers for online social networking.

Q10. Safe/Unsafe use of computer according to you.

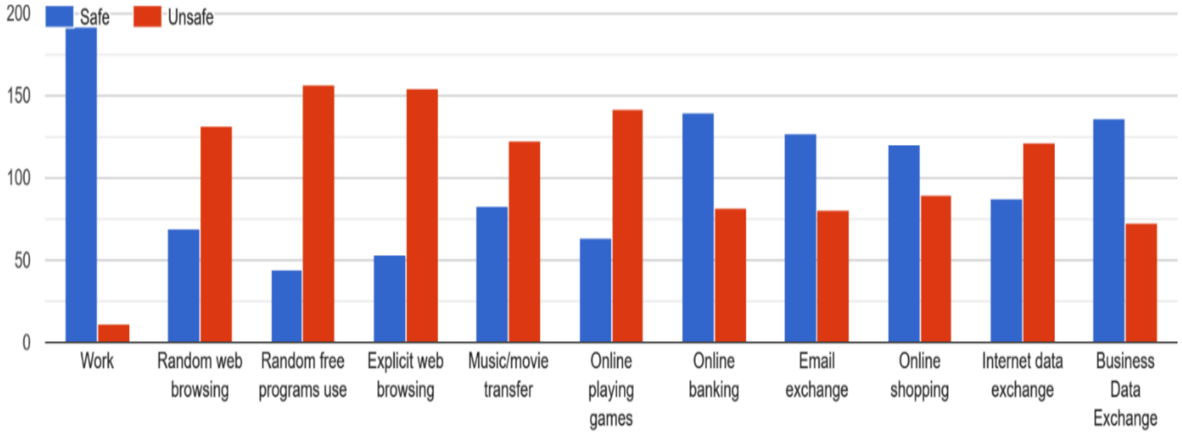

Figure 7

In the contemporary digital world, ensuring the safety and security of online activities such as work, online banking, and business data exchange has become of paramount importance. In this report, we delve into the perceptions of individuals concerning the safety/threat of these activities.

FINDINGS:

A. SAFETY

1. WORK:

The survey outcome shows that most participants trust the safety of performing work-related tasks online. This trust is a consequence of the following factors:

a) Implementation of strong and reliable security measures by employers.
b) Regular software and system updates and patches.
c) Awareness and training programs on cybersecurity practices.

2. ONLINE BANKING:

Respondents perceived online banking as safe due to two-factor authentication, biometric verification, encryption of data during transmission, and monitoring systems for suspicious activities.

3. BUSINESS DATA EXCHANGE:

The respondents have expressed a favorable perspective of the security measures for exchanging business data online. The key factors that have contributed to this positive perception include the implementation of secure file transfer protocols, encrypting sensitive information, and compliance with data protection regulations, such as GDPR and HIPAA.

The outcome of this survey reveals that the respondents have demonstrated a high level of confidence in the safety of performing work-related activities, online banking, and exchanging business data online. However, it is imperative to continuously monitor and update security measures to proactively address evolving cyber threats and ensure the continued safety of these digital interactions.

B. THREAT

In the digital age, online activities have become an intrinsic part of daily life. However, concerns about cybersecurity and safety persist, particularly regarding certain activities like random free program use, explicit web browsing, and online gaming. This report aims to analyze the perceptions of respondents regarding the safety of these activities based on a recent survey.

1. **RANDOM FREE PROGRAM USE:**
   a) Many respondents rated random free program use as unsafe.
   b) Concerns included the risk of malware, viruses, and potential data breaches.
   c) Many respondents expressed hesitation due to the inadequacy of accountability and verification associated with free programs.

2. **EXPLICIT WEB BROWSING:**
   a) A high number of respondents deemed explicit web browsing as unsafe.
   b) Concerns primarily centered around exposure to inappropriate content, malware, and the potential for legal repercussions.
   c) Some respondents highlighted the psychological impact of explicit material and its potential to desensitize individuals.

3. **ONLINE GAMING:**
   a) Respondents considered online gaming as unsafe.
   b) Safety concerns included exposure to cyberbullying, phishing attempts, and potential for addiction.
   c) Several respondents also mentioned worries about personal information exposure during online gaming sessions.

The findings suggest a prevalent perception among respondents that engaging in random free program use, explicit web browsing, and online gaming poses significant safety risks. These concerns are multifaceted and encompass both technological and psychological aspects. The fear of malware, exposure to inappropriate content, and risks associated with online interactions were recurring themes across all three activities.

In conclusion, the survey highlights widespread apprehension regarding the safety of certain online activities. As technology continues to evolve, individuals must adopt proactive measures to alleviate risks associated with these activities. Moreover, policymakers and digital platforms should prioritize user safety and implement robust measures to safeguard users from potential harm.

Q11. Do you through the terms & conditions of a software/application before signing in?

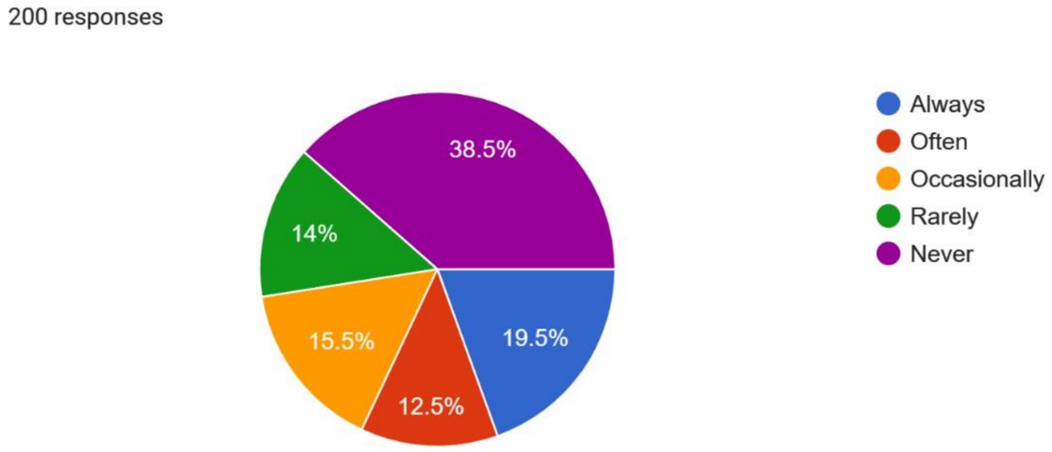

Figure 8

Software programs are becoming an essential element of everyday life in the digital age, both individually and professionally. Software is utilized by both individuals and organizations to improve efficiency and simplify processes. This includes social networking platforms and productivity applications. But in the rush to use new software, terms and conditions are frequently disregarded or approved quickly. This study examines the importance of understanding software terms and conditions through to the end and emphasizes the consequences of skipping this important step.

