IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

EVALUATION OF CYBER SECURITY THREATS AND ITS IMPACT ON SOCIAL MENTAL HEALTH

Dr. Nimbalkar A.B.[1] , Manisha Gadekar[*]

[1]Department of Computer Science, PDEA's Annasaheb Magar Mahavidyalaya, Hadapsar, Pune, Maharashtra, India

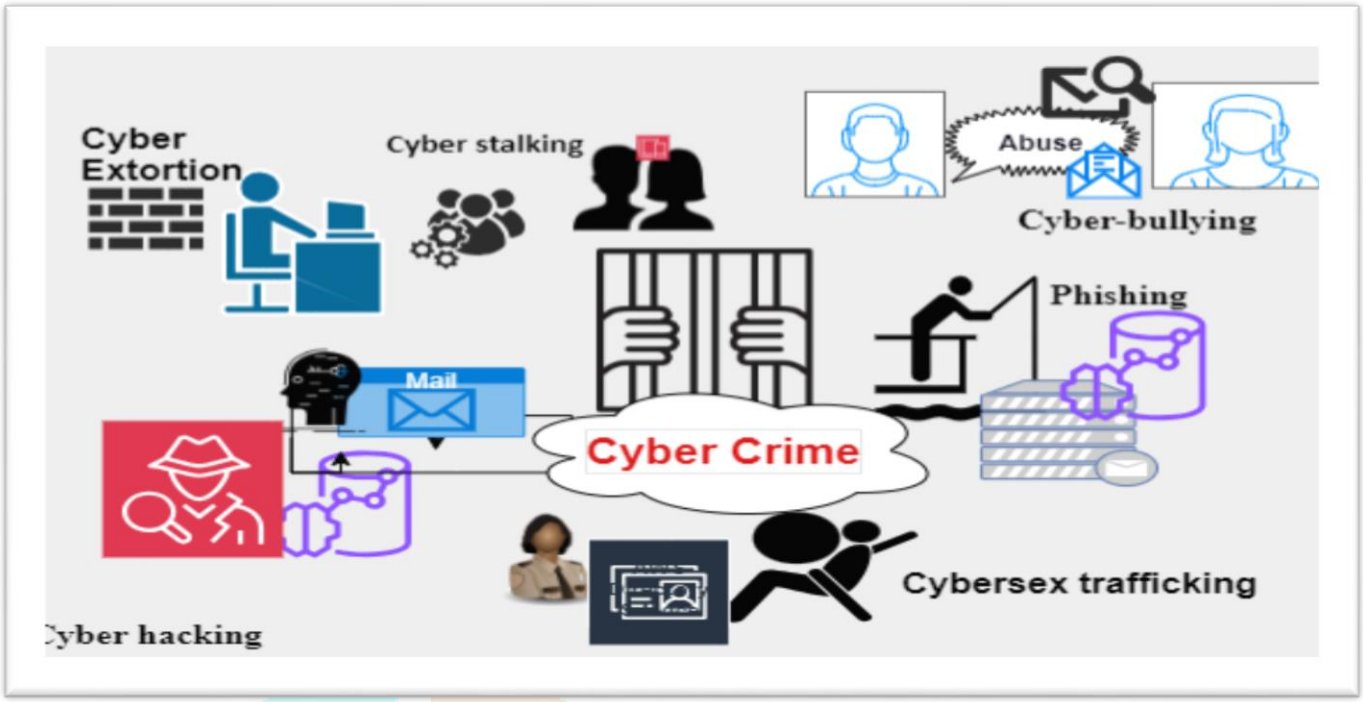
Abstract

Crime is nothing but illegal behavior or activities and which people are punished. Cyber-crime is nothing but person who has done something illegal or criminal activity that either victim or uses a computer or laptop, a computer network or a networked device. Cybercrime is committed by cyberpunk (cyber-criminals or cyber crooks) or hackers who want to make money. Cyber-crime aims to harm or destruction computers or networks for reasons other than profit, these could be political or personal. Cyber-crime can be executed by individuals or organizations. Some cyber crooks are organized, use advanced techniques and are highly technically skilled. Others person who is beginning to learn a job or an activity and has little or no experience or skill in it.

