IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Critical Study of Online Cybercrime and Its Effects onModern Indian Society

Ponam Yadav

The Bhopal School of Social Sciences (BSSS), Bhopal, M.P., India

ABSTRACT

In the current era of online processing, the majority of information is stored online and is thus responsible to cyberattacks. There are a large variety of cyber risks whose early behaviour is difficult to comprehend, making it difficult to limit cyberattacks in their early stages. Cyberattacks may be motivated in some way, as they may be executed unwittingly. Cybercrime refers to attacks that are carried out intentionally and have severe effects on society in the form of economic disruption, psychological disturbance, danger to national defence, etc. The restriction of cybercrimes is contingent upon a thorough investigation of their behaviour and comprehension of their effects on different societal levels. The present study of paper focused on cybercrimes, their effects on society to make society aware of and concerned about any illegal harm and the future developments against cybercrime. The present paper study focused on cybercrimes, their effects on society, and the future developments against cybercrime in approach to make society aware of and concerned about any illegal harm.

Keywords: - Cybercrime Effects, Society Awareness, Morden Society, Computers & internet, online scam, Cybercrime Damage

1. INTRODUCTION

The step of the modern period makes it impossible to use time as a performance-enhancing component. Only using the Internet is a viable option. The collection of millions of computers that function as a network of electrical links between the computers is known as the Internet. The Internet is linked to millions of computers. Everyone enjoys using the Internet, but there is also a negative aspect to it: criminality committed online. Cybercrime is defined as an act that is performed or neglected in violation of a law that forbids or commands it and that carries a sentence upon conviction. Cybercrime is any criminal behaviour that involves the use of computers, including unauthorised access to another person's computer system or database, data alteration or theft, and damage of hardware and data. Cyberworld, often known as the Internet, is expanding quickly, which has led to an increase in cybercrimes descriptiveinferences.

1.1 What does cybercrime mean?

Although the word "cyber-crime" has no universally agreed-upon meaning, it is used in this article to refer to "any crime that is assisted or performed utilising a computer, network, or hardware device." Networked computers and other information and communication technologies provide quick, anonymous, secure, and inexpensive multi-media communication. They may be used as a means of organisation and communication to further develop already- existing illegal activity, provide fresh methods for carrying it out, broaden the geographical scope of criminal activity, or develop new forms of criminal activity.

1.2 The Historical Evolution of Cybercrime

Online Crime Since the beginning of the digital era, criminals have used computers to aid their illicit acts. Criminals utilise computers in much the same way that they would use a lockpicking instrument or a counterfeiting machine. Criminals have discovered that using computers allows them to maintain an anonymity that was before impossible in society.

2. LITRATURE REVIEW

(Yarovenko & Rymar, 2023) Cybercrime is increasing exponentially in the modern world. This is a result of the widespread automation of various aspects of society. Detecting and preventing cybercrimes in a timely manner, allowing business entities and state authorities to respond rapidly to mass threats, is therefore an urgent issue. In practise, numerous strategies and tools are employed to combat cybercrime. Popular today are software and cyber-physical systems based on contemporary mathematical techniques. Effective technologies include artificial intelligence, neural networks, genetic algorithms, blockchains, robots, etc. In addition to such powerful tools, we believe that cybercriminal profiling should also be utilised.

(Choi & Parti, 2022) Modern technologies that have been applied to cryptography are used by criminals to get illicit benefits while remaining anonymous. Little research has been done in this area, despite the fact that developing effective preventative measures requires a knowledge of cybercrime utilising this approach. In order to better comprehend the two papers that make up the special edition of the International Journal of Cybersecurity Intelligence and Cybercrime, which covers everything from cryptocurrencies and the dark web market to password cracking, read this paper's synopsis of the two articles. At the International White Hat Conference in 2022, the articles were delivered by the top students in the paper competition.

(Mohsin, et al. 2021) Technology has spread computers and the internet. Business, education, and culture can now collaborate remotely. Open information has caused internet irresponsibility. People benefit and cybercriminals target them. Legal institutions must adapt to new technology to prevent abuse. Web users can share photos, text, videos, and audio. Websites offer many chances. They spread child sexual abuse, hate speech, and slander. Unauthorized distribution violates writers' and artists' IP rights. Online anonymity helps.