- **Comprehending Legal Responsibilities:** The terms and conditions of software specify the legal arrangement between the program provider and the user, including roles, obligations, and restrictions. Users can learn about their legal responsibilities for software usage, licensing, and intellectual property rights by carefully reading these terms.

- **Data Security and Privacy:** The privacy policy, which controls the gathering, storing, and use of user data, is one of the most important components of software terms and conditions. Users can learn how their personal information is handled, if it is stored securely, and whether it is shared with third parties by reading this section.

- **Usage Restrictions and Forbidden Activities:** To guard against improper use or abuse of the platform, software terms and conditions frequently include usage restrictions and forbidden activities. Users can make sure they are abiding by permissible usage norms and steer clear of actions that might go against the law or morality by carefully reading these terms. Hacking and the unapproved sharing of copyrighted content are examples of common limitations.

In conclusion, it is critical to read software terms and conditions before signing or accepting them to comprehend legal responsibilities, safeguard data privacy and security, adhere to usage constraints, efficiently manage licenses, and remain updated about upgrades or adjustments. Ignoring this crucial step could put consumers at risk for legal trouble, privacy violations, and unanticipated outcomes. To reduce potential hazards and make educated decisions on software usage, people and organizations should give careful consideration to the terms and conditions of any program they use. However, large number of respondents **(38.5%)** to the study declared that they **never** read the software's terms and conditions.

Q12. How often do you receive a fake/spam call? Did you ever fall for it?

200 responses

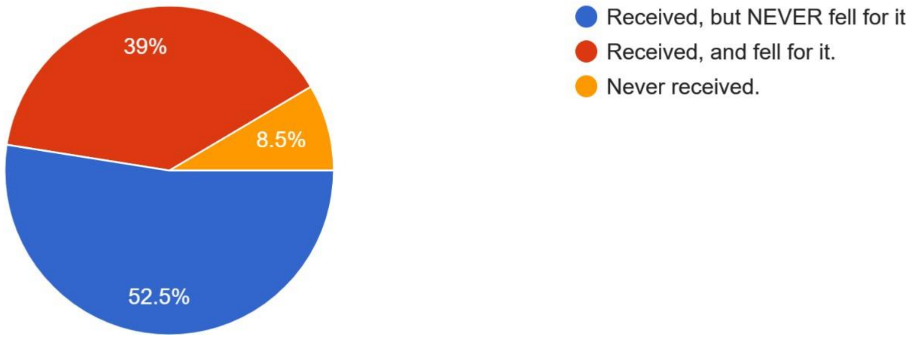

Figure 9

Scammers and fraudulent organizations frequently use fake calls, which continue to be a serious threat to people's financial security and privacy. The results of this survey aimed at determining the frequency of bogus calls and the percentage of participants who experienced them are shared in this report. The analysis seeks to clarify the consequences of answering phone calls and the precautions people might take.

Typical repercussions of answering bogus or spam calls include:

1. **Financial Losses:** Scammers may trick victims into giving their credit card numbers, bank account information, or money under pretenses, which can lead to financial losses.
2. **Identity Theft:** Phishing or fake calls intended to collect passwords or personal information, such as Social Security numbers, can result in identity theft and subsequent misuse of private information.
3. **Emotional Distress**: Falling for a bogus or spam call can leave recipients feeling vulnerable, embarrassed, and emotionally distressed—especially if they discover they have been duped.
4. **Compromised Security:** Giving scammers sensitive data or login credentials puts personal accounts, gadgets, and online profiles at risk of additional exploitation or illegal access.

The prevalence of fake calls is demonstrated by the fact that **39%** of respondents said they frequently received them and had been victims of them, while **52.2%** of respondents received them but did not fall for them. This suggests that the phenomenon is quite common.

The results of this survey highlight how commonplace bogus calls are and how much of an impact they have on people's mental health, financial stability, and privacy. Given that a significant percentage of respondents acknowledged falling for bogus calls, there is an immediate need for increased knowledge, instruction, and safeguards to reduce the dangers connected to this type of scamming. All parties involved may contribute to the creation of a more secure and safe telecom environment by providing people with the information and resources they need to recognize and steer clear of fraudulent calls.

Q13. Have you or someone you know ever been a victim of cybercrime?

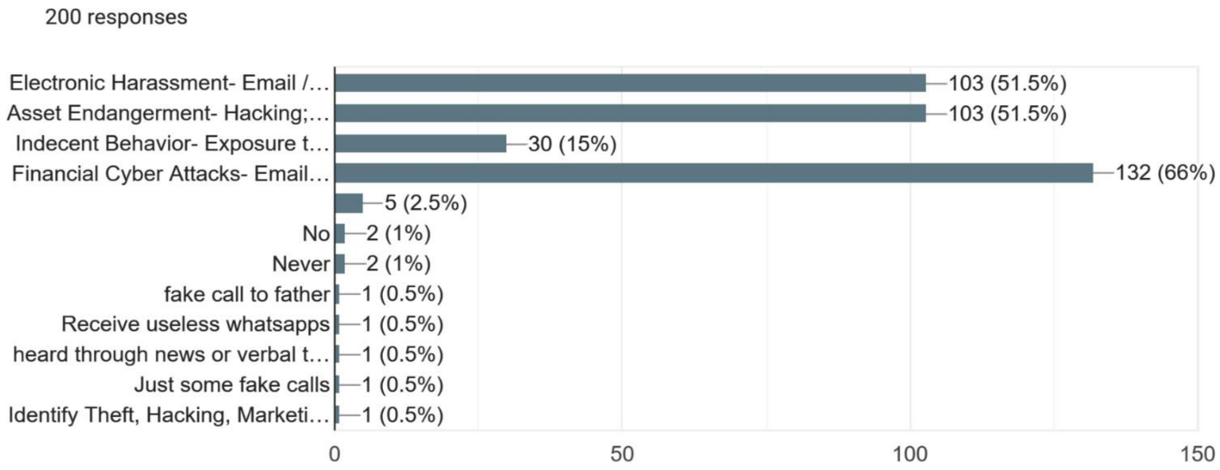

Figure 10

Globally, cybercrime is a serious threat to people and businesses. Financial cyberattacks, asset endangerment, and electronic harassment are some of the most prevalent forms of cyber threats.

Financial Cyberattacks: These included attack categories along with a broad spectrum of fraudulent actions targeted at obtaining confidential financial data, stealing money, or, conducting identity theft. **66%** of the respondents have been the victims of Financial Cyberattacks.

