



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN



WHITE BLACK
LEGAL.

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.



WHITE BLACK
LEGAL

EDITORIAL **TEAM**

Raju Narayana Swamy (IAS) Indian Administrative Service **officer**



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru

and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

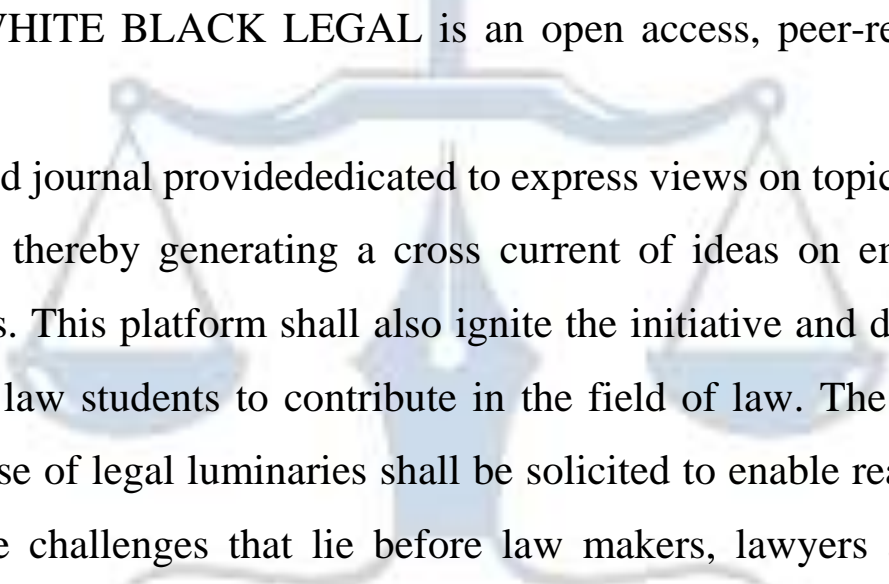


Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

FROM BYTES TO THREATS: UNMASKING CYBER-CRIMES TRENDS

AUTHORED BY - MITHIL GOYAL & NITIN GUPTA

Abstract

There are almost 8.5 billion searches on Google in one day and approximately 2 trillion searches all across the globe. This is only for search engines and Google itself. In this digital contemporary era, the Internet users are expanding tremendously. These digital societies are becoming unbound, unprecedented and unknown with enlarging crimes. This paper is an in-depth analysis into cybercrimes. This research study comprises the introduction to cybercrime, different cybercrimes, cyber laws in India (IT Act 2000), evolution of cybercrimes, challenges, government action and future uncertainties. It includes a quantitative offline and online survey with analysis of the results augmenting the interview of officials. This research focuses more on the challenges, perception, awareness and trends of cybercrimes and cyber security in Punjab and Chandigarh.

Key words: Cyber Crime, Espionage, Doxing, Sextortion, Hacking, IT Act 2000

Introduction

Cybercrime in the present scenario has become a necessary evil, acting as a deterrent against over-sharing and careless behavior on the internet. Without the fear of cybercrime, people might continue to use online platforms indiscriminately, ignoring potential risks and side effects. The threat(s) vis-vis financial fraud, theft of identity and personal data breaches encourages users to be more vigilant about their online activities and privacy. While the rise in cybercrime is alarming, it also serves as a wake-up call, emphasizing the importance of cyber security measures and responsible online behavior. In response to the growing trends of cybercrime, various countries, including India, have implemented stringent cyber laws to protect individuals and organizations. India's legal framework for addressing cybercrime includes several key regulations and acts, primarily centered around the Information Technology Act, of 2000 (IT Act 2000). This act was a landmark in the realm of Indian cyber law and has undergone several amendments to address the evolving nature of cyber threats.

Meaning -

But before that, we need to understand what Cybercrime is, also known as computer crime or cyber fraud, refers to illegal activities that involve the use of computers, networks, or the internet. These activities can target individuals, organizations, or governments, ranging from financial fraud to hacking and data theft. Cybercrime encompasses a broad spectrum of offences, including but not limited to:

1. **Hacking**: Illegal access to computer systems or networks i.e. without any authorization/ permission in order to steal, manipulate, or destroy data.
2. **Identity Theft**: Breach of privacy and dignity by way of theft of personal information such as Social Security numbers, credit card details, or other personal identifiers to commit fraud.
3. **Phishing**: Using deceptive emails, websites, or messages with the intent to deceive or induce individuals into sharing sensitive information like passwords or financial details.
4. **Malware**: Creating and distributing malicious software such as viruses, worms, ransom ware and spyware to damage or gain unauthorized access to computer systems.
5. **Online Fraud and Scams**: Conducting fraudulent activities online to deceive individuals or organizations, including e-commerce fraud, auction fraud, and investment scam.
6. **Cyber stalking and Harassment**: Using the internet or other digital means to harass, threaten, or stalk individuals.
7. **Child Exploitation**: Distributing, producing, or possessing child pornography, or exploiting children through online platforms.
8. **Cyber Terrorism**: Using cyber-attacks to instill fear, cause harm, or disrupt critical infrastructure, often for political or ideological purposes.

9. **(DoS) Attacks:** Unbridled loading of networks to make them unavailable to users, often disrupting services or operations.
10. **Intellectual Property Theft:** Stealing or infringing on copyrighted materials, patents, trade secrets, and other intellectual property through digital means.

The Key Provisions of the IT Act (2000) –

1. **Legal Recognition of Electronic Transactions:** The IT Act 2000 provides legal recognition for electronic transactions, making electronic contracts and digital signatures legally valid.
2. **Offences and Penalties:** The Act defines various cybercrimes and prescribes penalties for offences such as hacking, identity theft, cyber terrorism, and the distribution of obscene material. Notable sections include:
 - Section 66: Deals with computer-related offences, including hacking and data theft.
 - Section 66C: Pertains to identity theft and fraudulent use of electronic signatures.
 - Section 66D: Addresses cheating by personation using computer resources.
 - Section 67: Punishes the publishing or transmission of obscene material in electronic form.
3. **Adjudication and Redressal Mechanisms:** The Act establishes a framework for adjudication of cyber disputes and the appointment of adjudicating officers to resolve such issues. The Cyber Appellate Tribunal is also set up for appeals.
4. **Data Protection and Privacy:** Amendments to the IT Act have introduced provisions for data protection and privacy, holding organizations accountable for securing personal data and sensitive information.

5. **Cyber Terrorism:** Section 66F addresses cyber terrorism, making it a punishable offense to threaten the sovereignty, integrity, or security of India through cyber activities.

Recent Developments and Enhancements -

In addition to the IT Act, other initiatives and laws have been introduced to strengthen cyber security in India:

1. **Personal Data Protection Bill:** A comprehensive bill aimed at protecting personal data and regulating its processing by both government and private entities. It emphasizes consent, transparency, and accountability in data handling.
2. **CERT-In (Indian Computer Emergency Response Team):** Established under the IT Act, CERT-In is responsible for responding to cyber security incidents, providing incident prevention and response services, and enhancing the overall security of India's internet domain.
3. **National Cyber Security Policy (2013) -** This policy outlines a framework for ensuring cyberspace security in India, promoting a secure and resilient cyber environment, and encouraging collaboration between various stakeholders.

Literature Review

The literature on cybercrime in India is rich and varied, with numerous books providing in-depth analyses of different aspects of cybercrime, its impact, and the legal framework in place to combat it. This review explores some of the key books on the subject, highlighting their contributions to understanding the nature of cybercrime in India, the socio-economic consequences, legal challenges, and possible solutions.

Key Books on Cybercrime in India –

1. **"Cyber Law in India" by Farooq Ahmad –**
 - **Overview:** This book provides a comprehensive analysis of the legal framework governing cyber activities in India. It covers the Information Technology Act, of 2000, and its subsequent amendments in detail.

- Contributions: Ahmad's work is instrumental in understanding the legal nuances of cybercrime in India, offering insights into various legal provisions, case laws, and judicial interpretations.
- Relevance: It serves as a crucial resource for legal professionals, students, and researchers interested in the intersection of law and technology.

2. **"Cyber Crime in India: Problems, Perspectives and Solutions" by Dr. Vishwanath Paranjape –**

- Overview: Dr. Paranjape's book delves into the different types of cybercrimes prevalent in India and discusses their impact on society.
- Contributions: The book provides a detailed analysis of cybercrimes like hacking, identity theft, and cyber stalking. It also offers potential solutions and preventive measures.
- Relevance: This book is particularly useful for law enforcement officials, policymakers, and researchers focusing on cybercrime prevention and control.

3. **"Cyber Crimes against Women in India" by Debarati Halder and K. Jaishankar**

- Overview: This book addresses the specific issue of cybercrimes targeting women, including cyber stalking, online harassment, and revenge pornography.
- Contributions: Halder and Jaishankar provide empirical data and case studies, highlighting the unique challenges faced by women in the digital space.
- Relevance: It is a vital resource for understanding gendered aspects of cybercrime and for developing gender-sensitive cyber policies and laws.

4. **"Cyber Security and Cyber Laws" by Alfred Basta and Nadine Basta –**

- Overview: Although not exclusively focused on India, this book includes significant sections on the Indian context of cyber security and laws.
- Contributions: The authors discuss global cyber security issues with specific references to Indian laws and regulations, providing a comparative perspective.

- Relevance: This book is beneficial for those looking to understand India's cyber security landscape within the global context.

Objective

The objective of this research is to investigate the prevalence and types of cybercrimes committed in the regions of Punjab and Chandigarh. The study aims to identify the demographics and characteristics of individuals who fall victim to these crimes. Additionally, it seeks to assess the level of awareness and understanding of cybercrime among the population in these areas. The research will provide insights into the nature of cyber threats faced by the residents and the effectiveness of current measures in place of educating and protecting them.

Scope

This present research is aimed at comprehending the distinct and various forms of cybercrimes which are prevalent in the regions of Punjab and Chandigarh and identifying the demographics of the victims. The study and survey will examine individuals within the age range of 15 to 65 and older. It delves to measure the level of awareness and understanding of cybercrime among this demographic populace. The primary constraint and hurdles of this research is the inability to conduct face-to-face interviews with victims of cybercrimes. These reservations may affect the depth of qualitative data obtained and necessitate reliance on other data collection methods such as surveys, online questionnaires, and secondary data sources.

Research methodology

This research aims to gather insights into the trends, challenges, and awareness of cyber-crimes in Chandigarh and Punjab. As these aspects involve the personal sentiments and perception of the general public regarding cybercrime, the qualitative method of research is used. The research is done via hybrid means. While the majority of the responses have been collected by Google Forms, some have been collected by the on-field research conducted by the researchers. The responses filled in by Google Forms are best suited for this research as it made analysis of results much easier and made it more detailed with the help of pie charts. For the discussion, an interview was also conducted with a cybercrime official and expert in this field. A comprehensive analysis has also been made based on the data provided by these personnel to us. All these methods were ideal for our research, which required a large number of participants for an elaborate evaluation of the related subject. All these various sources added to the

collection of combined useful data and made our research more insightful. This research includes the popular perception of citizens as well as the information shared by previous research conducted by researchers on this new and vast topic.

Conceptual clarity

The thriving use of the Internet across the globe in disparate sectors including education, entertainment, public policy, information, laws, awareness, research, banking, entrepreneurship, navigation, etc. This internet boom has also enlarged the scope of Cyber Crimes. According to The Hindu (2024), India is the 80th severely targeted country of Cyber Crimes affecting 34% of users through local threats.

According to Deepak Singh PPS, "There are 74 complaints per day with 50 lakhs average cases per year with 40% recovery rate of the registered cases." These Cyber Crimes include Cyber terrorism, Cyber Bullying, Sextortion & Pornography, Cyber Stalking & Harassment, Financial Frauds & Internet Gambling, Identity Theft, Deepfake AI, Cyber Embezzlement, Cyber Laundering, Forgery, Data breaches, Dark Web and attack of viruses like Malware. These are categorized both under violent and non-violent Cyber Crimes.