Miscreants act worse if they think they'll get away. "Cyber-stalking" targets people who post personal information on employment and marriage websites or social media. Sex-offenders may target women and children who give their contact information. Cyberbullying, child pornography, and others are digital crimes. Trafficking, uploading, appropriating, and spreading obscene and erotic content is a major cyber law violation today. Technology makes the world a village. Our global community is nearly distance-free. Globalization has impacted culture and economics. Thus, information technology has benefited humanity, but this paradigm shift in humankind is also reflected in crime. There are many negatives, and sadistic people are using them to commit cybercrimes.

3. OBJECTIVES OF THE STUDY

1. The main objective of the study focused on cybercrimes, their effects on society.
2. Cybercrime awareness among peoples of society.
3. Future developments against cybercrime that will make society aware of and concerned about any potential criminal harm.

4. MATERIAL AND METHODOLOGY

1. Tools of data collection

An instrument is assistance with required and related data that could be collected methodically to the subject material. Google Form was used to record responses. In a data set, we collected 151 responses based on that we conclude the data. The Survey process was the means for information gathering, which was used by the scholars for the determination of assembling information from the respondents. The Survey technique is the best way for gathering the maximum data in an organized technique.

2. Data Collection and Procedure

The research is constructed on primary information gathering from Google form and the data for the study was acquired from the respondents. The information was composed by a simple random sampling process. Belief and understandings of the respondents were composed through the Survey method. The scholar after building an understanding with the respondents defined the determination, importance, and meaning of the study.

5. TYPES OF CYBERCRIME

A. Computer & Internet are target in cybercrime

B. Using a computer as a tool

C. Using computers as a by-product of other crimes

D. Increase in computer-related crime

A. Computer & Internet are target in cybercrime

- Physical damage
- Data theft or loss
- The spread of viruses and worms
- software theft, hacking
- A self-replicating computer software known as a "computer virus" is designed to change how a computer functions without the user's knowledge or consent.

B. Using a computer as a tool

This category encompasses offences committed by altering the contents of computer systems or by using computers or their contents to facilitate an unlawful act. They could include sending emails, ransom notes, or computer content manipulation for theft, telecommunications fraud, or credit card fraud.

C. Using computers as a by-product of other crimes

This category encompasses traditional crimes, and with the invention of the computer, criminals have begun to use technology as a tool to further their activities. They involve the use of computers in traditional crimes like forgery, extortion, abduction, and other similar ones.Computers are being used to perpetrate these crimes.

D. Increase in computer-related crime

The relationship between crime and the use of computers and copyright infringement, software piracy, component theft, etc.

6. DIFFERENT FORMS OF CYBERCRIME

From terrorist groups to white collar crooks, from teenagers to adults, everyone uses computers. Conventional dress code is similar Computers are being used to communicate for anything from export to import to kidnapping and other related activities. Different Forms of Cybercrime are:-

1. Hacking-In plain English, "hacking" refers to unauthorised access to a computer system without the owner's or user's consent.

2. Denial-of-service assault-This is a criminal conduct in which the perpetrator saturates the victim's network with traffic or overflows his email account with spam, depriving him of the services he is legally allowed to receive or offer.

3. Virus Transmission-Harmful programme that integrates with other apps (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious software).

4. Software theft-This crime involves the theft of software via the unauthorised duplication of original software or the production and sale of imitated goods. Global retail revenue losses are on the rise, and this crime may be committed in a number of methods, including end-user copying, hard disc loading, counterfeiting, illegal internet downloads, etc.

5. Pornography-The first continuously profitable e-commerce product is pornography. Pornography entices clients to enter their websites via deceptive marketing strategies and mouse capturing technology. Anyone, including youngsters, can use a computer to connect to the internet and click a mouse to view websites containing pornographic material. According to the terms of section 67 of the Information Technology Act of 2000, it is unlawful to publishor send any content in electronic form that is lewd or appeals to the desires of the genitalia.

6. IRC Crime- Internet Relay Chat (IRC) servers feature chat rooms where individuals from all over the globe may assemble and converse. Criminals utilise it to connect with potential accomplices. It is used by hackers to share strategies and discuss their vulnerabilities. Chat rooms are used by paedophiles to seduce young children. In cyber stalking, a woman's phone number is distributed to third parties under the guise of wanting to befriend a guy in order to harass her.