In the age of technology, financial cyberattacks, asset endangerment, and electronic harassment pose serious risks to people and businesses. These cybercrimes affect their victims' psychological well-being, reputations, and security in addition to monetary losses. Individuals and companies need to implement proactive cybersecurity measures, like frequent software upgrades, strong password management, and cybersecurity best practices training for staff members, to reduce the dangers connected with cybercrime. In addition, effective cybercrime combat and maintaining the safety and security of online communities depend on cooperation between law enforcement organizations, cybersecurity specialists, and technology suppliers.

Q14. How would you rate your awareness/knowledge of cybercrime and cybersecurity issues?

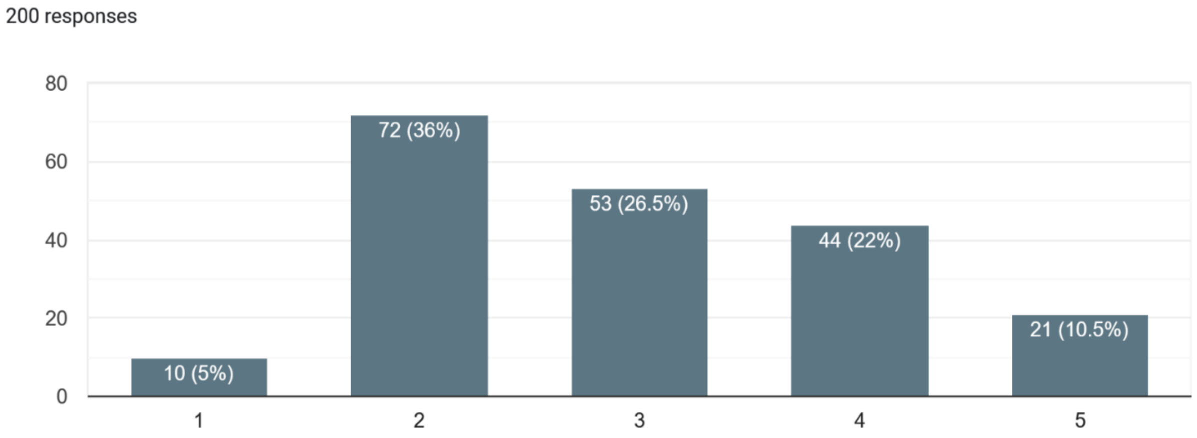

Figure 11

Through the administration of surveys to a wide sample of people across various demographics, including age, occupation, and educational background, the awareness of cybercrime and cybersecurity issues was assessed. Questions about participants' understanding of cybersecurity procedures and cybercrime were posed to them. Data on awareness and knowledge levels were analyzed. Overall, the results show that **36%** of respondents' knowledge of cybersecurity concerns and cybercrime is minimal, with several areas in need of improvement.

❖ <u>CYBERCRIME CAUSES</u>

Q15. What, in your opinion, are the main motivations behind individuals engaging in cybercriminal activities?

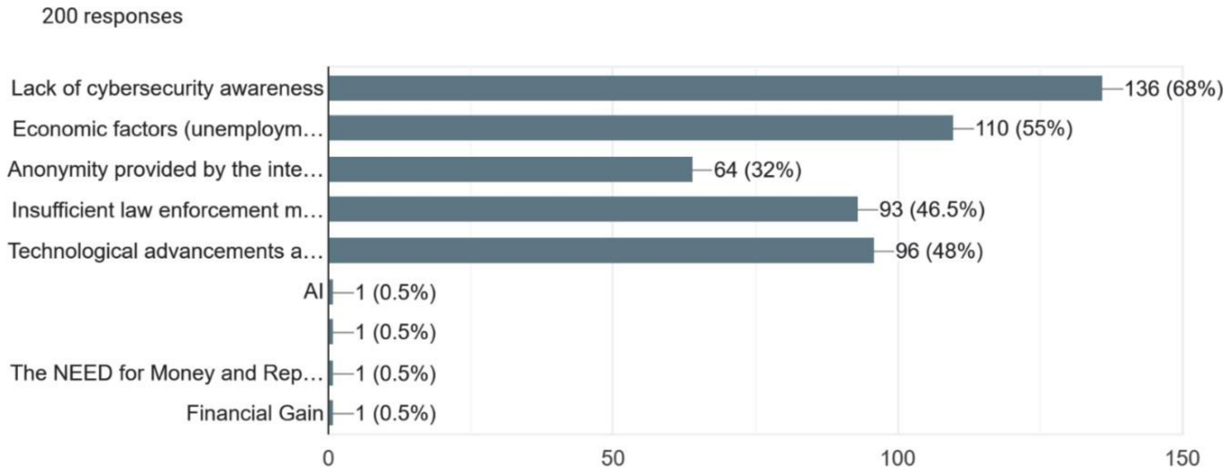

Figure 12

In the digital age, cybercrime has grown in frequency as people take advantage of loopholes in technology and online platforms to commit crimes. Developing successful strategies to counter cyber risks requires an understanding of the motivations behind people's engagement in cybercrime. The primary drivers of cybercrime are examined in this paper, including a lack of knowledge about cybersecurity, economic factors, a lack of adequate law enforcement, and technological improvements.

1. **Lack of Cybersecurity awareness:** One of the main causes of the rise in cybercrime is a lack of awareness regarding cybersecurity. Many people are still innocent about typical cyber threats, defense strategies, and the possible repercussions of their online behavior. Due to their ignorance, people are more likely to become victims of cyberattacks or inadvertently engage in illegal actions like phishing schemes, virus distribution, and identity theft. It is imperative to bridge the knowledge gap by employing education, training, and awareness efforts to enable citizens to safeguard themselves and deter cybercrime. **68%** of respondents believe that lack of cyber security awareness is the main motive behind cybercriminal activities.

2. **Economic Factors:** Since cybercrime can be extremely profitable with minimal risk of detection and prosecution, many people are motivated by financial concerns to engage in abusive actions. Cybercriminals may target companies, financial institutions, or citizens to steal cash, private data, or priceless items. Cybercrime's black market thrives on the selling of hacking tools, stolen data, and illegal services, providing rich opportunities for individuals who are willing to take advantage of technology flaws for personal benefit. Cybercrime is ubiquitous in the digital world because of factors including unemployment, economic inequality, and the desire for quick profits. **55%** of all respondents believe that economic factors are the primary reason behind cybercriminal activities.