Cyber Crimes explanation in detail:

1. Cyber Bullying:

- Cyber Bullying is committed by the way usage of hate or aggressive and even threatening comments, messages, posts or tweets on social media platforms or messenger apps to defame a person. The causes can vary including personal aggression towards a person, intimidation by stereotyped ideas of someone, empathy gaps among people and even entertainment. A bully is usually uncovered with pseudo or fictitious usernames.
- Women in comparison to men are in jeopardy of cyber bullying and harassment. Even Digital Shakti Campaign 4.0 was launched by NCW for safe cyber spaces for Women (Press Information Bureau, 2020). UNICEF's data suggests almost 33% of young online users have faced cyber bullying in the survey in 30 countries across the World (UNICEF, 2020). According to Deepak Singh PPS "There is a 40% depression rate and less than 1% suicide rate among women in harassment and bullying cases".

2. Online Financial Frauds:

- A study at IIT Kanpur-based non-profit startup (Future Crime Research Foundation) reveals that among all the Cyber Crimes, financial fraud accounts for 77.41% during the period 2020-2023 (Hindustan Times, 2024). The various subcategories include UPI transactions, Debit & Credit cards, e-banking, and email frauds.
- These frauds affect the general public, government, and even commercial companies. It is generally made through fraudulent phone calls, links in SMS, QR codes, ATM frauds, OTP frauds or cheating frauds.
- Ludhiana is close to becoming second in the Cyber Crimes across India (Times of India, 2023). Online Gambling which includes betting, lotteries, and poker have created platforms for increased money laundering, illicit funds, financial frauds, and surplus in parallel economy, even terrorist funding, and inadequate dispute resolution mechanism. Forgery also includes financial frauds where fraudsters make counterfeit currency notes.
- In 2020, the Punjab State Cyber Crime Cell achieved great success in arresting a fraudster gang for fraud of Rs 5 crores in HDFC Bank in a tech-savvy manner. They withdrew this amount from 5 bank accounts with regular changes in email IDs and mobile numbers, making it identical to the mobile number and email ID of the victim, hence becoming the virtual controller of their account. The KYC documents and identities were fabricated and fake. The money was withdrawn from the bank in the form of cheques and ATM cards. They were involved in multi-crore frauds and all three accused were arrested at different locations in Ludhiana. The FIR was registered under 66, 66C, 66D IT Act, 420, 467, 468 IPC. Recoveries were made for the victims. Taking into consideration cyber frauds and crimes, the Punjab government announced 28 new cyber police stations, one in each district across the state (Hindustan Times,2024).

3. Sextortion and Cyber Pornography:

- There are no fixed definitions of pornography. What may not be obscene in countries like Canada or the USA, may be considered in India. It mainly includes publishing,

printing, downloading, and transmitting pornographic material making it accessible on websites and magazines through the Internet.

- Section 67 of the IT Act in the Indian Constitution comprises serious laws for dealing with cyber pornography. Child pornography is illegal across the world. Sextortion cases have been spreading like wildfire through job opportunity scams, dating apps, phone calls, etc. with the least registered formal complaints among Cyber Crimes in India. Surprisingly, men (mostly older) are more vulnerable to sextortion cases. Bharatpur in Rajasthan is the hotspot for sextortion cases.
- A famous case like Vincent Vikram vs State of Karnataka where the husband breaches the privacy of his wife by sending obscene photos to her father and two of her friends, has made judiciary of supreme importance to combat cybercrimes involving sexual offences (Indian Kanoon, 2022).
- The Chandigarh University case of cyber pornography faced massive rumors and protests. A women student was arrested for making and sending objectionable videos of not only her own but some other girls in the bathroom to her boyfriend. According to the authorities, only her own video has been sent and her boyfriend was also arrested and charged under Section 354 A, 354C, 354D, 506, 509, 511 of Indian Penal Code and sections 66C, 66D, 66E, 67A, 84C of IT Act (Hindustan Times, 2022).

4. Deepfakes AI:

- The algorithms of artificial intelligence are being used to create pseudo videos, audio and information seeming to be real. The cases of Deepfake AI are dealt with at the center level by cyber cells. Even retired officers and celebrities have fallen Prey to deepfake AI.
- In the campaigning of 2024 elections, Ranveer Singh and Amir Khan were fabricated campaigning for the Congress party (BBC News). Macfee Survey has suggested that 75% of Indians have consumed fabricated content in the last year (Economic Times, 2024). The first Deepfake AI case in India was registered in 2022 in Kerala. The victim was a 73-year-old man who sent Rs 40,000 to the fraudster in a WhatsApp call

mimicking his friend's voice and appearance through AI software, who got information about their friendship through social media. This brings each digital user on high time to a holistic use of their devices.

5. **Cyber Stalking Online Harassment:**

- Cyber Stalking is to harass, threaten, stalk and intrigue into the privacy of a person through social media, messaging apps, email or phone calls. They are concealed under pseudo names similar to bullying. There are consistent deliberate efforts to stalk or harass the victim varying from inoffensive messages to aggressive life-threatening emails.
- In *Anish Jose Antony vs State of Karnataka*, the accused chased the girl and pressurized to love her despite her own disinterests after which he started threatening her through messages and later the case was registered for cyber stalking under Section 354D of the Indian Penal Code, 1860. The chairperson of NCW communicated that cyber stalking against women has increased by 500% since the pandemic (Times of India, 2021).

6. **Cyber Terrorism:**

- Cyber terrorism is a term referring to terror attacks on software, websites or data breaches affecting the infrastructure of the country like healthcare, banking or nuclear plants and even cause loss of lives usually to fulfill political motives. "*Recruitment, training, funding and execution of terrorism is done in cyberspace*" Dr. Varun Kapoor, IPS (TEDx talks, 2023). After Taiwan, India is the second severely target country in Asia in 2023 (Mint, 2024).
- The first cyber terrorism case was experienced in Maharashtra where a 32-year-old man named Ansari who was in consistent communication with Omar Elhaj, a member of banned ISI. They were not only accused of sending objectionable messages affecting the unity and integrity of the country but also planning for Lone wolf bomb attack in American school with intent of spreading terror and killing foreign nationals (Rebecca Samervel, 2022). In the IT Act of 2000, unlike the other Cyber Crimes which are bailable in nature, cyber terrorism under Section 66 F leads to the punishment of life imprisonment.

- In 2019, a nuclear power plant in Kundankulam was hacked by North Korean hackers through malware that remained undetectable for months was not life threatening but a wake-up call for the authorities (The Washington Post, 2019). In 2023, an employee of ISRO's Space application Centre has been charged under section 66 (F) for cyber terrorism after he sent photographs of his workplace to a Pakistani woman without any permission from authorities leading to denial of his bail (The Times of India, 2024).

7. Data Breaches, Dark Web, and viruses Attacks:

- India has faced data breaches since 2010 beginning from Operation Rat to attacks like the OPM data breach (2015), and Demonetization attacks (2016) and following the largest data breach in the history of India which was the data breach of Aadhar card and passport details of 815 million citizens (2023).
- The Chinese hackers caused a sensitive data breach of AIIMS- Delhi and threatened to sell this data (Deccan Herald, 2023). The founder of Tagg labs mentions in an article that at least one data breach has been experienced by the majority of organizations in the last year. This highly affects the trust of people, causing them financial loss, serving the headlines of the news, and highly affecting the market Demand.
- The surface web is only on the outskirts of the entire web, counting the information, websites etc. found on search motors and the web. The dark web includes specialized information where only a few users can access the information, almost above the reach of an average user. Recently UGC-NET was cancelled by NTA, and the authorities claimed that the exam had been interrupted by the "dark web" and the re conducting of the paper is hindered by hacking of the data by terrorist organizations (Deccan Herald, 2024).
- A virus enters a computer user through a harmless seeming email or infected disk, causing the breach of data, loss of data and affecting the operations of the computer. There are various types of viruses including Trojan horses, worms, boot sector viruses etc. The unknown hackers attacked the Indian Defence and energy companies through

the invitation by air forced through channels causing malware attacks on the system (The Hackers News, 2024).

8. **Identity Theft & Doxing:**

- Identity theft is stealing someone's name and personal details like PAN number, bank details, Aadhar Card details, visa details etc. for unlawful exercises (fraud) and causing such emotional distress, economic loss and reputational harm. Doxing is an act of sharing these personal details to embarrass or defame the individual.
- In our offline survey, Priya, a woman working in the banking industry, experienced identity theft where the hacker got access to information after she clicked the link in the SMS, causing the leakage of personal details like Aadhar number and bank details. Later this identity theft turned to threatening of posting all her pictures on the website. She complained but no action was taken. She was harassed for months after which she not only blocked her number but also changed her mobile phone.
- In conversation with Deepak Singh PPS, he explained how in their workplace identity theft was experienced. The hackers used the DP of their senior on WhatsApp and asked for money from the office staff, causing them a financial loss of 2-3 lakhs.

9. **Cyber laundering:**

- Cyber laundering is an act of concealing and moving parallel money. It can be a smart way of fabricating illegal money into authenticated sources and use.
- Some politicians use virtual money laundering. The simplest example includes converting illegal money into authentic means by portraying the money as a donation fund to NGOs that never existed. They use sophisticated website creation of a fake NGO to prove their act of social and public welfare as true. Crypto currency and internet gambling augment cyber laundering.

10. **Hacking** - A hacker is user who sans any authorization and attempts to or gains access to an information system. Hacking is a crime even if there is no visible

damage to the system since it is an invasion and breach of the privacy of data. There are different classes of Hackers.

- a) White Hat Hackers – They under the bona fide belief that information sharing is an act of goodness and equity, therefore they must share their expertise by facilitating access to information. However, some white hat hackers are just "joy riding & quote, on computer systems.
- b) Black Hat Hackers – They act under the mysterious circumstances and commit breach by way of intrusion and cause damage, steal or modify data or insert viruses or worms which damage the system. They are also called 'crackers'.
- c) Grey Hat Hackers – Undoubtedly hackers, however ethical but occasionally violate hacker ethics. Hackers hack into networks, stand-alone computers and software. Network hackers tend to gain access without authorization to private computer networks just for challenge, curiosity, and distribution of information. Black Hat Hackers perform unauthorized intrusion damage like stealing or changing information or inserting malware (viruses or worms).

11. **Spoofing** - It is the act of impersonation of one computer to electronically "look" like another computer, in order to gain unauthorized access to a system that would be normally restricted. Spoofing was used to gain access to valuable information stored on a computer belonging to security experts.

12. **Corporate Espionage** – It means the theft of trade secrets through illegal means such as wiretaps or illegal intrusions.

13. **Password Sniffers**- Password sniffers are programs that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the sniffer can pretend to be an authorized user and log in to use restricted documents.

Case laws -

Cyber-crime means any criminal activity in which a computer or network is the source, tool, target or place of occurrence of crime. The Cambridge English Dictionary defines cyber-crimes as crimes which are committed by usage of computers or with respect to computers, significantly through the internet. Crimes involving the use of information or the usage of electronic means in furtherance of crime are covered under the umbrella of cybercrime. Cyber Crimes may be committed against individual people, property and government.

Evolution of cyber-crimes:

Cybercrime has evolved from Morris Worm to ransom ware. Many countries including India are working to stop such crimes or attacks, but these attacks are continuously changing and affecting our nation.

<u>Years</u>	<u>Types of Attacks</u>
1997	Cyber-crimes and viruses initiated that included Morris Code Worm and others.
2004	Malicious code, Trojan, Advanced worm etc.
2007	Identifying thief, Phishing etc.
2010	DNS Attack, Rise of Botnets, SQL attacks etc.
2013	Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransomware attack etc.

In India, the Information Technology Act 2000 was passed to provide legal recognition for transactions carried out using electronic communication. The Act operates to deal with the law with respect to Digital Contracts, Digital Property, and Digital Rights. Any violation of these laws constitutes a crime. The Act prescribes very high deterrent punishments for commission of such crimes. The Information Technology (Amendment) Act, 2008(Act 10 of 2009), has further enhanced the punishments. Life imprisonment and fines up to ten lakh rupees may be given for certain classes of cyber-crimes. Compensation up to five crores rupees can be given to affected people if the damage is done to the computer, computer system or computer network

by the introduction of a virus, denial of services, etc. Sections 65-74 of the Act specifically deal with certain offences, which can be called Cyber Crimes.