7. Credit card fraud- For online purchases, just enter the credit card number into the vendor's website. transaction, and if electronic transactions are not encrypted, hackers may use this card fraudulently by impersonating the card's owner. Counterfeiting: replicating authentic credit cards and using them for illicit purposes Lost/Stolen: unlawful use of a credit card due to its loss or theft Identity Theft: acquiring the personal or financial information of another person with the intent of engaging in fraudulent actions under that person's identity.

8. Net extortion-To extort a substantial sum of money from a firm by copying its secret data.

9. Phishing- It is a method of obtaining sensitive information from bank/financial institution account holders via deception.

10. Spoofing

Obtaining access to other computers on a network by having one computer on the network assume the identity of another computer, generally one with specific access rights.

11. Cyber stalking

The Criminal stalks the victim by sending encrypted emails and frequenting chat forums in order to get credit card data.

12. Cyber defamation-The offender sends defamatory emails or publishes defamatory content on a website to everyone who are associated with the victim.

13. Threatening-The perpetrator sends threatening emails or interacts with the victim in chat rooms. Anyone dissatisfied with their job, friend, or official may do this.

14. Salami assault-In such crimes, the perpetrator makes tiny modifications in such a way that they go undiscovered. The criminal creates a software that deducts a tiny monthly sum from the accounts of all bank clients and deposits it into his own account. In this scenario, no account holder would visit the bank for such a tiny sum, but the criminal will get a substantial sum of money.

15. Sale of illicit preparations- On the Internet, drugs may be sold and purchased. There are websites that offer the sale and delivery of illegal substances. They may utilise stenographic methods to conceal the communications.

16. Email-related offence

- Email spoofing
- Transmitting dangerous malware through email
- Email bombing
- Sending ominous emails
- Insulting emails
- Email scams

17. Hacker Profile- The word "hackers" is now used to describe those who breach into computers. Hackers might be of any age, religion, or country of origin. Due to their exploits in recent years, hackers have developed a terrible reputation. Hackers may engage in illegal conduct for the thrill, the challenge, or financial gain. Hackers are often young men with exceptional brains and curiosity. There has been an upsurge in the number of women with the ability to hack into computer systems. Hackers may organise themselves into hacking groups, which may sometimes compete with one another to determine whose group can exploit the most systems within a certain time period.

18. Internet Criminals- The introduction of the Internet enables cybercriminals to commit a crime from a computer located distant from the real location of the crime. A burglar on another continent may get into a computer network and take a credit card and financial information without being physically present at the crime site. Using a computer and the Internet, criminals engage in unlawful activities such as drug trafficking, child pornography, and bank fraud, among others. Officials in law enforcement must be informed of the many strategies used by criminals and how to react to this evolving crime scene. Criminals may also create cyber gangs that are distributed around the continent. They use the abilities of persons who may be adept in breaking into 55 data bases. These cybercriminals often identify themselves to the group by "handles" or "NICs."

7. THE COSMOS BANK CYBERATTACK – A CASE STUDY

One of the types of cyberattack, malware attack's recent a case in cosmos bank in 2018 has been observed.

7.1 Biggest cyberattack in recent

One of the first cooperative banks to be created in India was the Cosmos Bank cooperative bank Ltd. Cosmos Bank was the most recent victim of a significant hack in august 2018. Hackers stole the information of several Visa and Rupay debit card owners by breaking into the bank ATM switch server in Pune. On August 11, the information was utilised to conduct about 12000 fraudulent transactions across 28 countries, with an additional 2841 transactions taking place in India. The incident continued two days later on August 13 when another bank system was compromised by malware, and money was sent through SWIFT to the Hanseng, Hong Kong, account of ALM Trading Limited. The assault caused 94 crores, or 13.5 million USD, in total damages. Cosmos Bank was compelled to stop doing business and discontinue its online and financial services. One of the first cooperative banks in India was founded in 1906: The Cosmos Bank Cooperative Bank Ltd. The bank has its headquarters in Pune in the Cosmos Tower, which is close to Ganesh hind Road in Shivajinagar. Headquarters: Pune, India; Sector: Commercial Banking; Financial & Banking services.