3. **Inadequate Law Enforcement:** Cybercriminals can operate with impunity in an environment where law enforcement is insufficient or lacking, which in turn leads to the spread of cybercrime. Cybercriminals operate internationally, taking advantage of legal loopholes and jurisdictional complexity to avoid detection and prosecution. Effective measures to counter cyber threats are hampered by law enforcement agencies' lack of coordination and collaboration, which gives cybercriminals less reason to worry about the repercussions of their actions. Deterring cybercrime and holding offenders liable for their conduct requires bolstering international collaboration, improving legal frameworks, and investing in law enforcement capabilities.

4. **Technological Advancements:** These developments have made it easier for cybercriminals to commit crimes and have opened-up new avenues for creativity in cybercrime. Technological advancements, such as anonymization tools, encryption methods, and cryptocurrency, allow attackers to successfully disguise their identities, avoid detection, and launder money obtained through illegal means. Furthermore, the proliferation of internet-connected gadgets and the growing interconnection of digital ecosystems increase the attack surface available to hackers opening new channels for infiltration and exploitation. People who commit cybercrimes do so for array of reasons, including a lack of knowledge about cybersecurity, financial incentives, a lack of effective law enforcement, and advances in technology. A comprehensive strategy that includes increasing awareness, resolving socioeconomic inequities, bolstering law enforcement capacities, and keeping up with technological advancements is needed to address these underlying reasons.

Q16. How do you think socio-economic factors, such as income inequality and unemployment, may influence individuals to engage in cybercriminal activities?

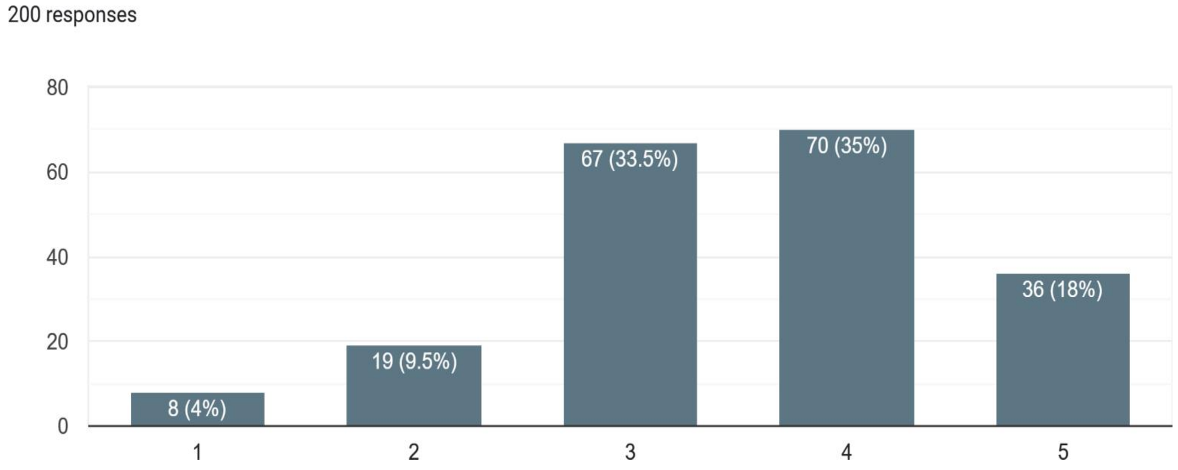

Figure 13

The intersection of socioeconomic factors and cybercrime is a multifaceted issue that involves individual circumstances, economic conditions, and technological opportunities. The purpose of this report is to examine how income inequality and unemployment may influence individuals' propensity to engage in cybercriminal activities. This analysis aims to shed light on the underlying motivations and dynamics driving cybercrime.

INCOME INEQUALITY AND CYBERCRIME

1. **INCOME DISPARITIES:**
   - Income inequality is a major concern, exacerbating existing disparities in access to resources and opportunities. This can create significant financial strain for marginalized communities and individuals.
   - For those with limited economic prospects, seeking alternative means of income generation may become necessary, including engaging in illicit activities such as cybercrime.
   - The potential for quick financial gains in the cyber realm may be especially alluring for those facing economic hardship and lacking legitimate employment options.

2. **MOTIVATION FOR CYBERCRIME:**
   - Economic motives are known to be significant drivers of cybercriminal behavior, with financial gain serving as the primary incentive for engaging in illicit activities.
   - Individuals who are experiencing financial distress or struggling to make ends meet may perceive cybercrime as a viable means of supplementing their income or overcoming socioeconomic barriers.

- Income inequality can foster a sense of relative deprivation, where individuals compare their economic standing to others and may resort to cybercrime as a means of achieving perceived parity or upward mobility.

UNEMPLOYMENT AND CYBERCRIME

1. **JOBLESSNESS AND UNEMPLOYMENT:** High levels of unemployment and underemployment can lead to negative consequences among segments of the population, such as feelings of frustration, disenchantment, and hopelessness. The absence of secure employment opportunities can result in social exclusion, diminished self-esteem, and a sense of alienation from mainstream society. In the absence of legitimate avenues for employment and advancement, some individuals may choose to engage in cybercrime as a way to assert agency, gain recognition, or exert control over their circumstances.

2. **PSYCHOLOGICAL FACTORS:** Unemployment can often lead to an increase in feelings of insecurity and anxiety, which can in turn create a sense of desperation and a willingness to take risks to improve one's financial situation. It is worth noting that the digital landscape can provide a sense of anonymity and perceived impunity, which may encourage some unemployed individuals to experiment with cybercriminal activities as a form of escapism or rebellion against societal norms.

Socio-economic factors such as income inequality and unemployment exert a multifaceted influence on individuals' propensity to engage in cybercrime. These factors create a fertile ground for exploitation, as individuals facing financial hardship and limited opportunities are more likely to resort to illicit online activities. Addressing the root causes of income inequality and unemployment requires comprehensive interventions that encompass economic empowerment, education, and social support systems. By tackling the underlying socioeconomic vulnerabilities and promoting inclusive economic growth, societies can mitigate the allure of cybercrime and foster greater resilience against digital threats. This approach can also help build more stable and prosperous communities.

❖ CYBERCRIME PREVENTION STRATEGIES

Q17. How confident are you in the effectiveness of current cybersecurity measures (e.g., firewalls, antivirus software) in preventing cybercrimes?