Keywords:

Cyber-attack, Digital, Education, Threat, Type of Crime

Graphical Abstract



1. INTRODUCTION

India is one of the rapidly developing country where major population is addicted to the use of the internet in daily use. During Covid 19 pandemic lockdown period, the major money transactions was done by the online mode using the apps like Gpay, BHIM, phonepay, and Paytm. During the pandemic period, there was extensive use of the internet for study, entertainment, job work, and online shopping (Menasinkai, and Patil,, 2021). In Tamil Nadu,digital tools were used for the agricultural marketing during the Covid-19 lockdown period (Pandi et al., 2023).This leads to the emergence of cyber-crime. This review, discusses the concepts about the cyber-crime like cyber extortion, phishing, cyber extortion(sextortion), cyber bullying, cyber stalking, cyber hacking and trafficking.

1.1 Cyber Extortion

Having a successful business thanks to the internet is great. Though, criminals who are always focus for ways to ravage human can also use the internet for unethical achieve. Organization have special or private information that they keep secure from the exposed. Cyber extortion is the term for the illegal behavior wherein cybercriminals utilise such information to demand money from organizations. Cybercriminals or hackers may also use cyber extortion, also referred to as cyber blackmailing, as a means of intimidating a target or corporation by threatening to reveal confidential data. The attackers generally demand money in return for not disclosing confidential information also demand a ransom for not rupture the systems. Types of Cyber Extortion are blackmail, Ransomware and Denial–of–Service (DoS) etc. Example of Cyber Extortion an email exchange between

organization's higher authorities contains confidential information that can benefit their business rivals. Cybercriminals might threaten to reveal this data to their competitors. Spread by spam emails or dubious websites, infectious malware is often the first step in cyber blackmail (O'Malley et al., 2022).

1.2 Cyber Phishing:

Cybercriminals send fictitious emails with links to certain webpages in an attempt to coerce the recipient into divulging personal information like passwords and contact data or with the intention of infecting the recipient's device with harmful viruses as soon as the link is opened in order to profit. These emails and texts popup to be authentic way. Then, using the victim's bank account and private information, the attackers carry out dubious transactions from the victim's bank account to their own. Types of phishing are spear phishing, whaling, vishing and email phishing etc. Phishing email attack examples Social engineering takes use of people's innate desire to trust other people and businesses (Barraclough et al., 2021).

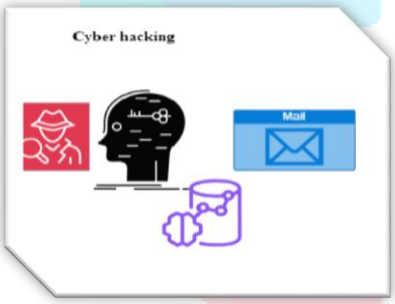
1.3 Cyber stalking:

Cybercriminals using technology and the internet (online) to harass or stalk a person is known as cyberstalking. It can be looked into as a continuation of both physical and online stalking. It can be looked into as a continuation of both physical and online stalking. Though, stalking takes form of, e-mails, social media posts, text messages and other mediums and is frequently persistent, conscious, and well planned. Cyberstalking begins with a seemingly innocent contact that develops into a systematic, upsetting, or frightening behavior. Types of Cyberstalking Catfishing, Monitoring check-ins on social media, Hijacking webcam, Spying via Google Maps and Google Street View, Tracking location with geotags. Example of cyber stalking Engaging with all online posts made by the victim , Posting offensive, suggestive, or rude comments online, Sending unwanted gifts or items to the victim etc (Stevens et al., 2021).

1.4 Cyber-bullying:

Cyberbullies are people who send texts, emails, or instant messages via the internet, computers, cellphones, or other electronic devices; they also make remarks on social media or in chat rooms; or in other ways use private or public forums to attack their victim in order to harm or frighten them.To hurt or terrify someone else, particularly by sending them offensive texts or by using other means, including using public or private forums to abuse their victim. Cyberbullying is mainly happening in a child, preteen, or teen is threatened, harassed, humiliated, embarrassed, or targeted through the internet, interactive and digital technologies, or electronic devices by another individual of the same age range (Agatston et al., 2007). Types of Cyberbullying Harassment, Outing/Doxing, Exclusion, Fraping etc. Example of cyber bullying are Hate speech, pejorative labels, or defamatory false accusations, ganging up on a victim by ridiculing them in online forums and discussions, posting rumors about the victim online to convince others to dislike or participate in their online denigration. Forty-one measures are required to avoid cyber bullying (Vivolo-Kantor et al., 2014).