7.2 Timeline

- On august 11, the hackers cloned the card details and did over 12000 card transactions and transferred rupees 78 crore out of India.
- The fraudulent transaction was carried out on 11 august and on 13 august 2017 through 25 ATM located in Canada, Hongkong and few in India (10:00 pm IST)
- A complain has been filed with Pune police about the malware attack and the bank is doing internal audits to investigate the breaches on 14 august 2017(4:00AM IST)
- AS a precautionary measure, the bank has closed all its server and net banking facilities, according to the officials (14 august 5:00 AM IST)
- Realising the cyberattacks the bank then registered an FIR with the Chatusringi police station on 14 august 2018, (6:00 AM IST)

7.3 Vulnerability

- Infrastructure was not fully updated
- Imanage/ file site patch was not installed
- Multi factors authentication was not enabled for users
- Lack of training and education in IT security team and user.

7.4 Overall Summary

Banks software and infrastructure was not fully updated. Most of the data was saved on premises server. file server patch was not installed though it was scheduled. Lack of communication between different IT department made situation more worse.IT security team was not fully equipped and trained to stop these kinds of attacks. users were not properly educated to save their personal information.

7.5 Preventations

- Back up data regularly -verifying data integrity and testing the restoration process.
- Secure your offline backups- ensuring backups are not connected permanently to the computer and they are backing up on.
- 3.Audit firewalls, servers and intrusion preventation system (IPS)-configuration block access to malicious IP address and server message block (SMB) ports 139 and 445, and disabled SMBV1 and windows management. Instrumentation command line (WMIC) in servers and active directory (AD)
- 4 patch operating systems, software and firmware on devices-use a centralized patch management system.
- Scan all income and outgoing emils-detect threats and filter executable files from reaching end users using sandboxing
- enable stronge spam filter to prevent phishing emails -authenticate inbound email using technologies such as sender policy framework (SPF), domain message authentication Reporting and conformance (DMARC) and domain keys identified mail (DKIM) to print spoofing.

8. SOCIOLOGIST VIEW AND THEORIES IN CONTEXT OF CRIMEIN SOCIETY

A summary of the sociological theories of crime which seek to examine the relationship between crime and society, are listed

Anomie theories – Robert Merton’s theory of anomie is caused as a socially-fostered state of discontent and deregulation that generated crime and deviance as part of the routine functioning of a society which promised much to everyone but denied them equal access to its attainment. In a society where failure is interpreted as personal rather than social weakness, where failure tended to lead to guilt rather than political anger, the pressure to succeed may be so powerful that it impelled people thus disadvantaged to bypass legitimate careers and take illegitimate careers.

Control theory – To control those who seek to commit crime because it's "profitable, useful or enjoyable" and will certainly break the law if they have to. Travis Hirschi believes the question is not "why do they do it" but should be – "why don't we do it?"

Four chief elements were held to induce people to comply with rules:

- Attachment – a person's sensitivity to the opinions of others
- Commitment – investment of time, energy and reputation in conformity
- Involvement – engrossment in conventional activity
- Belief – mirrors a person's conviction that he or she should obey legal rules

9. QUESTIONNAIRE SURVEY ON CYBER CRIME ANALYSIS

On connecting theories of sociologist with society and crime in society, to become aware more about the causes behind crime and mentality of criminal in recent we have conducted a questionnaire survey to know the ground reality and cause and found this.

- **Questions responses**

In figure 1 we show the age collection of respondents. The age of the respondents, 31% of the respondents belong to the age group of 16-20years, 36% of the respondents belong to the age group of 20-24years, 25% of the respondents belong to the age group of 24-28 years and only8% belong to 28-35 years of age group.

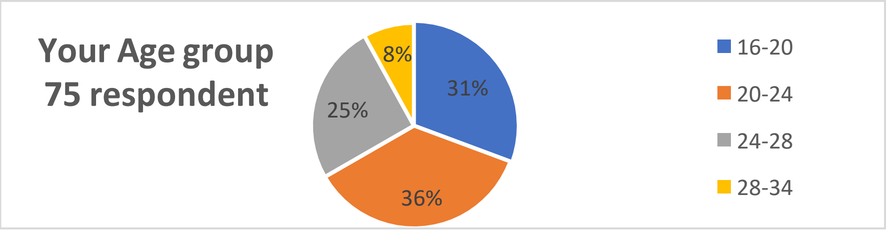

Figure 1: Age group of male & females

In figure 2 respondents were categorized according to gender. Respondents based on gender, 69% of the respondents were female and 31% of the respondents were male.