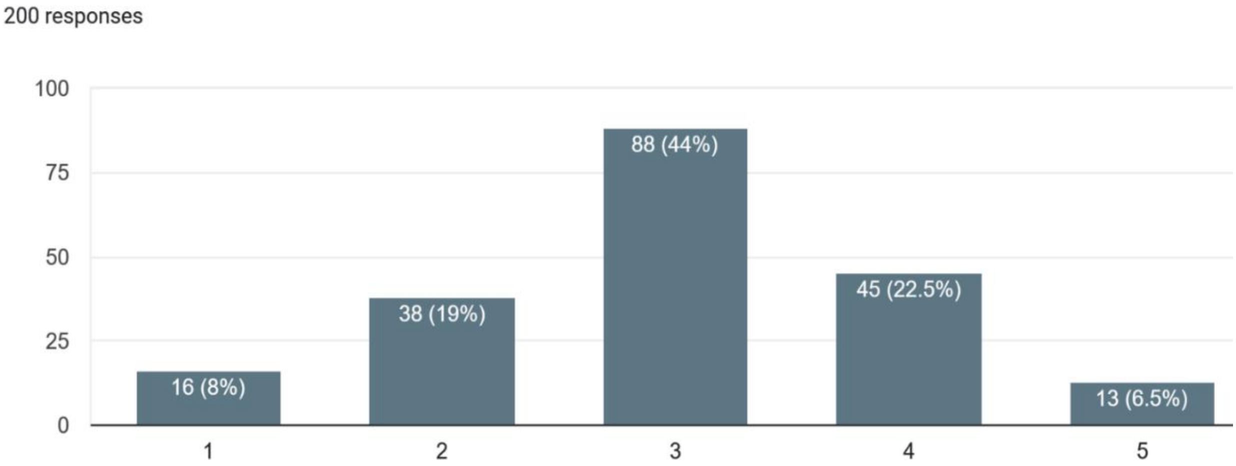

Figure 14

In today's modern era, cybersecurity is a paramount concern that demands the utmost attention from individuals and organizations alike. The protection of sensitive data from cyber threats is critical, and to ensure this, key components of cybersecurity measures such as firewalls, antivirus software, and other defense mechanisms are essential. The purpose of this report is to analyze the level of confidence of the respondents regarding the effectiveness of these measures in preventing cybercrimes. The findings of this report will help to provide insights into the current cybersecurity landscape and assist in developing strategies to mitigate the risks associated with cyber threats.

RESULTS

Confidence Levels:

- The survey revealed that majority of respondents expressed a **moderate level** of confidence in the effectiveness of current cyber security measures.
- Approximately **22.5%** of respondents rated their confidence **level at 4**, indicating a significant degree of trust in the protective capabilities of firewalls and antivirus software.
- Around **44%** of respondents rated their confidence **level at 3**, indicating a moderate level of confidence, while only a small minority **(8%)** expressed low confidence **(ratings of 1)**.

Overall, the survey findings suggest a substantial level of confidence among respondents in the ability of current cybersecurity measures to prevent cybercrimes. However, vigilance and proactive measures are necessary to address emerging threats effectively and ensure robust protection of sensitive data and digital assets.

This report provides valuable insights into the perceptions and attitudes of individuals towards cybersecurity measures, informing stakeholders about the current state of confidence and areas for potential improvement in cybersecurity strategies.

Q18. Do you think international collaboration and law enforcement efforts are essential in preventing and combating cybercrime?

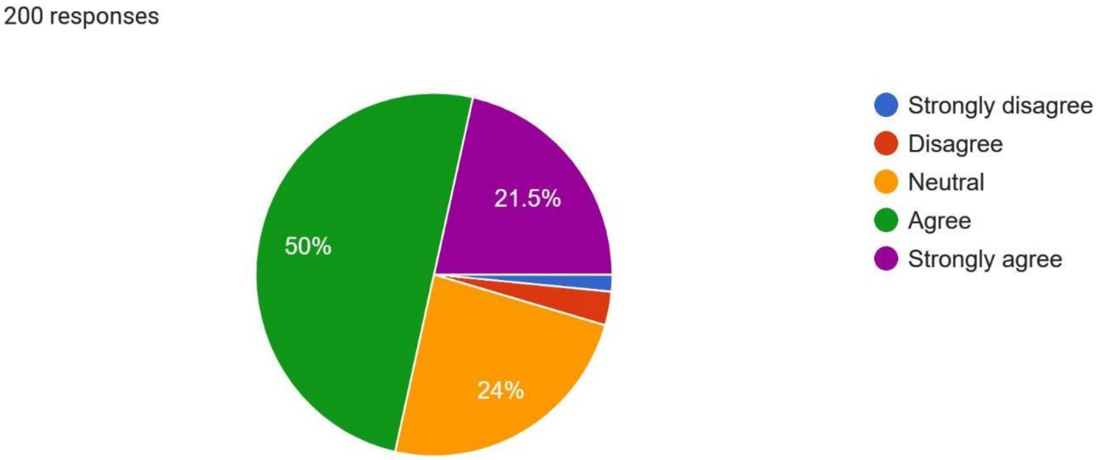

Figure 15

Cybercrime has become a permeant threat in the digital age, with individuals, businesses, and governments facing increasingly sophisticated attacks. In response to this growing menace, international collaboration and effective law enforcement efforts are seen as crucial pillars in the fight against cybercrime. This report presents findings from a survey conducted to gauge public sentiment on the importance of international collaboration and law enforcement in preventing and combating cybercrime.

1. **Overwhelming Consensus:**
   - **50%** of respondents agreed that international collaboration is essential in preventing and combating cybercrime.
   - **50%** of respondents emphasized the importance of coordinated law enforcement efforts across borders to combat cyber threats effectively.
2. **Trust in Law Enforcement:**
   - **50%** of respondents indicated that trust in law enforcement agencies, both domestic and international, is crucial for effective cybercrime prevention and prosecution.
   - **50%** of respondents expressed confidence in the ability of international law enforcement agencies to effectively tackle cybercrime when they work together.

The survey results underscore the widespread recognition of the importance of international collaboration and law enforcement efforts in addressing the complex challenges posed by cybercrime. With cyber threats transcending geographical boundaries, cooperation among nations, along with the establishment of robust legal frameworks, emerges as imperative in safeguarding cyberspace. As technology continues to evolve, fostering trust among stakeholders and promoting global partnerships will remain pivotal in the ongoing battle against cybercriminal activities.

Q19. To what extent do you believe cybersecurity education programs can reduce the risk of individuals and organizations falling victim to cybercrime?