1.5 Cyber hacking:



The act of intentionally exploiting vulnerabilities in a company's computer network is known as cyber hacking, where it can be used for objective such as stealing confidential information or compromising, disturbing communication or procedures, or to satisfy other harmful objectives. Cyber hacking, also known as cyber attacking. Hacktivists, Green Hat, Blue Hat, Red Hat, Black Hat, Grey Hat, White Hat / Ethical Hackers, Script Kiddies, and Malicious Insiders are some of the several types of hackers or Whistleblower**,** State/Nation Sponsored Hackers etc. Examples of cyber hacking are like false news and information now than ever before. After clicking on malicious URLs, the women were the victims of cyber hacking, malware downloaded all of their personal information to their phones, turned on the microphone and camera, and took their intimate photos and videos etc (Xu et al., 2018).

1.6 Cybersex trafficking:

Cybercrime and a type of modern slavery is cybersex trafficking, also known as online sexual exploitation. The act of broadcasting, recording, or photographing a victim participating in sexual or personal actions from a central location and then selling the content online to customers and sexual predators is known as cybersex trafficking. Women have been sexually abused by the criminals who have coerced, threatened, and blackmailed them into engaging in cybersex trafficking. In the midst of the pandemic, perpetrators targeted women with online sexual assaults, manipulating their images for use in pornographic content (Raines, J., 2022).

1.7 Criminals :

People and surroundings have a big influence. For example, a child raised in a well-mannered home with strong moral standards is less likely to turn to crime, even if they have genes that could otherwise lead them in that path. Physical aspects of the environment, including topography, geography, pollution, crowded areas, and leisure options. These ecological elements can influence an individual's physical and mental development throughout their life, as well as the degree of anger, fear, or well-being they experience on an ongoing basis. According to Gottfredson and Hirschi (1990), criminal behaviour is a type of strategic behaviour defined by low self-control, self-centeredness, and disregard to the needs and suffering of others. Criminals who conduct political offences like election fraud or terrorism want to acquire symbolic resources like prestige or power. They also try to obtain money through gambling and drug trafficking, which may be swapped for material goods. People find enjoyment obtaining resources that heighten pleasant feelings or lessen bad feelings in crimes as knock-associated theft, sexual assaults, and illegal drug usage.

1.8 Analysis of data

The records below are those that the National Crime Records Bureau (NCRB) has evaluated. In accordance with the Indian Penal Code (IPC) and Special and Local Laws (SLL), it is an Indian government organisation tasked with gathering and evaluating crime data. Founded in 1986, NCRB was intended to serve as a database of criminal activity and information to help detectives connect the dots between crime and its perpetrators. In accordance with the Task Force's 1985 suggestion and the National Police Commission's 1977 recommendation, it was established by the merger of the Central Fingerprint Bureau, the Inter State Criminals Data Branch, and the Directorate of Coordination and Police Computer (DCPC) of the Police Bureau. Data was collected from the website https://ncrb.gov.in/ and https://www.mha.gov.in/en/national-crime-records-bureau-ncrb for the years 2015 to 2021 and represented in the format of bar diagram.