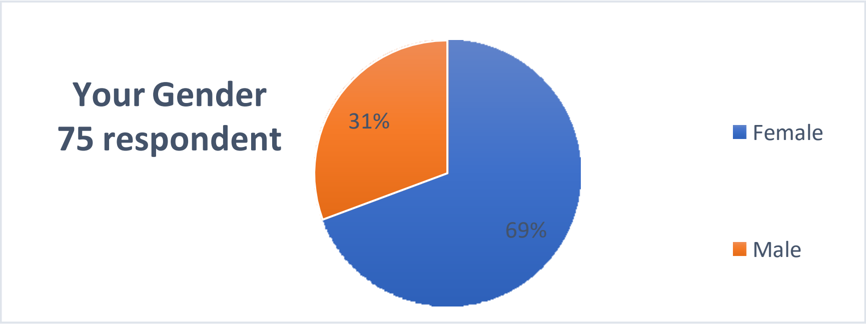

Figure 2: Response based on gender

- **Awareness about cyber crime**

In figure 3 respondents were asked they know about Cybercrime/Cyberterrorism, 100% of the respondents were know about Cybercrime/Cyber terrorism from such age group.

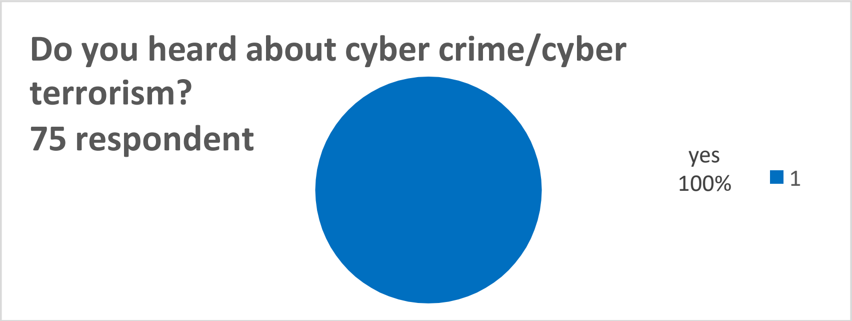

Figure 3: People awareness about cybercrime

- **Source of awareness about cyber crime**

In figure 4 respondents were asked about from where they heard about cyber-crime in multiple- choice question form in which 63% of the respondents knew about this from internet, 1% of the respondents were heard from the friends, 14% of the respondents were heard from their family members, 49% from newspaper, 3% from television, 10% from teacher and 1% from school and left are from other sources18.5% of the respondents heard from any other sources.

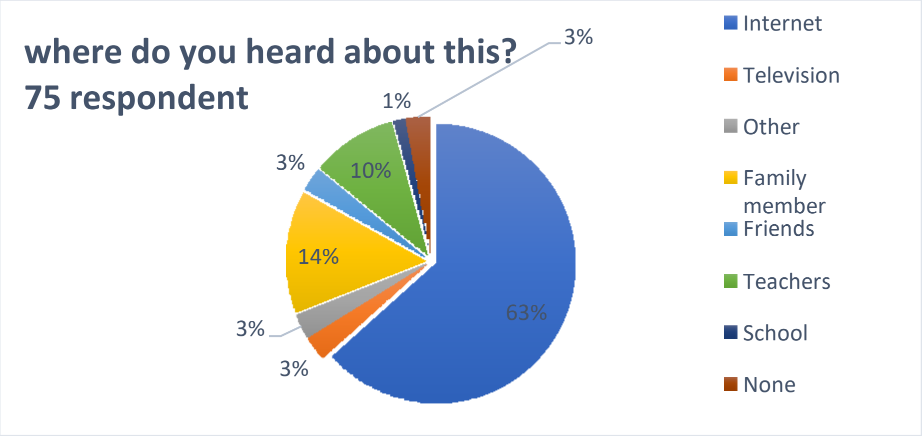

Figure 4: Source of awareness about cyber crimes

- **Cyberattack in near locality**

In the figure 5 respondents were asked about them about cyber-attack in their locality, respondents were heard about cyber-attack, 16.6% of the respondent where they may be heard about cyber-attack, while 6% of the respondents about don't about the cyber-attack.