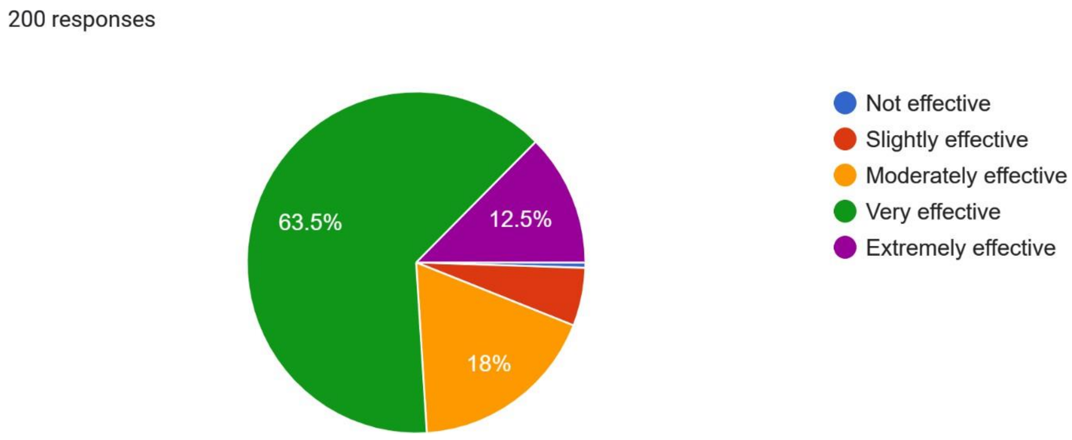

Figure 16

With the increasing prevalence of cybercrime, there is a growing recognition of the importance of cybersecurity education in mitigating risks for individuals and organizations. This report presents findings from a recent survey that sought to gauge respondents' beliefs regarding the effectiveness of cybersecurity education programs in reducing the likelihood of falling victim to cybercrime.

FINDINGS

1. **Agreement Levels:**
   - **63.5%** of respondents indicated agreement with the statement.
   - Only **0.5%** of respondents disagreed with the effectiveness of cybersecurity education programs.
   - **18%** of respondents remained neutral on the issue.

2. **Reasons for Agreement:**
   - Increased Awareness: Many respondents emphasized the role of cybersecurity education in raising awareness about common cyber threats and best practices for mitigating them.
   - Empowerment: Respondents highlighted that education programs empower individuals and organizations to recognize potential risks and take proactive measures to protect themselves.
   - Behavior Change: Several respondents noted that effective cybersecurity education can lead to behavioral changes, such as practicing better password hygiene and being cautious with online activities.

3. **Challenges and Opportunities:**

- Continuous Learning: Some respondents emphasized the need for ongoing education and training to keep pace with evolving cyber threats and technologies.
- Accessibility: A few respondents highlighted the importance of making cybersecurity education programs accessible to individuals from diverse backgrounds, including those with limited technical expertise.
- Collaboration: Several respondents suggested that collaboration between government agencies, educational institutions, and private sector organizations could enhance the effectiveness of cybersecurity education initiatives.

The overwhelming agreement among respondents regarding the effectiveness of cybersecurity education programs reflects a widespread recognition of their importance in combating cyber threats. Education serves as a foundational pillar in building a cyber-resilient society by empowering individuals and organizations with the knowledge and skills necessary to protect themselves against cybercrime.

In conclusion, the survey findings underscore the critical role of cybersecurity education in reducing the risk of individuals and organizations falling victim to cybercrime. As cyber threats continue to evolve, investing in comprehensive and accessible education programs is essential for fostering a cybersecurity-aware culture and enhancing overall resilience in the digital landscape. Collaboration among stakeholders is key to developing and implementing effective education initiatives that address the diverse needs of today's interconnected world.

Q20. What cybersecurity measures do you believe are most effective in preventing cybercrime? (Select all that apply)

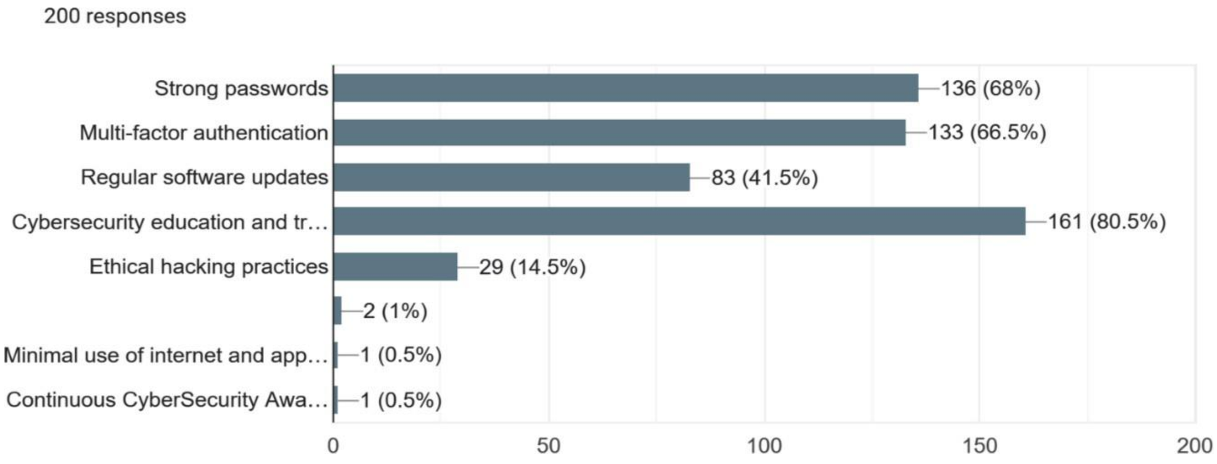

Figure 17

Cybercrime continues to pose a significant threat to individuals, businesses, and organizations worldwide. In response to this escalating challenge, various cybersecurity measures have been developed and implemented to mitigate risks and protect against cyber threats. This report analyzes the perceptions of respondents regarding the effectiveness of key cybersecurity measures in preventing cybercrime.

KEY FINDINGS

1. **Strong Passwords:**
   - **68%** of respondents believe that strong passwords are effective in preventing cybercrime. Strong passwords, characterized by their complexity and uniqueness, are considered a fundamental security measure for protecting accounts and sensitive information from unauthorized access.
2. **Multi-Factor Authentication (MFA):**
   - **66.5%** of respondents recognize the effectiveness of multi-factor authentication in enhancing cybersecurity. MFA adds a layer of security by requiring users to provide multiple forms of verification, such as passwords, biometrics, or security tokens, thereby reducing the risk of unauthorized access even if passwords are compromised.
3. **Regular Software Updates:**
   - **41.5%** of respondents acknowledge the importance of regular software updates in preventing cybercrime. Keeping software and operating systems up-to-date with the latest security patches and fixes is crucial for addressing vulnerabilities and strengthening defenses against cyber threats, including malware and exploits.