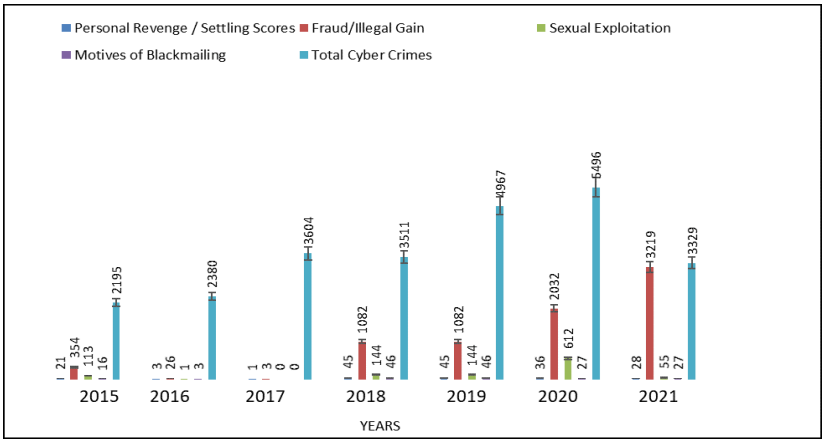


Fig 1 :Cyber Crimes in Maharashtra

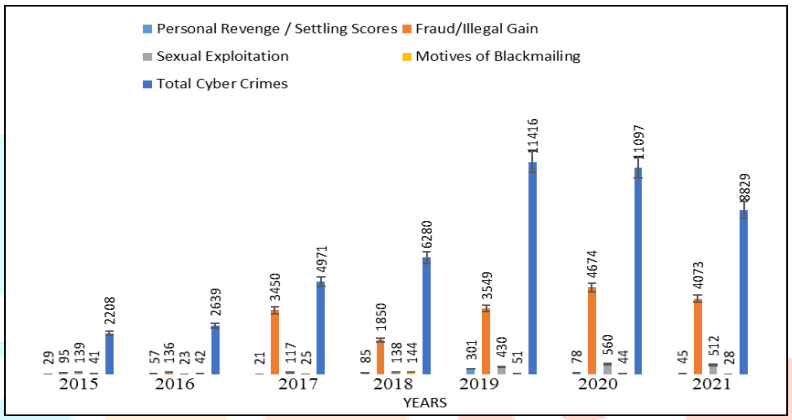


Fig 2: Cyber Crimes in Uttar Pardesh

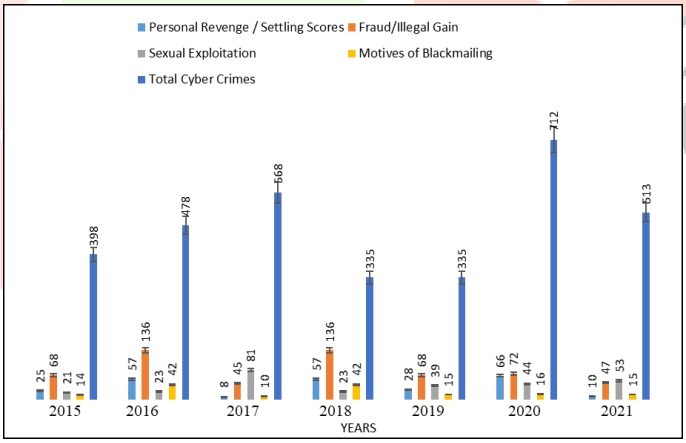


Fig 3 : Cyber Crimes in West Bengal

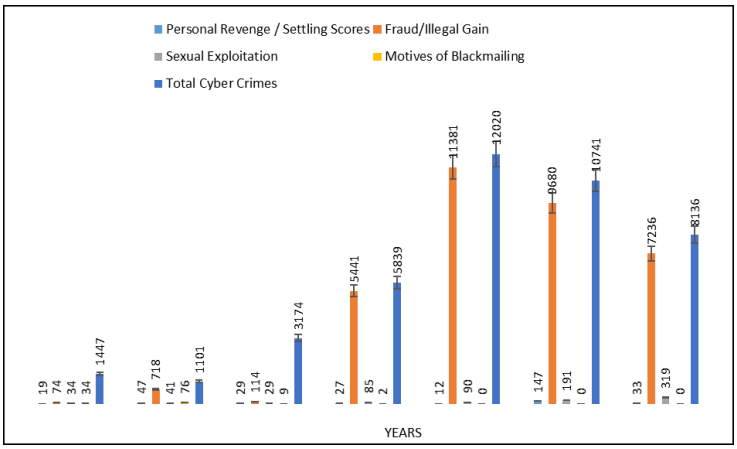


Fig 4: Cyber Crimes in Karnataka

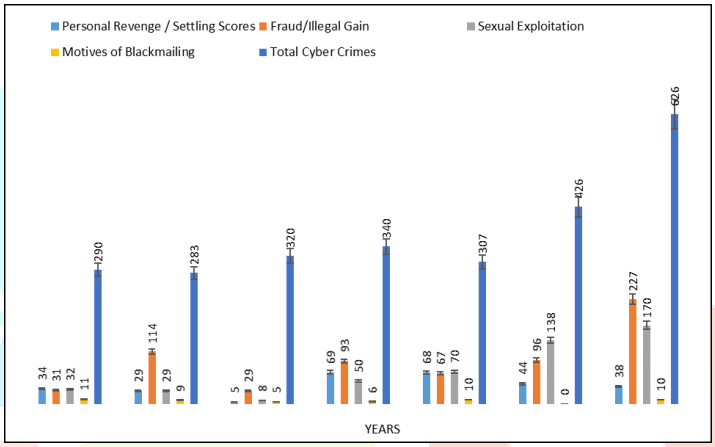


Fig 5 : Cyber Crimes in Kerala

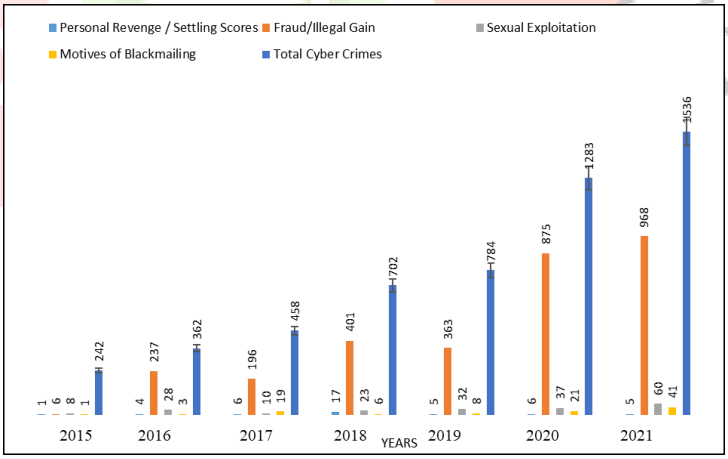


Fig 6 : Cyber Crimes in Gujarat

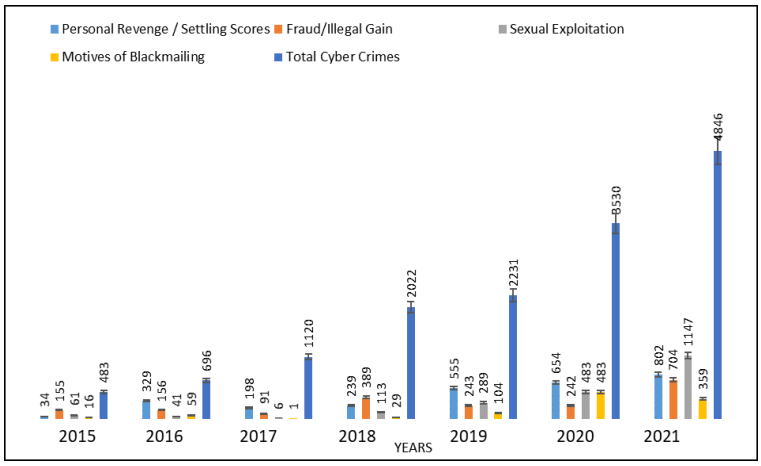


Fig 7 : Cyber Crimes in Assam

As per the data, cybercrime was at peak level during Covid 19 pandemic period in all the states of India.

1.9 Cyber Laws in India:

Cyber laws in India are contained in the Information Technology Act, 2000 (often known as "the IT Act"), which went into effect on October 17, 2000. The primary goals of the Act are to expedite the filing of electronic records with the government and to provide electronic commerce legal status.

Cyber laws include the following Acts, Rules, and Regulations:

• Information Technology (Certifying Authority) Regulations, 2001;
Information Technology Act, 2000;
Information Technology (Security Procedure) Rules, 2000;
Information Technology (Certifying Authority) Regulations, 2004
The entire body of Indian law that severely regulates cybercrimes is based on the IT Act (MEIT, 2000).

1.9a National Cyber Security Policy : A National Cyber Security Policy has been developed by India to offer a structure for dealing with cybersecurity risks. The goals of this policy are to promote a safe cyber ecosystem, develop capacities to stop and neutralise cyberthreats, and safeguard data and information infrastructure in cyberspace.

1.9b Legal and Regulation Framework: The Information Technology (IT) Act, 2000, and its later revisions are among the laws and regulations that India has passed to address cybersecurity issues. Cybercrimes are defined by these regulations, which also specify punishments for offences involving hacking, illegal access, data breaches, etc.

1.9c CERT-In: In response to cybersecurity issues, the Indian Computer Emergency Response Team (CERT-In) acts as the national nodal agency. In addition to offering cybersecurity awareness and training programmes, CERT-In offers early warning, detection, and response to cybersecurity issues. When dealing with cyber incidents that start outside the nation, the CERT-In collaborates with its counterpart authorities abroad.