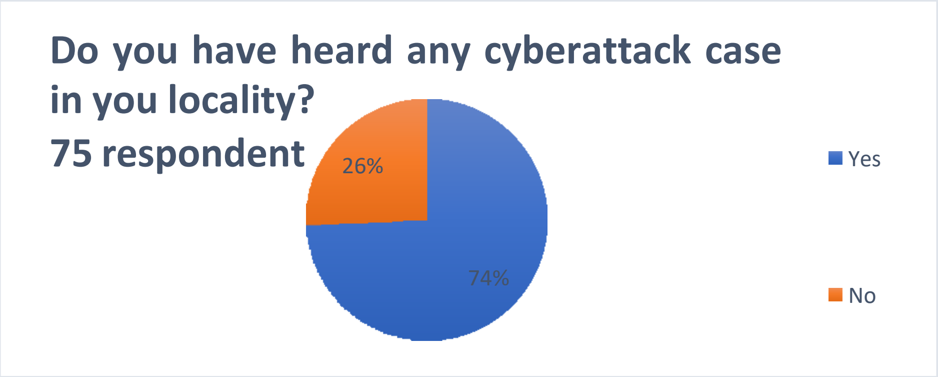

Figure 5: Awareness about cyberattack

- **Awareness about major cyber attacks**

In figure 6 respondents were asked about from where they heard about major cyber-attacks in multiple-choice question form in which 37% of the respondents know about yahoo! data breaches attack,12%% of the respondents know about Marriott Starwood data breach,24%% of the respondents know about Denial-of-Service attack, , 3% of the respondents know about South Korea Cyber Attack,24% of the respondents don't know about any of the above-listed cyber-attacks.

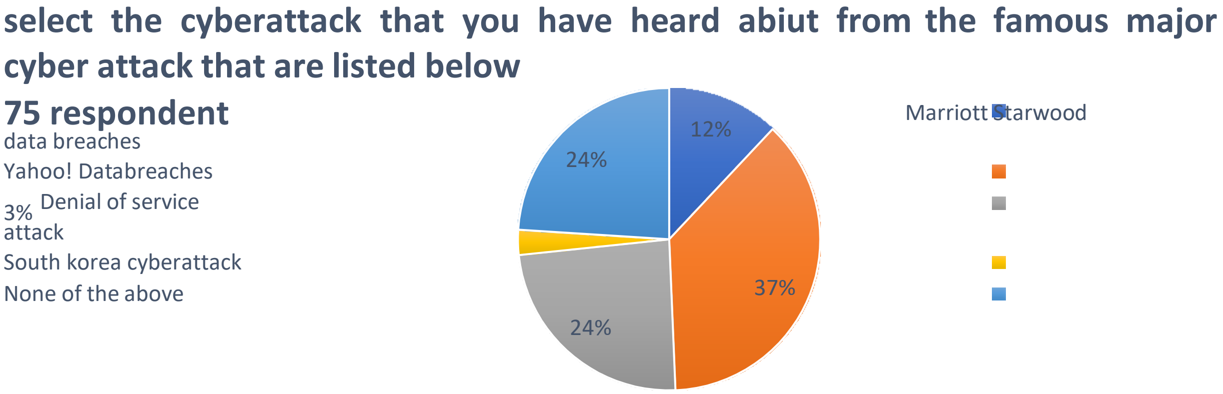

Figure 6: Awareness about major cyberattacks

- **Awareness about the prevention of cyber attack**

In the figure7 respondents were asked about from where they about in multiple-choice question form in which % of the respondents know about Firewall, 70.9% of the respondents know about Antivirus/Malware Software, 13.2% of the respondents know about Penetration Testing, 23.2% of the respondents know about IDS, 9.3% of the respondents don’t know about any of the listedsecurity software.