4. **Cybersecurity Education and Training:**
    - **80.5%** of respondents consider cybersecurity education and training to be highly effective in preventing cybercrime. Awareness and education initiatives aimed at promoting cybersecurity best practices, raising awareness about common threats, and fostering a culture of security-conscious behavior are viewed as essential components of comprehensive cybersecurity strategies.

The survey findings underscore the widespread recognition of cybersecurity measures as vital tools in the ongoing battle against cybercrime. While strong passwords, multi-factor authentication, regular software updates, and cybersecurity education and training are acknowledged for their efficacy, there remains room for improvement in promoting awareness and adoption of these measures across individuals, organizations, and society. Continued efforts to enhance cybersecurity practices, coupled with ongoing education and awareness initiatives, are essential for bolstering defenses and mitigating the risks posed by cyber threats in an increasingly interconnected digital landscape.

Q21. How much responsibility do you believe governments have in preventing cybercrime?

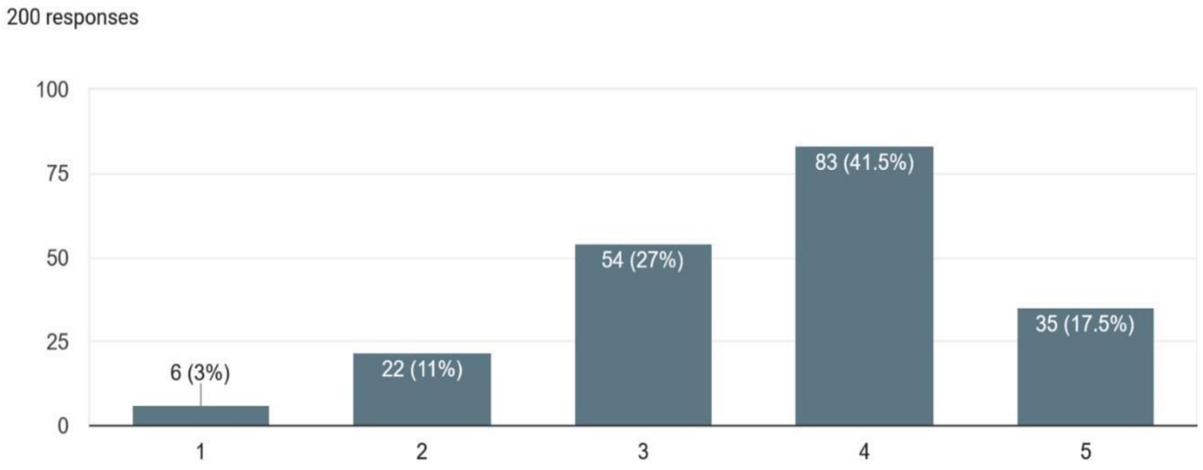

Figure 18

In the current digital era, cybercrime presents a significant threat to individuals, businesses, and national security. As the primary custodians of public safety and welfare, governments are entrusted with a crucial role in preventing and mitigating cyber threats. This report states that **41.5%** of the respondents believe that the government has a high extent of responsibility in combating cybercrime.

Government Responsibility in Preventing Cybercrime:

1. **Legislative Frameworks:** Governments are responsible for enacting and enforcing robust cybersecurity legislation that establishes clear guidelines and penalties for cybercriminal activities. These legislative measures should encompass a wide range of issues, including data protection, privacy rights, cyber fraud, intellectual property theft, and critical infrastructure protection.
2. **Law Enforcement:** Governments must equip law enforcement agencies with the necessary resources, training, and technological capabilities to investigate and prosecute cybercriminals effectively. Collaboration between national and international law enforcement entities is essential for combating transnational cyber threats and extraditing offenders across borders.
3. **Cybersecurity Education and Awareness:** Governments play a pivotal role in promoting cybersecurity education and awareness initiatives to empower individuals, businesses, and government agencies to recognize and mitigate cyber risks. Public awareness campaigns, cybersecurity training programs, and educational outreach efforts are instrumental in fostering a culture of cyber resilience and responsible online behavior.
4. **Public-Private Partnerships:** Governments should foster collaboration between the public and private sectors to share threat intelligence, best practices, and resources for enhancing cybersecurity resilience. Public-private partnerships enable the joint development of cybersecurity strategies, incident response plans, and infrastructure protection measures to safeguard critical systems and networks.

5. **International Cooperation:** Given the global nature of cyber threats, governments must engage in international cooperation and diplomatic efforts to address cybercrime on a multilateral scale. Participation in international forums, conventions, and treaties facilitates information sharing, capacity building, and mutual assistance in combating cyber threats across borders.

The prevention of cybercrime is a shared responsibility that requires concerted efforts from governments, private sector stakeholders, civil society organizations, and individual users. While governments bear a significant burden in establishing legal frameworks, law enforcement capabilities, and cybersecurity governance structures, collaboration and partnership with other stakeholders are essential for achieving meaningful impact. By adopting a comprehensive approach that integrates legislation, enforcement, education, partnerships, and international cooperation, governments can effectively address the evolving challenges posed by cybercrime and safeguard the digital infrastructure of society.

Q22. Fear of cybercrime

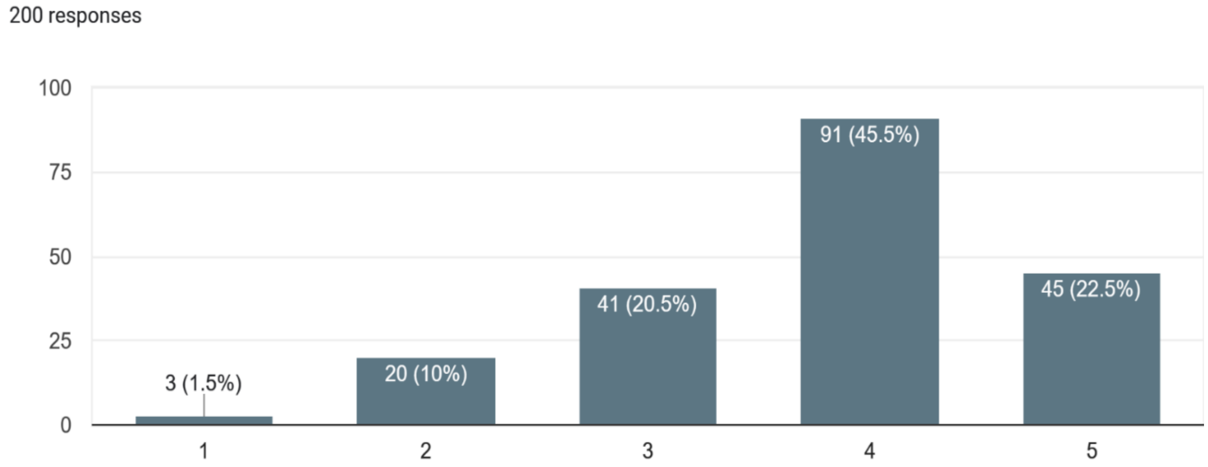

Figure 19

In the current age, digital technologies have become an integral part of our daily lives, and with this integration comes increasing concern about cybercrime. To gain insight into the public's perceptions and attitudes towards cyber threats, a comprehensive survey was conducted. The purpose of this report is to provide a summary of the survey findings and offer insights into prevailing attitudes toward cybercrime.