- Tampering with any computer source code used for computer programme, computer systems, or computer networks is punishable with imprisonment of up to three years, or with fine which may extend up to two lakh rupees, or with both. "Computer source code" means the listing of programmes, computer commands, design and layout, and programme analysis of computer resource in any form.
- Hacking a computer system is to be punished with imprisonment for up to three years, or with a fine which may extend up to five lakh rupees, or with both.
- Dissemination of offensive data or false information through a computer source or a communicative device is punishable with imprisonment of up to three years and a fine.
- Receiving or retaining stolen computer resources or communication devices is an offense punishable with imprisonment of up to three years and fine of up to one lakh or with both. (S.66B). The same punishment is prescribed for fraudulent use of electronic signatures, password etc. of any other person and for cheating using a computer, cell phone, etc.
- Capturing, Transmitting or publishing the image of a private area of any person without consent is punishable with imprisonment up to three years and with fine up to two lakhs or with both.
- Punishment of Cyber terrorism may extend to imprisonment for life.
- Publishing transmitting information that is obscene in electronic form shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

- Publication and transmission of containing sexually explicit act or conduct is to be punished with imprisonment up to five years and fine up to ten lakh rupees and for second or subsequent conviction with imprisonment for a term up to seven years and fine up to ten lakh rupees. The same punishment is prescribed for child pornography.
- Penalty for Misrepresentation - Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be punished with imprisonment for a term, which may extend to two years, or with a fine which may extend to one lakh rupees, or with both.
- Penalty for Breach of Confidentiality and Privacy -Any person who has secured access to any electronic record, book, register, correspondence, information, document, or other material without the consent of the person concerned discloses such an electronic record or book. Register, correspondence, information, document, or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with a fine which may extend to one lakh rupees, or with both.
- Punishment for disclosure of information in breach of contract is imprisonment for a term of up to three years or with fine up to five lakh rupees or with both.
- Punishment for publishing Digital Signature Certificate false in certain particulars.
- No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that
 - the Certifying Authority listed in the certificate has not issued it; or
 - the subscriber listed in the certificate has not accepted it; or
 - the certificate has been revoked or suspended,
- Violation of the above provision is punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
- Publication for Fraudulent Purposes.

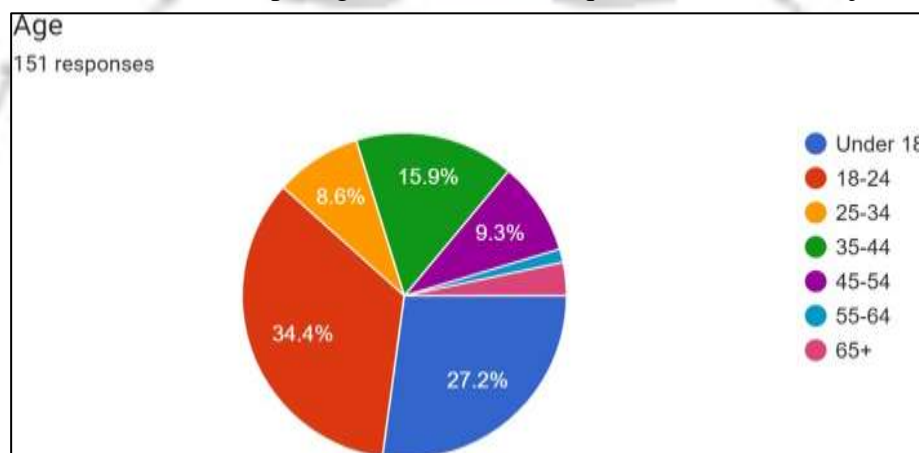
- Whoever having the requisite knowledge creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. In addition to the prescribed punishments Any computer, computer system, floppies, compact disks, tape drives, or any other accessories related to the crime shall be liable to confiscation. S.75 of the Act makes it clear that the provisions of this Act apply to any offence, or contravention committed outside India by any person notwithstanding his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system, or computer network located in India.

Results

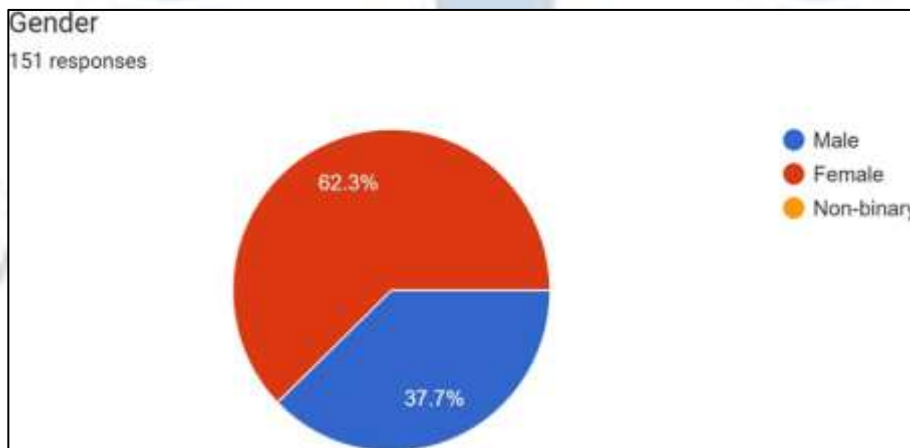
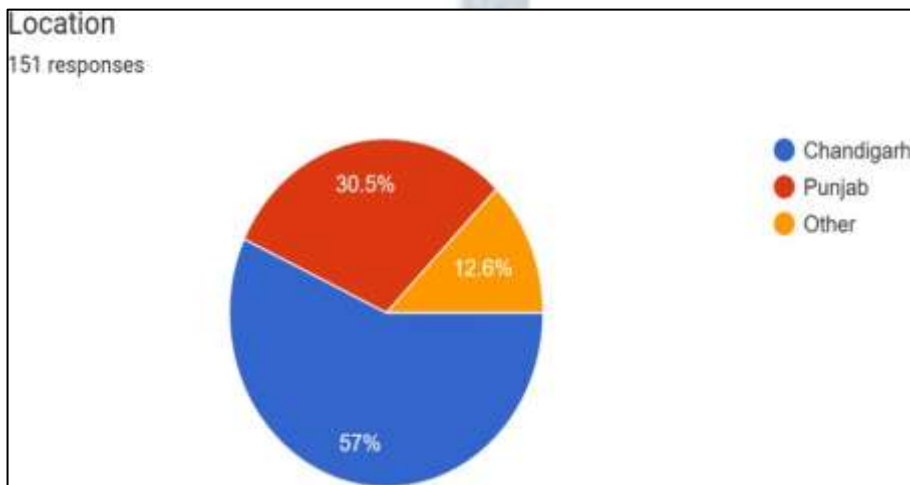
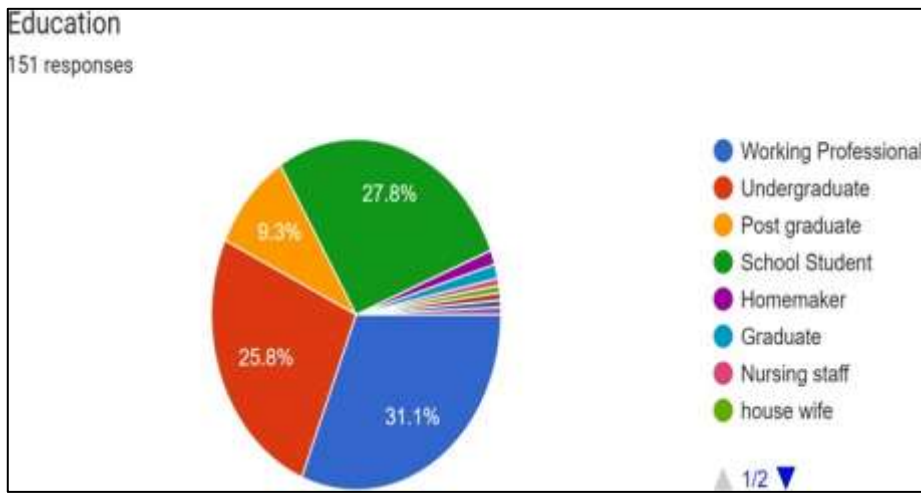
Online Survey –

Demographic information –

There are 151 respondents for the online questionnaire. Out of 151 respondents, 52 respondents are aged between 18 and 24, 42 respondents are under 18, 13 respondents are in age between 35 and 44, 15 respondents are between 45 and 54, and other 29 respondents are of 55-65 and 65+ age. 86 respondents belong to Chandigarh, 47 respondents belong to Punjab and 23 respondents belong to different locations of India. Among 151 respondents, 47 respondents are working professionals, 39 respondents are undergraduate students, and 15 respondents are postgraduate students or have post-graduation as their qualification. The major respondents are



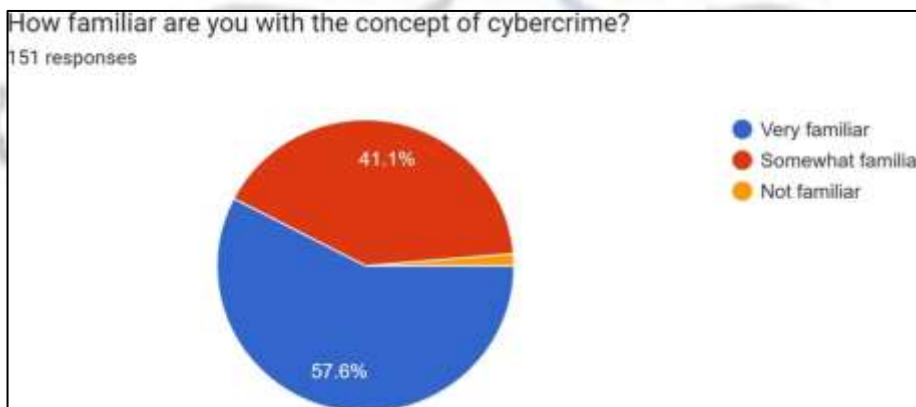
women, almost 95 in number whereas the male respondents are 57 in number. Multiple responses were allowed for certain questions.