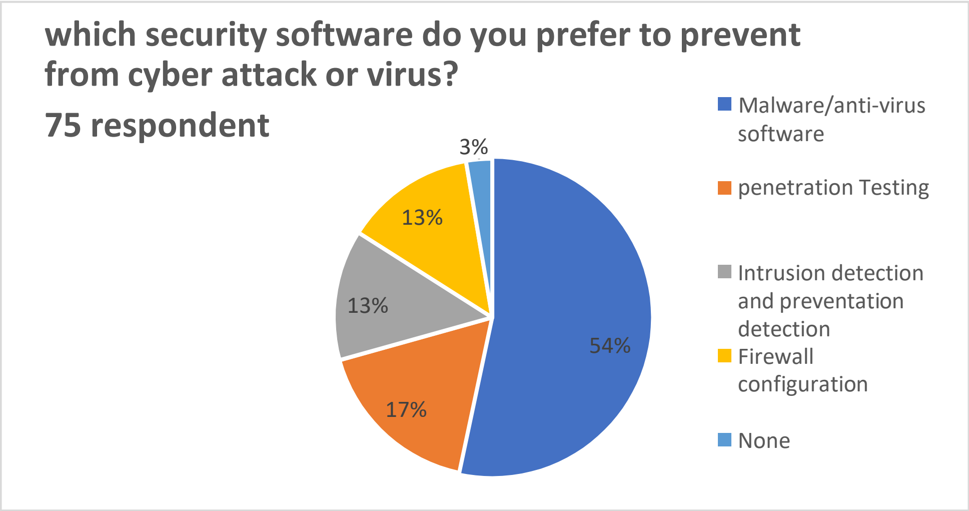

Figure 7: Awareness about the prevention of cyberattack.

In the Google form, we have asked to mention suggestions from the respondents to spread awareness towards cybercrime and what they expect from the government and security experts to stop cybercrime. From the respondent’s suggestions, we conclude their suggestions.

- **Analysis of survey**

There are so many different opinions about cybercrime crime terrorism and cyber security. Respondents compare cyber war with physical war. The rapid growth of internet users adds risks to cyberspace and it can to too dangerous to normal internet user respondents were asked about how can we prevent cybercrime; respondents gave different suggestions to prevent cybercrime. They suggested that an awareness campaign should be started to spread awareness among people. Knowledge of information technology should be mandatory for all people. India is the 2nd largest number of internet users. The government should make strict laws and regulations for crimes and start awareness programs in rural as well as urban areas because in rural areas people are most affected by spam calls and messages. Youths and aged people are easy targets for attackers. Organizations and experts make powerful tools and software to secure systems and information. A data breach is the main concern of the respondents due to the recent activities performed in the country. There should be an eye on suspicious activities on the internet and take action as soon as possible. Respondents take the major concern to suggestions on women safety, child pornography, and anti-national activities performed over the internet which damages our society, government and non-government org.

10. EFFECTS OF CYBERCRIME

- When talking about how computer crime affects our world, billions of dollars are lost every year as a result of computer crimes. Every day, there is an increase in computer crime, which results in significant stock losses for both companies and individuals. At the individual level, computer crimes may cost as little as 15 dollars, while at the corporate level, they cost as much as 225 billion dollars. Therefore, the amount of money lost as a result of computer crimes might range from 15 to 225 billion dollars.

- With around 35% of all cyberattacks worldwide, the United States leads, followed by South Korea with about 12%. Hackers and online criminals live or thrive in nations with lax regulations against computer crimes. They can simply launch attacks on wealthy nations from these nations. Protection firms now provide insurance against computer crimes as a result of the global rise in computer crimes. Following an assault, a company's stock price drops by 1% to 5%. As a result, firms incur losses on an individual level, but stockholdersalso pay a price due to the decline in stock price.

- When a hacker takes the firm's future plans and private information, the company suffers damages as a result of computer crime. The hacker just sells the data to a rival business, which then uses it to its advantage.

- Another issue is time wastage since many IT professionals must spend a lot of time managing detrimental situations that may be created by computer crimes and much time will be required to recover from the loss, rather than using that time for growth.

- When a hacker infiltrates a firm and obtains sensitive data, the people who entrust the company lose faith in it as a result of the disclosure of sensitive data, such as consumer credit cards, and they switch to someone else who can secure their sensitive data.

- Because businesses take precautions against cybercrime, there will be more password input and other behaviours, which lowers productivity.

- Costs associated with computer crimes will rise as businesses invest in robust security software to lower their vulnerability to malware and virus assaults. Sometimes the victim of a cyberattack may not even be aware that he has been assaulted, and the perpetrators areso cunning that they leave no trace at all.

- When you pay with a credit card at a shop, the transactions are encrypted and forwarded to the internet, which is accessible worldwide. Hackers can quickly decode the data because they are clever.

- There are a few safety precautions and solutions, including firewalls, cryptography, anti- virus and anti-spyware software.

- To curb cybercrimes, cybernetics and legislation have been developed. To protect consumers from cyberattacks, internet service providers must make the necessary measures to provide secure internet connections.

- We may draw the conclusion that cybercrime should be strictly prohibited by law and that computer crime is a major criminal offence that requires harsh punishment.