KEY FINDINGS

1. **High levels of fear:** According to the survey, **45.5%** of people are scared and worried about cybercrime. Participants expressed concerns about being a victim of cyber-attacks, which shows that people are fearful about online security.
2. **Perceived vulnerability:** Most of the respondents felt that they were at risk of cyber threats such as hacking, identity theft, phishing, and malware attacks. This perception of vulnerability highlights the recognition of potential risks associated with online activities.
3. **Financial concerns:** Financial security is a primary concern among respondents, with over **66%** expressing apprehension about financial losses resulting from cybercrime. The fear of unauthorized access to bank accounts, credit card fraud, and online scams ranked high among the concerns voiced by participants.

The results of the survey demonstrate the prevalence of fear and apprehension among the general population about cybercrime. It is noteworthy that overwhelming majority of individuals express concerns about online security and their perceived vulnerability to cyber threats. This highlights the urgent need for enhanced measures to address the growing challenges posed by cybercrime. To develop effective cybersecurity strategies, it is critical to prioritize not only technological solutions but also efforts to educate and empower individuals to protect themselves against online risks. By fostering greater awareness and collaboration, stakeholders can work towards building a safer and more secure digital environment for all.

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 on 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 opinions, preferences, and behaviors of the target audience. These findings can be utilized for decision-making processes, refine preventive strategies, and improve the overall offering to meet the needs and expectations of people better.

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.

- 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:

- 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 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.

REFERENCES

1. Park, H., Cho, S., & Kwon, H.-C. (2009). *Cyber Forensics Ontology for Cyber Criminal Investigation* (Vol. 8). http://www.netan.go.

2. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

3. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

4. Bhagwani, V., & Balasinorwala, S. (2023). CYBER SECURITY. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, *07*(02). https://doi.org/10.55041/IJSREM17691

5. *View of Combating Cybercrime: A Study on Problems, Preventions and Cyber Laws of India*. (n.d.). Retrieved April 26, 2024, from https://www.eelet.org.uk/index.php/journal/article/view/1220/1063

6. Office Science, H. (2013). *Cyber crime: A review of the evidence Research Report 75 Cyber crime: A review of the evidence*.

7. Das, S., & Nayak Asst-Prof, T. (2013). IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES. In *International Journal of Engineering Sciences & Emerging Technologies* (Vol. 6, Issue 2).

8. Lapuh Bele, J., Dimc, M., Rozman, D., & Sladoje Jemec, A. (2014). *Raising awareness of cybercrime-The use of education as a means of prevention and protection*. https://www.researchgate.net/publication/291317388

9. Ramdinmawii, E., Ghisingh, S., & Sharma, U. M. (n.d.). *A Study on the Cyber-Crime and Cyber Criminals: A Global Problem*.

10. Prasanthi, M. M. L. (2015). Cyber Crime: Prevention & Detection. *IJARCCE*, 45–48. https://doi.org/10.17148/ijarcce.2015.4311

11. Shah, J. (n.d.). A Study of Awareness About Cyber Laws for Indian Youth. In *International Journal of Trend in Scientific Research and Development* (Vol. 1, Issue 1). www.ijtsrd.com

12. Mohd Ali, M. (2015). Determinants of Preventing Cyber Crime: a Survey Research. *International Journal of Management Science and Business Administration*, *2*(7), 16–24. https://doi.org/10.18775/ijmsba.1849-5664-5419.2014.27.1002

13. Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change*, *66*(3), 313–338. https://doi.org/10.1007/s10611-016-9629-3

14. AISSMS Institute of Information Technology, & Institute of Electrical and Electronics Engineers. (n.d.). *2020 International Conference on Emerging Smart Computing and Informatics (ESCI) : AISSMS Institute of Information Technology, Pune, India. Mar 12-14, 2020.*

15. Abinanth, K. (n.d.). *A STUDY OF AWARENESS OF CYBER CRIME AMONG COLLEGE STUDENTS WITH SPECIAL REFERENCE TO KOCHI*. http://www.acadpubl.eu/hub/

16. *CYBERCRIME CATEGORIES AND PREVENTION 1 Manishaben Jaiswal*. (2019). www.ijcrt.orgwww.ijcrt.org

17. Muhammad Suleiman, M., Abdurrahman Anas, A., & Jafaru, A. (n.d.). Prevention And Detection Measures Against Cybercrimes Attack. *International Journal of Research Available*. https://journals.pen2print.org/index.php/ijr/

18. Sviatun, O. V., Goncharuk, O. V., Chernysh, R., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: Economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751–762. https://doi.org/10.37394/23207.2021.18.72

19. *PREVENTION OF COMPUTER CRIME THROUGH KNOWLEDGE OF THE CONCEPT OF CYBER SECURITY*. (n.d.). https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

20. Veena, K., Meena, K., Kuppusamy, R., Teekaraman, Y., Angadi, R. V., & Thelkar, A. R. (2022). Cybercrime: Identification and Prediction Using Machine Learning Techniques. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/8237421

21. Golam, M., & Sarker, R. (n.d.). *An Interlinked Relationship between Cybercrime & Digital Media*. www.ijfmr.com

22. The Sang, N., & Bao Trung, B. (n.d.). Cybercrime in the Digital Age: Challenges and Implication for Prevention. *International Journal of Social Science And Human Research*. https://doi.org/10.47191/ijsshr/v5-i11-36

23. Turaev, S. A. (2022). CRIMES COMMITTED USING THE INTERNET: CAUSES AND CONDITIONS. *Oriental Journal of Social Sciences*, *02*(01), 97–108. https://doi.org/10.37547/supsci-ojss-02-01-12

24. Bhagwani, V., & Balasinorwala, S. (2023). CYBER SECURITY. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, *07*(02). https://doi.org/10.55041/IJSREM17691

25. Qu, S. (2023). Causes for Public Figures to Experience Cyber Violence and Prevention Measures. In *BCP Social Sciences & Humanities ASSSD* (Vol. 2022).