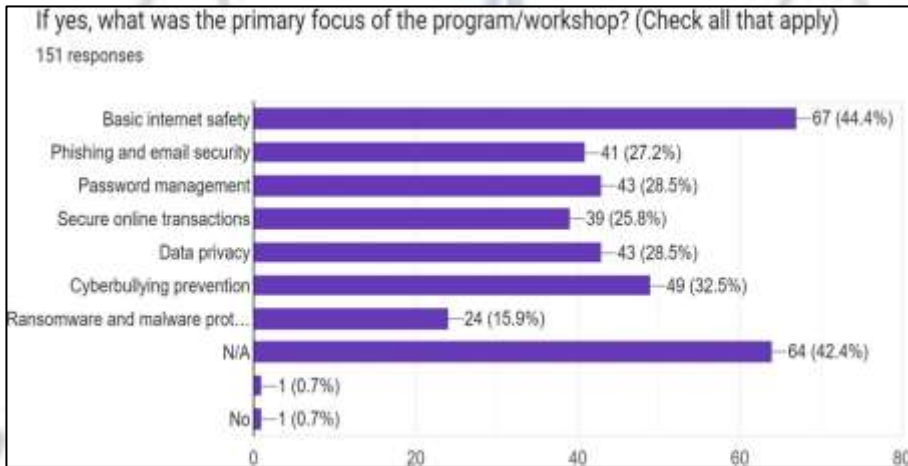
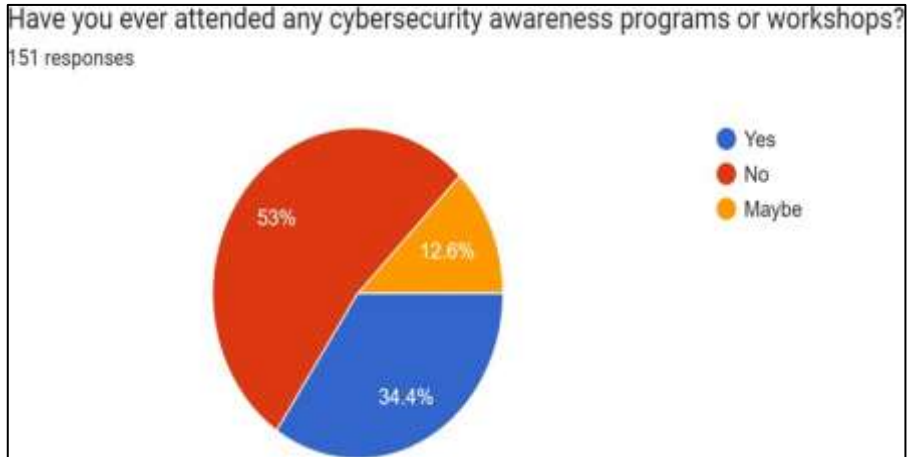
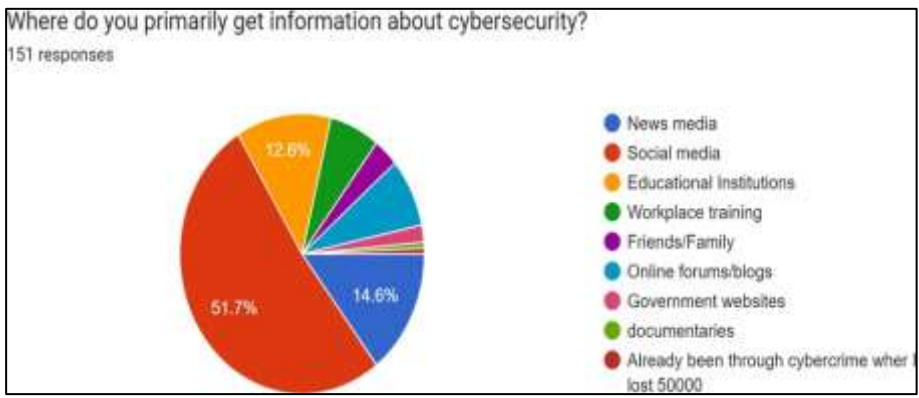


Cybercrime awareness –

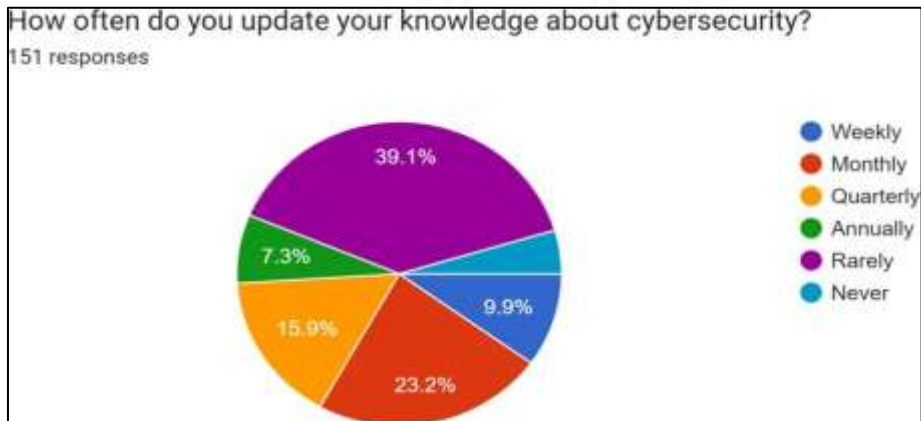
Out of 151 respondents, 87 respondents are very familiar, 63 are somewhat familiar and only 1 respondent is not familiar with the concept of Cyber Crime. The major source of information related to Cyber Crime is spread through social media platforms marked by 79 respondents, educational institutions are the second significant source of information marked by 20 respondents followed by online blogs and other sources of information like news media,

friends, family etc. Among 151 respondents, 80 respondents didn't attend any formal workshop on Cyber Crime Awareness and only 52 respondents attended the formal workshop where the rest of the respondents are not sure of their answer. Among the 52 respondents who attended the workshop on Cyber Crime had majorly received information on basic internet safety and cyberbullying prevention followed by other categories like phishing, password management, data privacy etc. depicts how often people update their knowledge about cyber security which suggests almost 60 respondents rarely update their knowledge, 35 respondents update their knowledge monthly followed by other categories who update quarterly, yearly and even never.

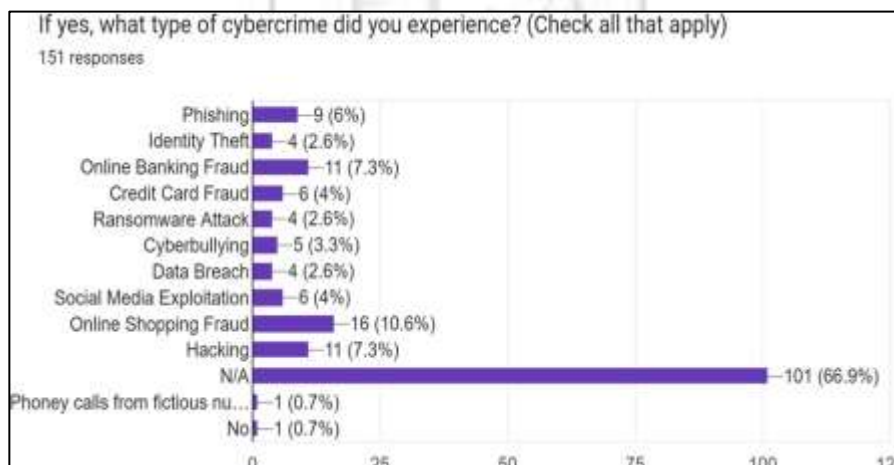
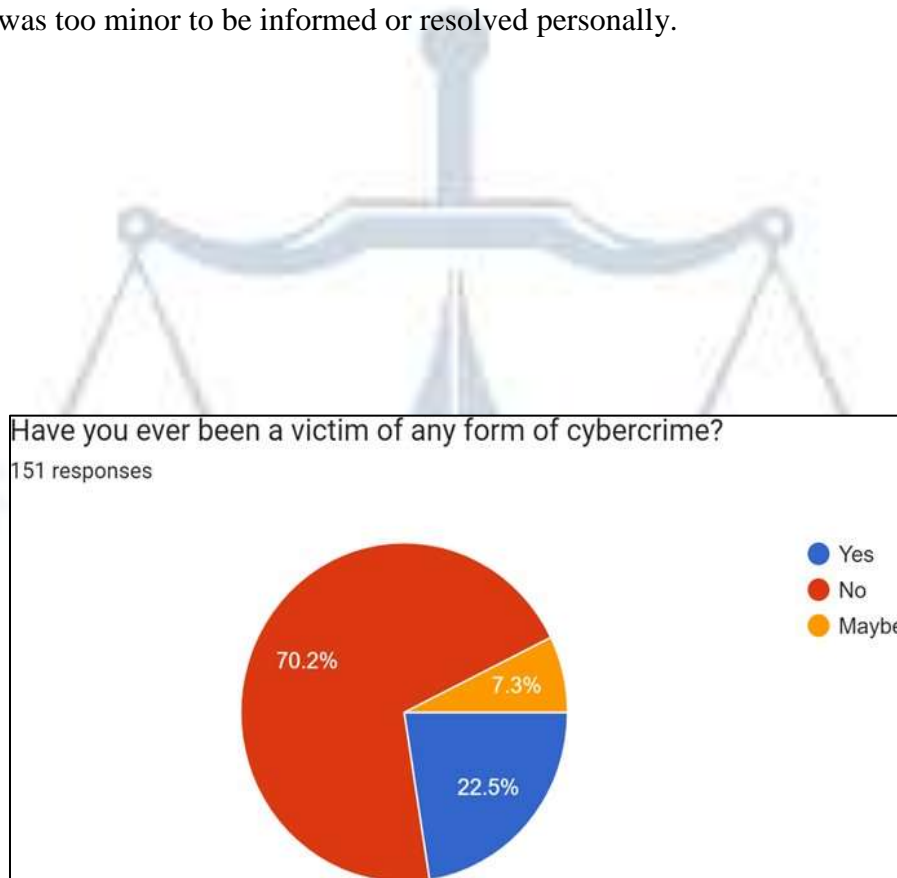


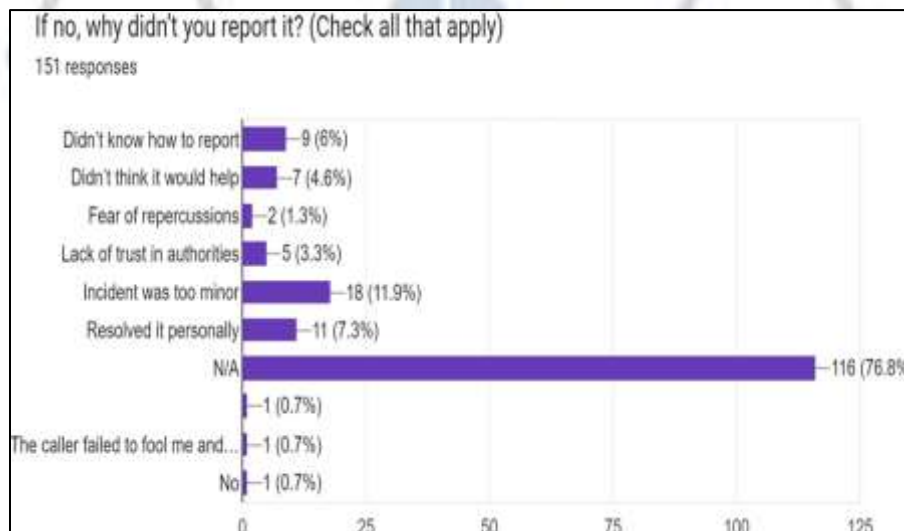
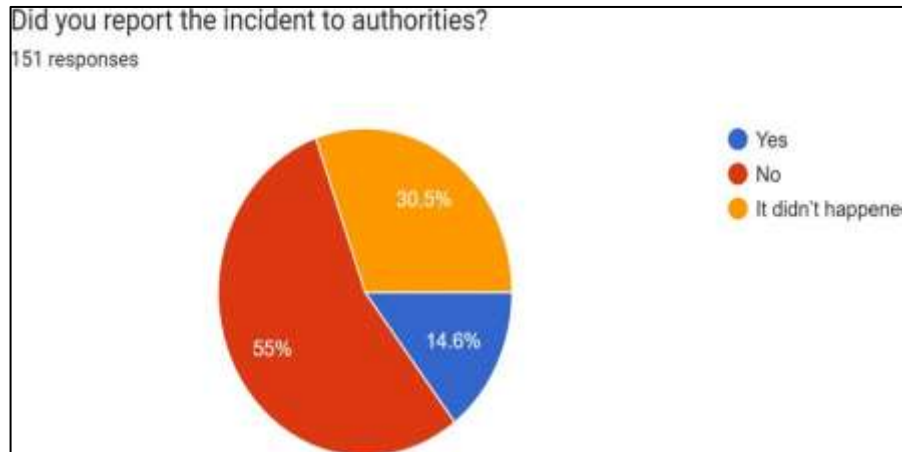
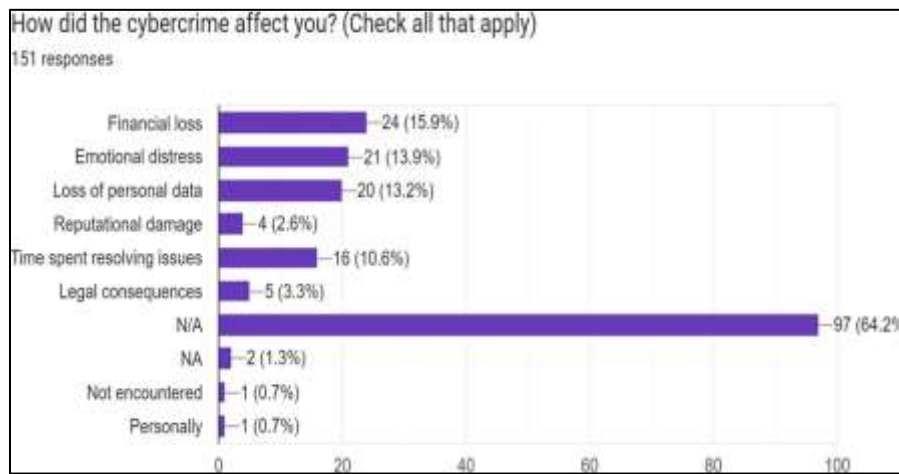


Personal experience with cyber-crime –



Among 151 respondents, 106 respondents have not been victims of Cyber Crime, 34 respondents have been victims of Cyber-Crime, and 11 respondents are not sure of their response. Among the victims of Cyber Crimes, 10.6% of respondents have experienced online shopping fraud, followed by online banking frauds and hacking which are 7.3% and the rest are shared by categories like data breach, phishing, fictitious phone calls etc. The maximum victims have suffered financial loss (15.9%), followed by emotional distress (13.9%) and loss of personal data (13.2%) with the least number of respondents suffering reputational damage. Almost 55% of respondents didn't report the incident to authorities because respondents thought it was too minor to be informed or resolved personally.