1.9d Public-Private Partnerships (PPPs): Addressing cybersecurity concerns requires cooperation between institutions of higher learning, the commercial sector, government agencies, and civil society. PPPs enable coordinated efforts to counter cyber risks, capacity building, and information exchange. Cyberbullying is not specifically covered by legislation in India. The Information Technology Act's Section 66A outlined the penalties for offensive and bothersome remarks made online.

1.9 e Cyber Awareness Campaigns: Creating a society that is aware of cybersecurity issues requires educating the public about cybersecurity best practices. The government launches awareness initiatives to encourage safe online conduct and increase public knowledge of cyberthreats, in collaboration with industry stakeholders. Computer contamination is defined in Section 43 and tampering with computer source materials in Section 65.

2.0 Control Measures of Cyber Security For Personal Level In India

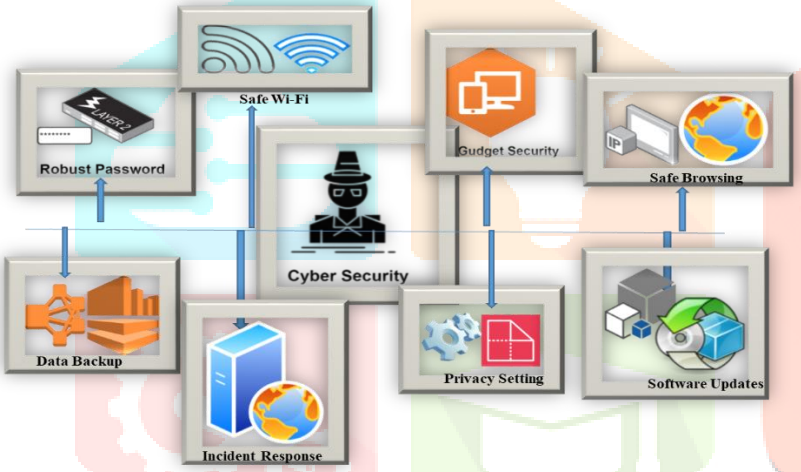
2a Robust Passwords: Create strong, one-of-a-kind passwords for every online account, and if feasible, enable multi-factor verification. Use password managers to safely store and manage passwords instead of utilising simple, easily guessed passwords.

2b Frequent Software Updates: Apply the most recent security patches and updates to antivirus, operating systems, and application software. Update computers, mobile devices, and other devices linked to the internet on a regular basis to guard against vulnerabilities that have been identified.

2c Privacy Setting: To manage the quantity of personal information disclosed publicly, check and modify the privacy settings on web browsers, social media sites, and other online services. Be careful about sharing information online and restrict the visibility of personal data.

2d Data Backup: Frequently store critical files and data on external drives or cloud-based services. Keeping backups can assist in restoring encrypted or lost data in the event of a ransomware attack or data breach without having to pay a ransom.

2e Email and Messaging Secure: Be cautious when clicking links in messages or opening attachments in emails, especially from senders you don't know or are unsure of. Before replying or acting upon unusual emails, be cautious of phishing attempts and make sure they are legitimate.



Mitigation Of Cyber Security

2f Safe Wi-Fi Networks: Safe Wi-Fi networks at home that use encryption techniques like WPA2(Wi-Fi Protected Access 2) and strong passwords. Steer clear of public Wi-Fi networks when doing critical tasks like online shopping or banking since they can be vulnerable to man-in-the-middle attacks and eavesdropping.

2g Safe Browsing Tips: Be cautious when opening files or clicking links from unidentified or dubious sources. Phishing emails, spoof websites, and harmful links that aim to infect your computer with malware or steal your personal data should be avoided.

2h Gudget Security: Guard devices against viruses, malware, and other harmful software by using trustworthy antivirus software and security tools. If you want to increase security against theft or loss, turn on device encryption and remote tracking on your laptops and smartphones.

2i Incident Response Plan: Identify theft, financial fraud, and unauthorised account access are examples of cybersecurity issues. Create an incident response plan. Be aware of the proper channels for reporting cybercrimes to law enforcement, and act quickly to lessen the effects of security breaches.