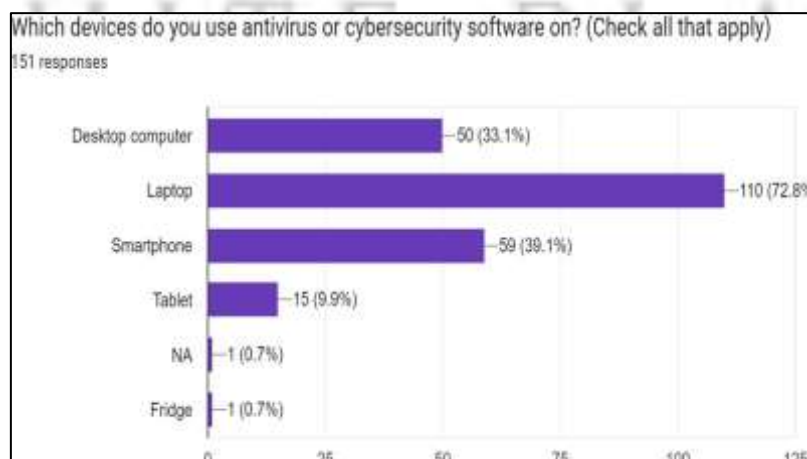
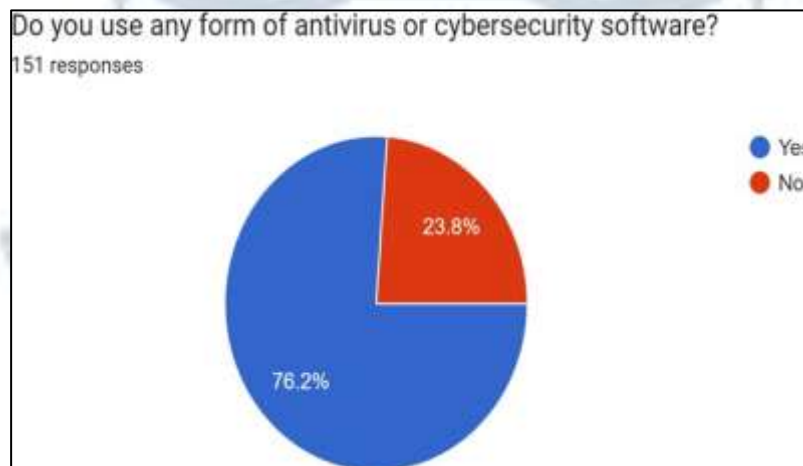




Cyber security practices -

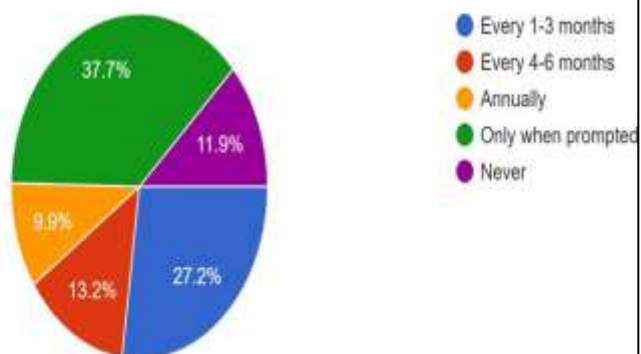
Among 151 respondents, 115 respondents have used antivirus or cyber security software and the rest of the 36 respondents don't use any antivirus or cyber security software. Most of the respondents used antivirus on their laptops, followed by smartphones, desktop computers and tablets. The maximum respondents only change their password when prompted, followed by the respondents who change their password security 1-3 months, following 4-6 months and annually, and 18 respondents never change their passwords. The two-factor authentication for

online accounts is used by 113 respondents and the remaining 38 respondents don't use the two-factor authentication for online accounts. Among the respondents, 73 people were somewhat cautious about opening their emails while 13 people were not cautious about opening their emails. A maximum number of respondents (116) have no formal training in cyber security in their workplace and educational institutions.



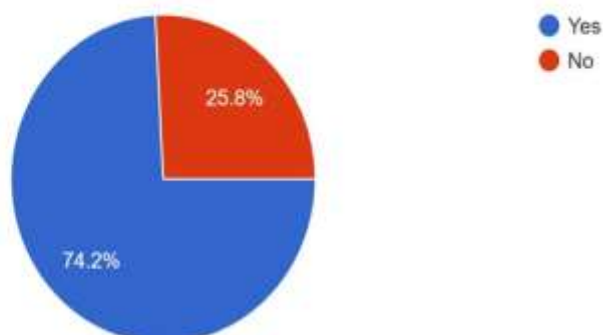
How often do you change your passwords?

151 responses



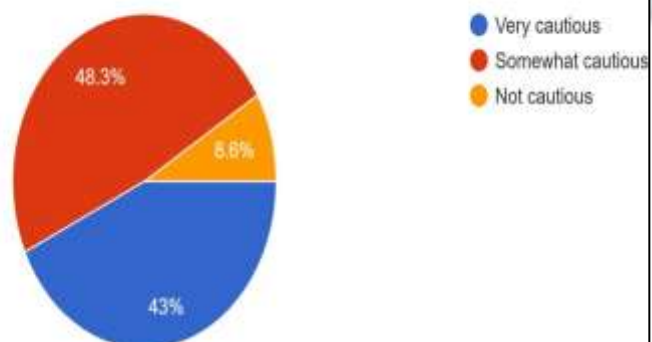
Do you use two-factor authentication (2FA) for your online accounts?

151 responses



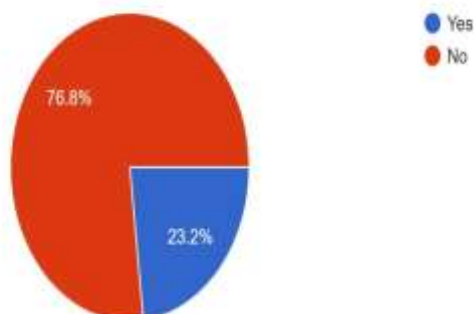
How cautious are you about opening emails from unknown sources?

151 responses



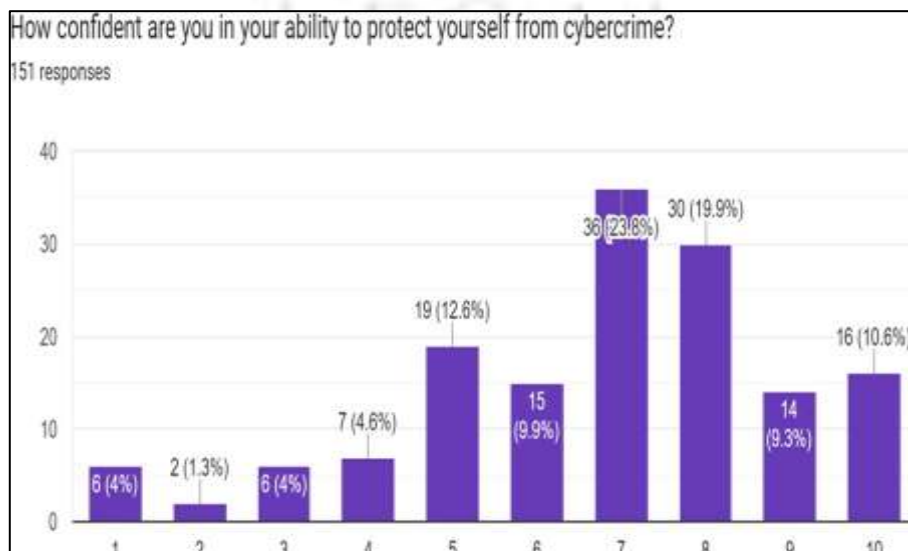
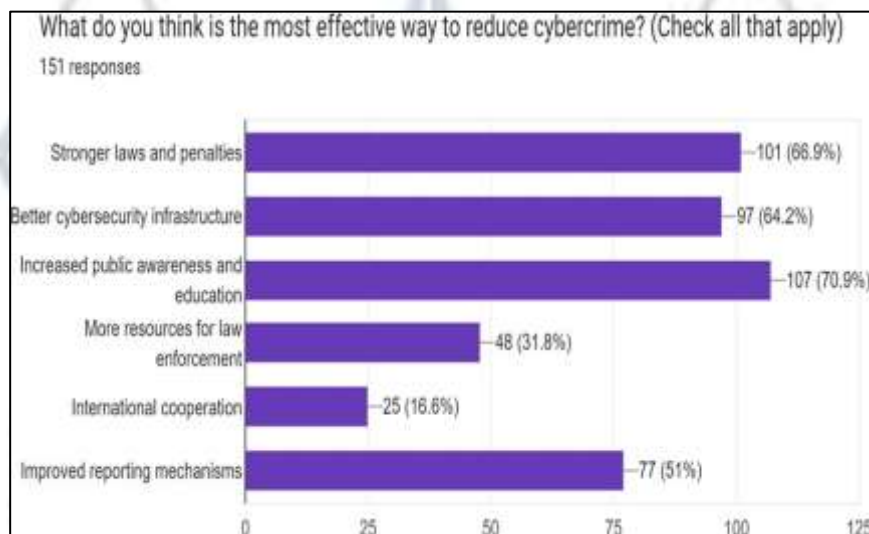
Have you received any formal training on cybersecurity at your workplace or educational institution?

151 responses



Attitudes and opinions -

Out of 151 respondents, 74 respondents are unsure of combating Cyber Crimes, and 65 respondents believe current laws are not sufficient to combat Cyber Crime. The most effective way to reduce Cyber Crime is increased public awareness and education, followed by stronger laws and penalties, following better cyber security infrastructure and other categories like international cooperation etc. The respondents have to rate their ability to protect from Cyber Crimes on a scale of 1-10 (1: unlikely, 5: somewhat likely, 10: very likely), where the maximum number of respondents have rated 7 which is between somewhat likely and very likely. The maximum topic which respondents would like to see covered in the cyber awareness programme is secure online transactions, followed by social media privacy, then data privacy and protection and other categories (24). On a scale of 1-10, opinion on phone spying on them as a part of government asset is marked 5 by most respondents and followed by 10 on the scale by respondents. Most respondents rated 10 for stricter laws and equal enforcement of cyber laws against Cyber Crimes. This followed the last question of additional comments.



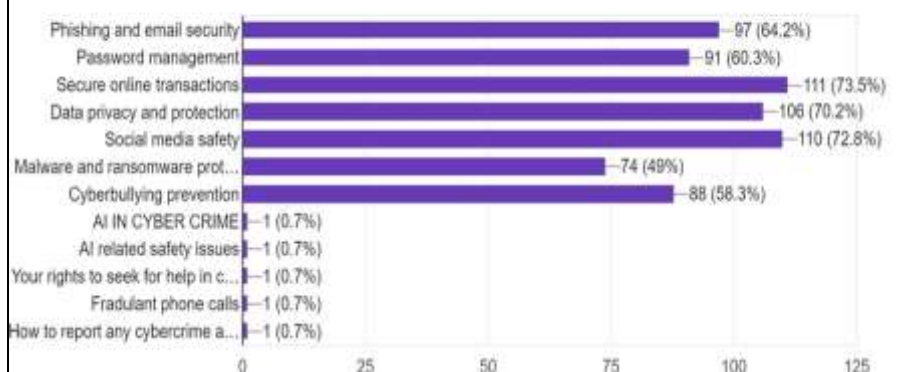
Any additional comments or suggestions on how to tackle cybercrime?

45 responses



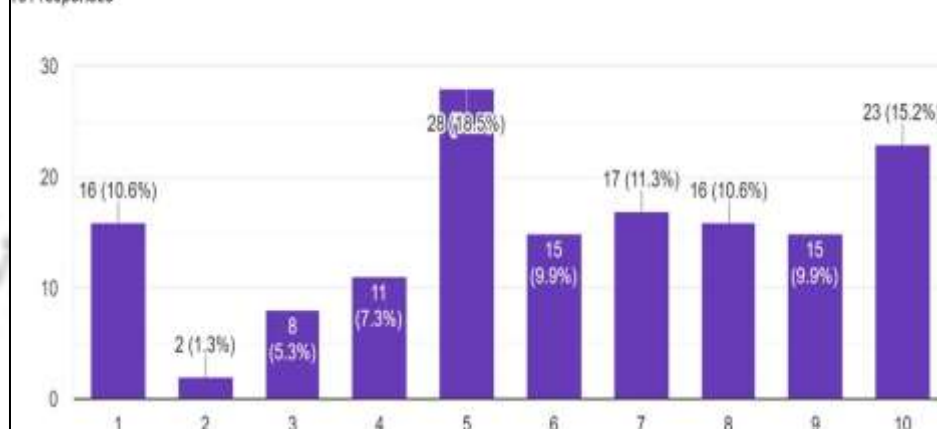
What topics would you like to see covered in cybersecurity awareness programs? (Check all that apply)

151 responses



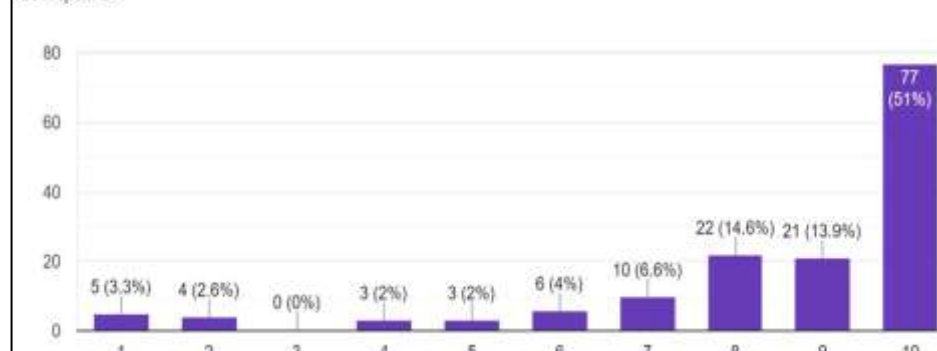
On a scale of 1-10, Do you feel your phone is a part of the government spying on you?

151 responses



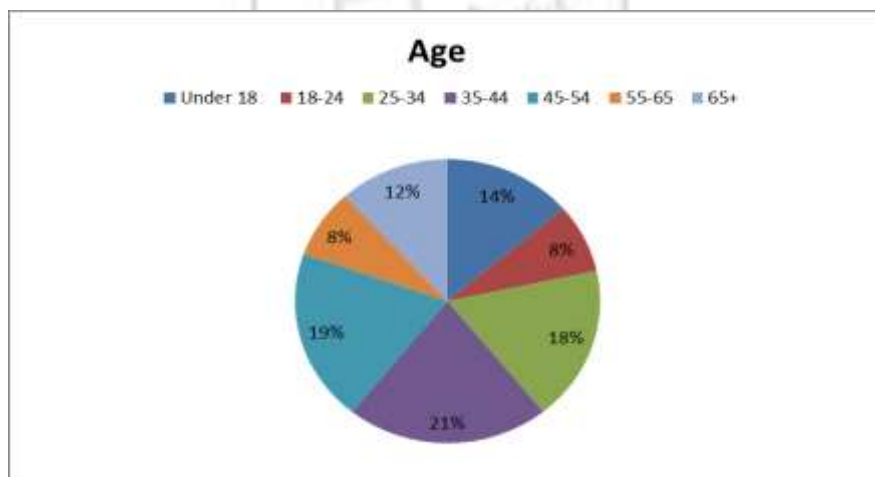
On a scale of 1-10, Do you feel there should stricter laws and equally strict enforcement of laws against cybercrime

151 responses



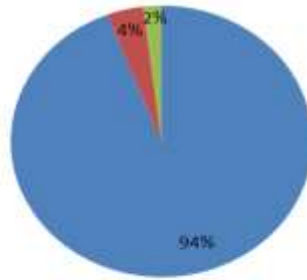
Offline Survey

There are 51 respondents for the offline questionnaire. Out of 51 respondents, 4 respondents are aged between 18 and 24, 7 respondents are under 18, 11 respondents are in age between 35 and 44, 9 respondents are of age between 25 and 34, 10 respondents are between 45 and 54, and the other 4 respondents are 55-65 and 6 respondents are of 65+ age. 2 respondents belong to Chandigarh, 48 respondents belong to Punjab and 1 respondent belong to different locations of India. Among 51 respondents, 15 respondents are working professionals, 14 respondents are self-employed, 6 respondents are retired, 14 respondents are students, and 2 respondents are homemakers. The different qualifications of the respondents include undergraduate students 4 in number, 22 respondents have graduation as their qualification, and 12 respondents have post-graduation as their qualification. The major respondents are men, almost 36 in number whereas the female respondents are 15 in number. Multiple responses were allowed for certain questions. There were bilingual forms- Punjabi and English.



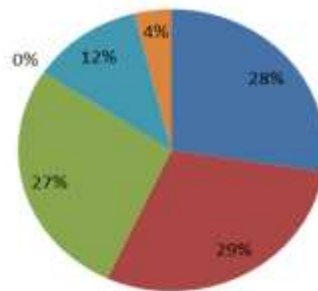
Location

■ Punjab ■ Chandigarh ■ Other



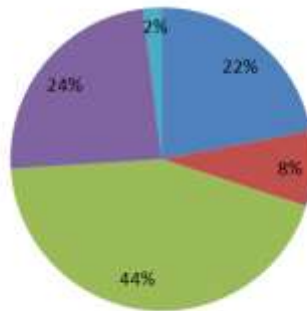
Occupation

■ Student ■ Employed ■ Self-employed ■ Unemployed ■ Retired ■ Homemakers



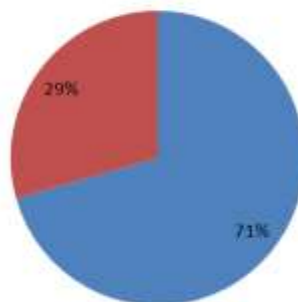
Education Level

■ High School ■ Undergraduate ■ Graduate ■ Post graduate ■ Other



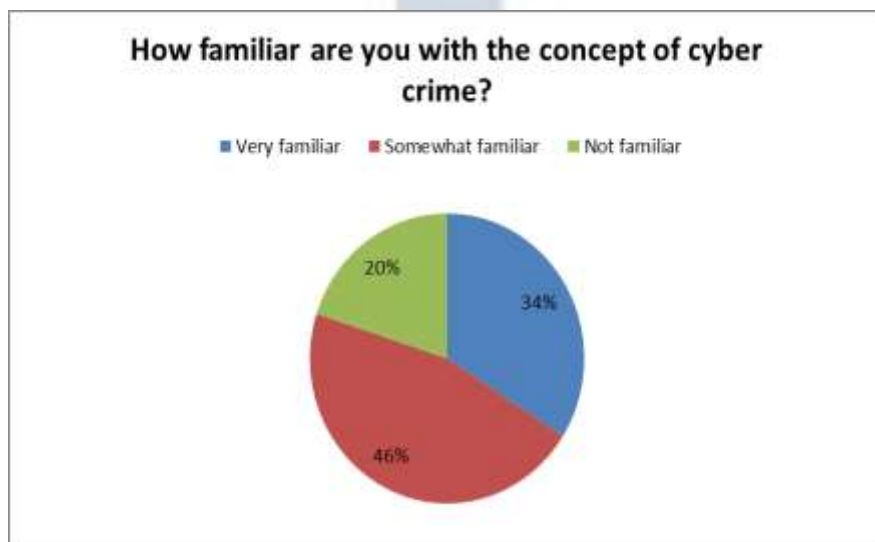
Gender

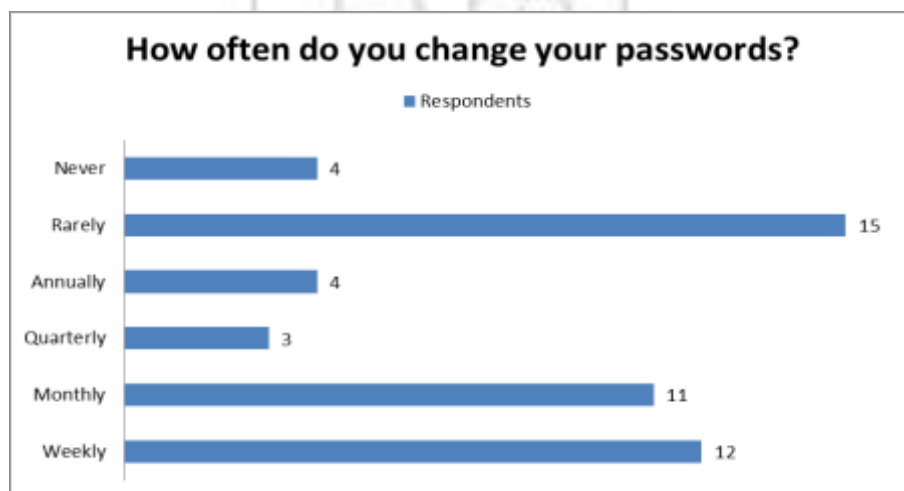
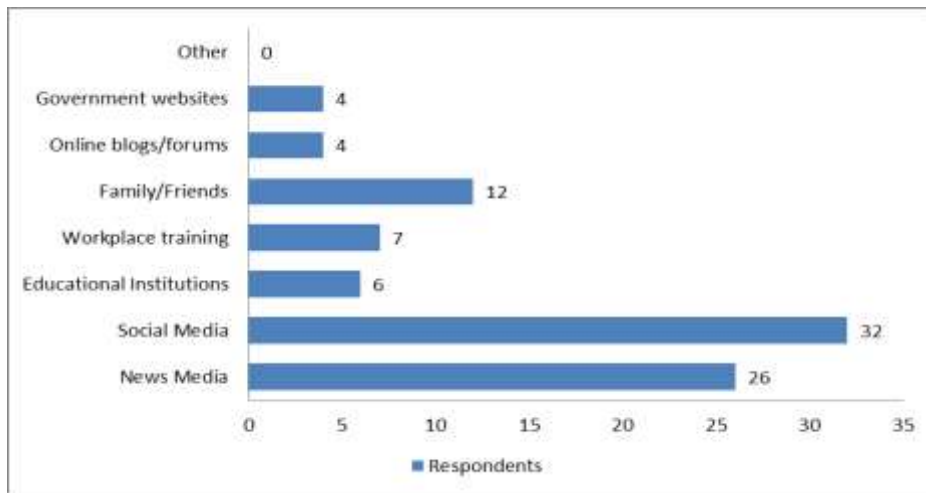
■ Male ■ Female ■ Non-binary ■ Prefer not to say



Cyber-crime awareness –

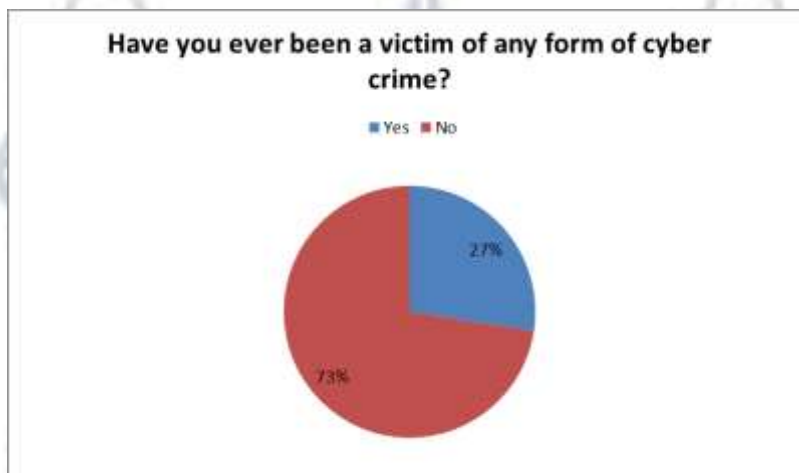
Out of 51 respondents, 17 respondents are very familiar, 23 are somewhat familiar and 10 respondents are not familiar with the concept of Cyber Crime. The major source of information related to Cyber Crime is spread through social media platforms marked by 32 respondents, News is the second significant source of information marked by 26 respondents followed by friend other sources of information like workplace training, online blogs etc. Among 51 respondents, 39 respondents didn't attend any formal workshop on Cyber Crime Awareness and only 12 respondents attended the formal workshop. Among the 12 respondents who attended the workshop on Cyber Crime had majorly received information on basic internet safety and Phishing and email security, data privacy followed by other categories like ransom ware and malware protection, secure online protection etc. depicts how often people update their knowledge about cyber security which suggests almost 15 respondents rarely update their knowledge, 12 respondents update their knowledge weekly followed by other categories who update monthly, quarterly, yearly and even never.