3.0 Conclusion

To improve the nation's economy, always transact on safe and secure websites. The government court will receive serious complaints about online transactions as part of the remediation rate for cyber legislation and the acknowledgement of electronic documents. Security flaws were resolved by the firms' authority to improve data security requirements and guarantee that the companies used private information appropriately. Communities can empower people to protect themselves online, seek help when necessary, and help create a safer and more compassionate digital environment by educating others about cybercrime and its connection to mental health. To inform people about the various forms of cybercrimes, such as phishing scams, identity theft, online harassment, and cyberbullying, start public awareness programs. Promoting awareness of the possible negative effects cybercrime might have on one's mental health is a good idea for these efforts. In order to educate kids about online threats and how to defend themselves from cybercrimes, schools should implement digital literacy and cyber safety programmes. Form alliances with tech firms, law enforcement agencies, women's organizations, and advocacy groups to create cooperative projects that combat cybercrime against women. Stakeholders can adopt more effective solutions for support, intervention, and prevention by combining their resources and knowledge. Enable women to recognise phishing attempts, manage passwords, and protect personal data online by offering them thorough cybersecurity best practices education and training. Create and share easily accessed materials, such infographics, films, and tip sheets, that provide helpful advice on defending against online dangers. These tools should cover common threats that women encounter, like intimate partner abuse, online harassment, and stalking, and offer detailed advice on how to secure accounts and devices. Encourage women to participate in online forums and peer support networks where they can give advice, offer mutual support, and share experiences related to overcoming obstacles linked to cyberspace. These networks can act as safe havens where women can talk about delicate subjects and get help without worrying about being judged or stigmatised. Educate women about their legal rights and available channels of support when they are the victims of online abuse, including revenge porn, cyberstalking, and cyber-harassment. Encourage women to critically assess online content, spot deceptive methods, and confront damaging preconceptions and attitudes that are reinforced in digital settings by incorporating media literacy components into cyber awareness campaigns. Women's resistance to cyber-exploitation and manipulation can be increased by giving them the skills to be astute consumers of information online. To enable women to take action against offenders and pursue justice, provide them with information about pertinent legislation, reporting procedures, and support services. It is imperative to guarantee that women have prompt and considerate crisis intervention services, such as qualified specialists manning hotlines, helplines, and online chat assistance. When required, these services ought to provide mental health and legal resource referrals, as well as safety planning and emotional support.

References :

1. Agatston, P.W., Kowalski, R. and Limber, S., 2007. Students' perspectives on cyber bullying. Journal of Adolescent Health, 41(6), pp.S59-S60.

2. Barraclough, P.A., Fehringer, G. and Woodward, J., 2021. Intelligent cyber-phishing detection for online. computers & security, 104, p.102123.
3. https://ncrb.gov.in/
4. https://www.mha.gov.in/en/national-crime-records-bureau-ncrb

5. Menasinkai, P.A. and Patil, B.L., 2021. Digital inclusion as a gate way to easy digital payments. Journal of Pharmacognosy and Phytochemistry, 10(3S), pp.32-35.

6. O'Malley, R.L. and Holt, K.M., 2022. Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. Journal of interpersonal violence, 37(1-2), pp.258-283.

7. Pandi, P.R., Theodore, R.K., Kumar, D.S., Balasubramaniam, P. and Ganapathi, P.S., 2023. Utilization Behaviour of Digital Tools by Farmers for Marketing Their Produce during Covid-19 Lockdown Period. Asian Journal of Agricultural Extension, Economics & Sociology, 41(9), pp.834-840.

8. Raines, J., 2022. Trafficking Without Borders: Why it is time for the law to properly address cybersex trafficking in the livestreaming context. Cath. UL Rev., 71, p.197.

9. Stevens, F., Nurse, J.R. and Arief, B., 2021. Cyber stalking, cyber harassment, and adult mental health: A systematic review. Cyberpsychology, Behavior, and Social Networking, 24(6), pp.367-376.
10. Vivolo-Kantor, A.M., Martell, B.N., Holland, K.M. and Westby, R., 2014. A systematic review and content analysis of bullying and cyber-bullying measurement strategies. Aggression and violent behavior, 19(4), pp.423-434.
11. Xu, M., Schweitzer, K.M., Bateman, R.M. and Xu, S., 2018. Modeling and predicting cyber hacking breaches. IEEE Transactions on Information Forensics and Security, 13(11), pp.2856-2871.