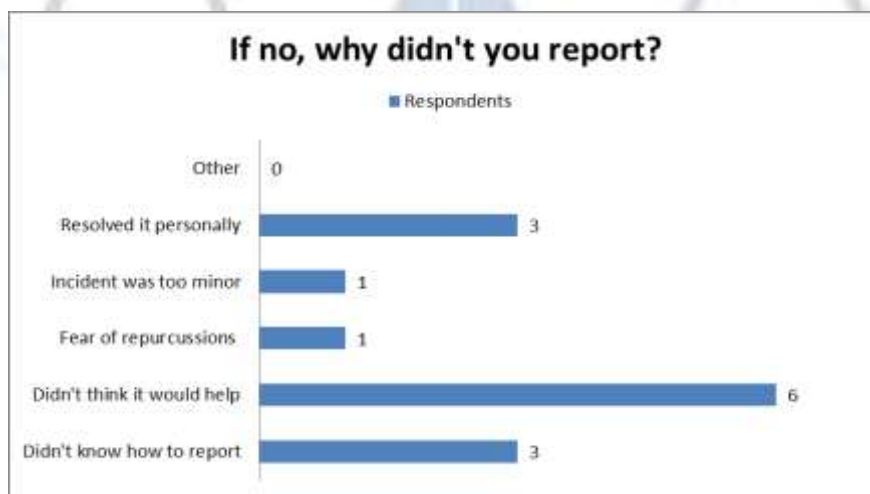
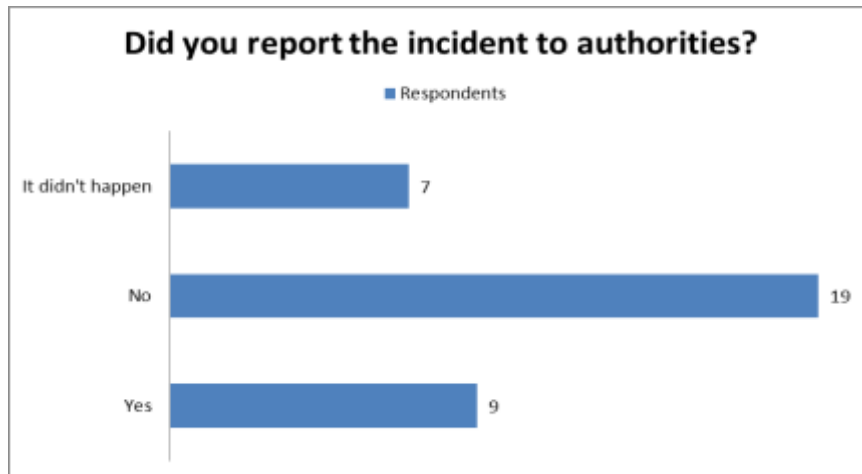
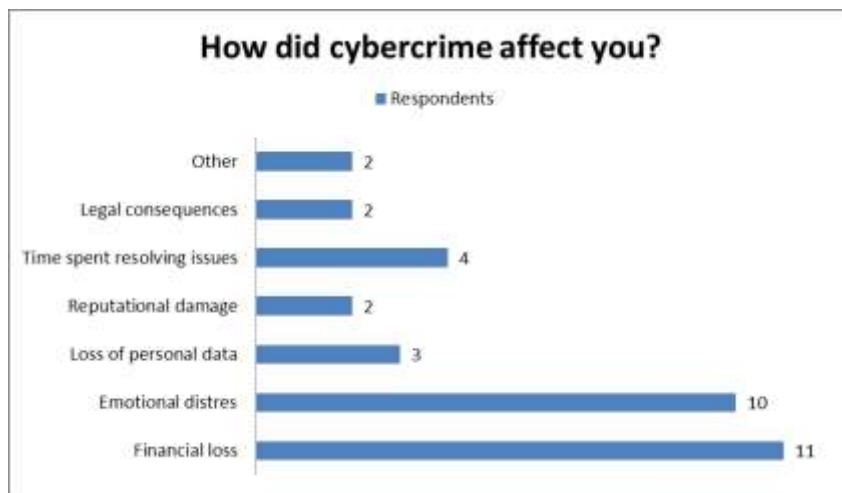




Personal experience with cybercrime -

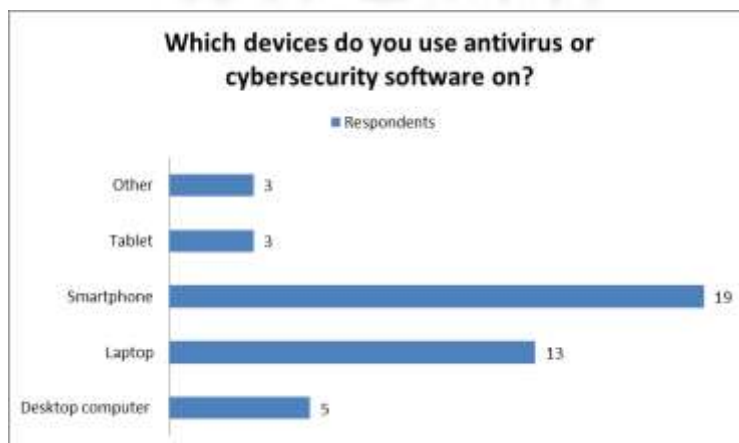
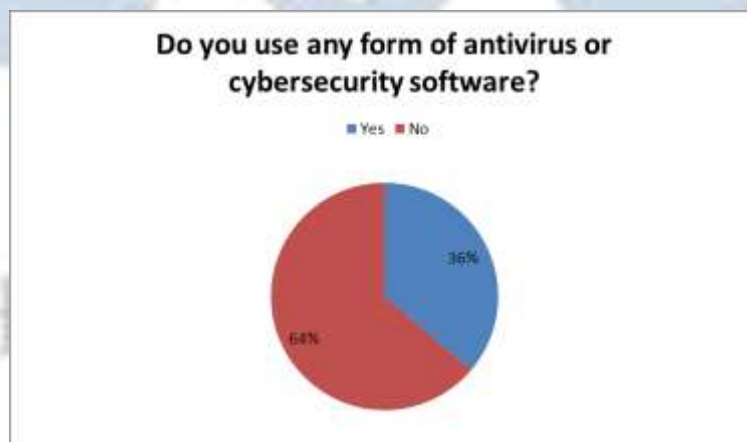
Among 51 respondents, 37 respondents have not been victims of Cyber Crime, 14 respondents have been victims of Cyber Crime. Among the victims of Cyber Crimes, 4 of respondents have experienced online banking fraud, Phishing and Cyber bullying, followed by data breach and identity theft and the rest are shared by categories. The maximum victims have suffered financial loss (11), followed by emotional distress (10) and time spent resolving issues (4) with the least number of respondents (2) suffering reputational damage and other categories. Almost 7 respondents didn't report the incident to authorities depicted in Figure (14) because respondents didn't think it would help (6) or didn't know how to report (3) or resolved it personally (3).



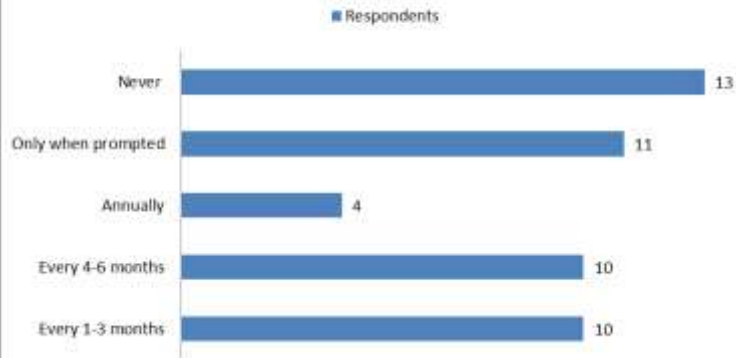


Cyber security practices –

Among 51 respondents, 17 respondents have used antivirus or cyber security software and the rest of the 30 respondents don't use any antivirus or cyber security software. Most of the respondents used antivirus on their smartphones, followed by laptops, desktop computers and tablets. The maximum respondents only change their password when prompted, followed by the respondents who change their passwords every 1-3 months and every 4-6 months and followed annually, and 13 respondents never change their passwords. The two-factor authentication for online accounts is used by 24 respondents and 24 respondents don't use the two-factor authentication for online accounts. Among the respondents, 19 people were somewhat cautious about opening their emails while 10 people were not cautious about opening their emails. A maximum number of respondents (49) have no formal training in cyber security in their workplace and educational institutions.

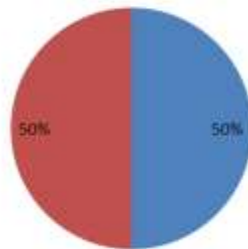


How often do you change your passwords?



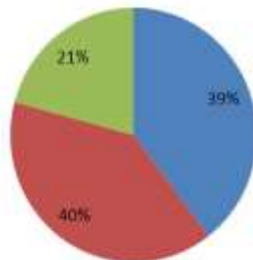
Do you use two factor authentication (2FA) for your online accounts?

■ Yes ■ No



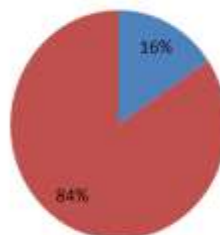
How cautious are you about opening emails from unknown accounts?

■ Very cautious ■ Somewhat cautious ■ Not cautious



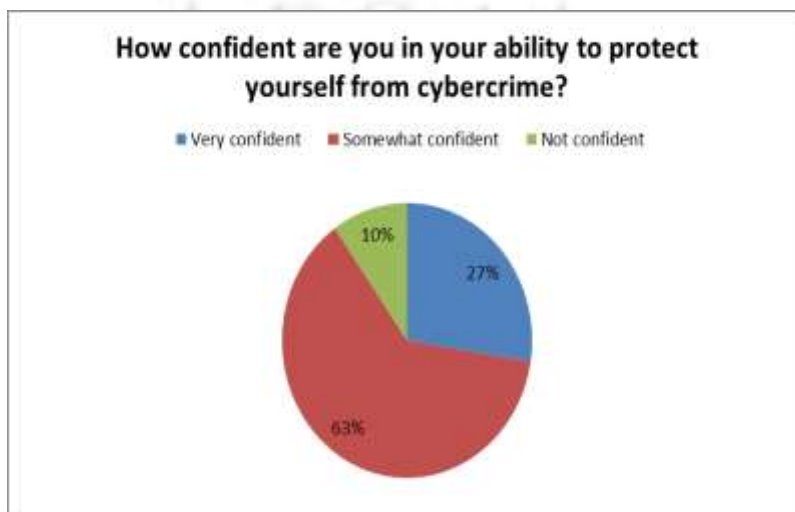
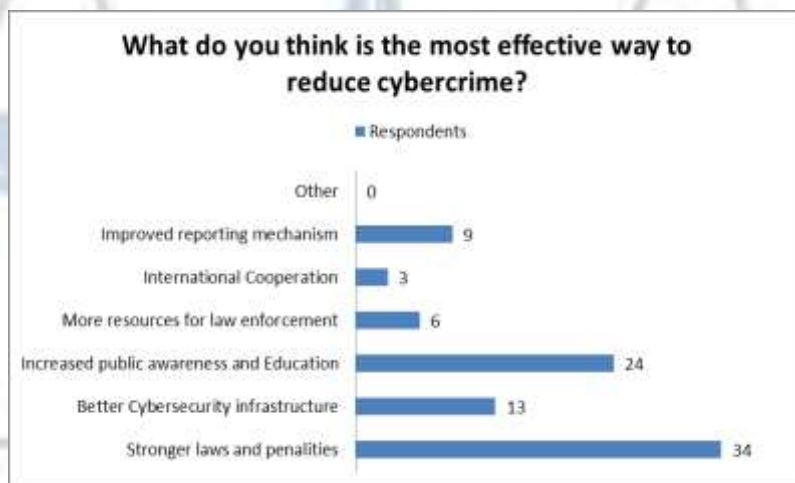
Have you received any formal training on cybersecurity at your workplace or educational institutions?

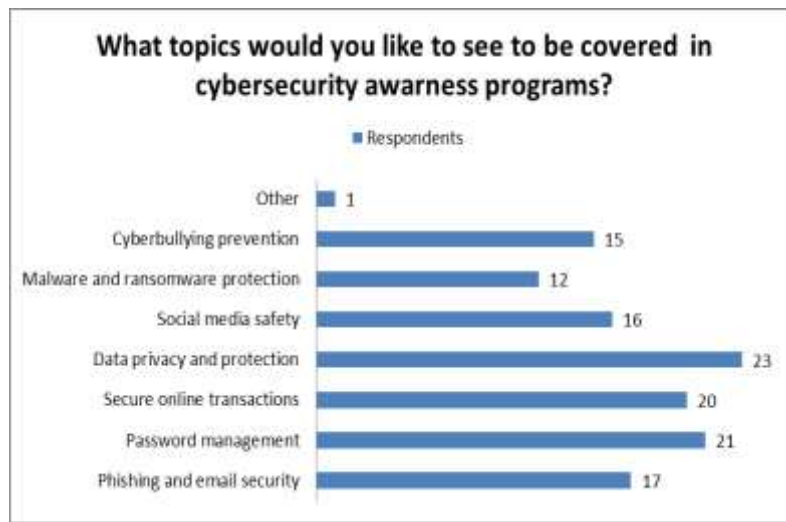
■ Yes ■ No



Attitudes and opinions -

Out of 51 respondents, 14 respondents are unsure of combating Cyber Crimes, and 33 respondents believe current laws are not sufficient to combat Cyber Crime. The most effective way considered to reduce Cyber Crime is stronger laws and penalties, followed by increased public awareness and education, following better cyber security infrastructure and other categories like international cooperation etc. The respondents have to rate their ability to protect from Cyber Crimes where 32 respondents were somewhat confident, 14 respondents were very confident, and 5 respondents were not confident. The maximum topic which respondents would like to see to be covered in the cyber awareness programme is data privacy, followed by password management, followed by secure online transactions and other categories. This followed the last question of additional comments.





The last question is about additional comments on cyber security and cybercrime awareness in which many people responded:

"Cyber Crime awareness is the need of the hour. Crime dealing mechanisms must be strengthened to track crime by giving training to officials. A separate wing to deal with cybercrime is needed. Cyber Crime awareness must be at different levels-student, citizens etc. through different modes of communication."

"In case of cyber bullying, a person shouldn't panic or get threatened instead lodging a complaint in the police or cyber department."

"Cyber teams should be well-trained and have strict penalties for doers. International tie-ups should be made for better enforcement."

"Stronger encryption methods for data and recommended cyber insurance." Cyber security should be made part of the school curriculum."

"Avoid disclosing more personal data or email ID in food courts or malls, considering reliable security software as a better approach to comprehensive protection of our devices."

Discussion –

The survey conducted shows that social media plays a crucial role in educating and awaring people regarding cyber-crime and its prevention. Social media campaigns help in spreading awareness. It indicates shocking results on the notion that a majority of urban individuals do not have professional training in cyber-crime and also do not update their knowledge regarding it. This is in contrast to the popular perception that urban elite would be specialised in formal cyber training. But fortunately, this number is ameliorating due to the initiative taken by the government authorities to educate people regarding the same. School is taking responsibility in educating students to combat this nefarious crime. The percentage of citizens falling into the cyber trap is comparatively less. Out of which, most of them fall into online shopping frauds which may lead to monetary loss, emotional distress, loss of personal data, etc. Majority of the

respondents have installed anti-virus software and use 2- factor authentication which expresses people's favour in terms of cyber- security, however majority of them only change their passwords when prompted which is a sincere concern. Ensure proper protection, attitude of the masses need to be changed as cyber- crimes would become a major problem in the near future due to the increasing role of AI. Many respondents were in support of the idea that there should be stricter laws and penalties so that these crimes could be reduced. They also believed that online secure transactions should be included in cyber-crime awareness programs. Overall, the regulations of the government and outlook of the people need to be changed to suit the changing legal and technological atmosphere.

Interview

As part of this research, we conducted a visit to the Punjab Cyber Crime Police Station, Phase 4, Mohali. During this visit, we interviewed the Police Inspector to gain insights into the functioning of the station and the current scenario of cybercrime in the region.

INTERVIEWER: What are the landmark cases solved in this station or are they still pending?

INTERVIEWEE: We have solved the famous case of a call Centre scam; it involved accused ranging from ages 27 to 32 years. One accused was a juvenile aged 17 years. A total of 155 were arrested, they were operating fake call centers and were using three different modus operandi to dupe foreign nationals by making them purchase gift cards of Target, Apple, Amazon, etc. And currently, we don't have any landmark cases pending.

INTERVIEWER: What is the most common and recurring cyber-crime in Punjab and Chandigarh?

INTERVIEWEE: The most common and recurring cybercrime in Punjab and Chandigarh is obscene content cases and financial fraud. Their averages are 30% and 70% respectively.

INTERVIEWER: What are the steps you have taken to create awareness among the citizens about cybercrime?

INTERVIEWEE: We conduct regular seminars in villages and for masses, also workshops are

set up for judges and other police personnel.

INTERVIEWER: Have you encountered any cybercrime related to AI?

INTERVIEWEE: No, we have never encountered any cybercrimes related to AI. They are mostly handled at the Centre level.

INTERVIEWER: How many students under 18 are affected by this crime?

INTERVIEWEE: Till now in cases reported to us not many students under 18 are involved, as they generally don't report their problems due to taboo.

INTERVIEWER: Cybercrime happens the most in which age group?

INTERVIEWEE: Cybercrime victims are mostly senior citizens because they are gullible and have more money.

INTERVIEWER: What are the punishments given to cybercriminals? Do you feel that stricter laws should be introduced to punish these criminals?

INTERVIEWEE: Mostly cybercriminals are punished according to the Criminal law or IT ACT, but they are not very strict, and the implementation also suffers because of it so the government needs to strengthen it, and they are introducing some amendments according to the news.

INTERVIEWER: Recently a case was discussed regarding a student at a school leaking morphed videos of his fellow classmates on an online website. Was this station involved in this incident and what measures should be taken to make these students cyber-aware?

INTERVIEWEE: No, we were not involved in it as the FIR was lodged in Sector 74 Mohali, and the students can be made cyber-aware by way of conducting interactive seminars, workshops and social media.

INTERVIEWER: Do you feel that our mobile camera takes our picture every 5-10 seconds to record our movement? Do you feel that our phone spies on us?

INTERVIEWEE: According to me our phones are not doing that but the apps that we allow to have our microphone and gallery access can spy on us. That is why before allowing these apps to do so we should read their terms and conditions carefully.

INTERVIEWER: Which loopholes are present in cyber law according to you?

INTERVIEWEE: The major loophole is the lack of resources and social media, and the rumors mitigated there.

INTERVIEWER: How can international cyber-crimes be reduced and mitigated?

INTERVIEWEE: It can be reduced by international cooperation, and it needs to be easy even though it still works quite well due to the MLAT signed with 148 countries.

INTERVIEWER: How many cases are reported per year?

INTERVIEWEE: Last year we received 37 cases and, in the year, currently we have received 16 cases.

INTERVIEWER: What is the most challenging thing to do for a cyber – crime official?

INTERVIEWEE: As a cybercrime official, the most challenging aspect is staying ahead of rapidly evolving cyber threats and technologies. Tracking and identifying anonymous cybercriminals operating globally adds complexity to our investigations. Limited resources and jurisdictional issues further complicate our efforts. Ensuring continuous training and maintaining a balance between privacy and security are constant hurdles we face.

The interview underscored prevalent cybercrimes in Punjab and Chandigarh, with a focus on financial fraud and obscene content cases. Despite notable successes, addressing resource constraints and enhancing legal frameworks are crucial for effective cybercrime management in the region.

Conclusion

As our research focused on cybercrimes in India, our objective was to comprehensively understand the extent and nature of cyber threats faced by the population. We found that while there is a notable level of awareness regarding cybercrime, evidenced by community seminars and workshops, there remains a gap in understanding the complexities and evolving nature of cyber threats. This highlights the necessity for continuous education and awareness initiatives to empower individuals and organizations with the knowledge to protect them effectively. Moreover, our study revealed that despite existing legal frameworks, there are challenges in enforcement due to resource limitations and jurisdictional complexities. Strengthening these frameworks with more stringent laws and enhancing their implementation could serve as significant deterrents against cybercriminal activities. By fostering a collaborative approach between law enforcement, policymakers, and the public, we can better address the dynamic landscape of cyber threats and ensure a safer digital environment for all residents of India.

Bibliography

- **Books -**

→ *"Cyber Law in India"* by Farooq Ahmad

→ *"Cyber Crime in India: Problems, Perspectives and Solutions"* by Dr. Vishwanath Paranjape

→ *"Cyber Crimes against Women in India"* by Debarati Halder and K. Jaishankar

→ *"Cyber Security and Cyber Laws"* by Alfred Basta and Nadine Basta

- **Online links -**

→ <https://www.businessupturn.com/technology/cyber-security/india-ranks-80th-in-local-cyber-threats-despite-booming-6-billion-cybersecurity-market/>

→ <https://blog.neoncyberspace.in/india-ranks-80th-globally-in-cybercrime-targeting-report-reveals/>

→ **Blocked over 74 mn local threat incidents in India last year: Kaspersky | Tech News - Business Standard**

→ **Evolution in the world of cyber crime | Infosec**

→ **The Biggest Cyberattacks in History: A Historian's Perspective**

→ **How oversharing on social media could put your personal information at risk**

→ <https://www.welivesecurity.com/2018/06/29/oversharing-social-media/>

→ <https://www.aura.com/learn/dark-web>

- **Research paper -**

→ *Research paper on Cyber crime against women India from COVID to the Presentera by Radha Rajan and Jivantika Gulati*

→ *Research paper" Cyber crime Changing everything - An empirical study" by Nilesh Jain and Vibhash Shrivastava*

→ *Cyber crime & digital evidence – Indian perspective authored by Rohas Nagpal*

- **Newspapers -**

→ *The Hindu, The Hindustan Times, The Times of India, Deccan herald and The Mint*

- **Bare act -**

→ *Information Technology Act, 2000*

→ *Indian Penal Code, 1861*



WHITE BLACK
LEGAL