11. CYBERCRIME SUMMARY & DISCUSSION

When undertaking unlawful activities, cybercriminals often use a certain technique. Based on their experience trying to hack into a computer and then breaking into computer systems, this method was developed. This offers law enforcement with a Modus Operandi (MO) with patterns (Under the Information Technology Act of 2000) that they may employ to establish a case. In their respective sectors, law enforcement officers should create databases detailing the cybercriminals' methods. Typically, cybercriminals will use a computer network that is difficult or impossible to detect. This is done to make it challenging for law enforcement agents to identify the cybercriminal. Cybercriminals will "hack" into a victim's computer or utilise cyber cafés to carry out their criminal activities. At 29.1% (up from 8.1% in Q2 2021), Webmail and SaaS users are the most frequent targets of phishing assaults. 17.8% of the population today belongs to the second-largest demographic, financial institutions. (Q3 2021 Phishing Activity Trends Report by the APWG) Hissing is the second most common sort of threat action after a hack, behind denial-of-service. (The Verizon Data Breach Investigation Report for 2021) In the last quarter of 2019, 74% of phishing sites used HTTPS, compared to only 32% two years before. (ENISA Threat Landscape: Phishing for 2020) In 2019, over 43 percent of infected attachments were Microsoft Office documents. (ENISA Threat Landscape: Phishing for 2020) More than 95% of emails that distribute malware need a human response, such as clicking on a link or accepting a security alert. (ENISA Threat Landscape: Phishing for 2020)

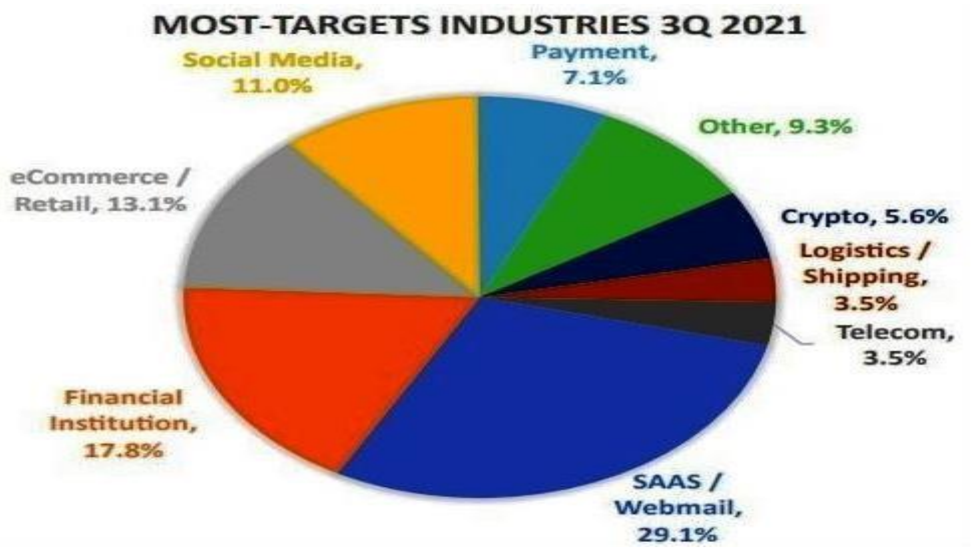

Fig 1: APWG's Phishing Activity Trends Report for Q3 2021(**Source: - ANDRA ZAHARIA** @Andrazaharia **UPDATED:** December 12, 2022)

- **Incidences of cybercrime were reported in India**

Computer-related crimes are often perpetrated, and only our reliance on technology allows us to identify them. Forgeries of computer source code, computer system hacking, obscene publications and transfer in electronic formats, and other crimes involving computers have led to the arrest of criminals. The table below provides specific information regarding the types of cybercrimes perpetrated in India, the charges that have been filed, and the number of people who have been detained in accordance with the I.T. Act between 2016 to 2020.

crime	persons reported					persons arrested				
Years	2016	2017	2018	2019	2020	2016	2017	2018	2019	2020
Tampering Computer source documents	78	233	257	173	338	30	54	122	42	76
Hacking with Computer system 1. Loss/ damage to Computer resource utility	6818	10108	14141	23612	21926	1203	6048	2730	3702	6435
2. Hacking	86	307	106	285	98	11	36	36		137
Obscene publication/ trans mission in electronic form	6	948	1334	1845	3008	0	372	440	742	1095
Failure 1. Of compliance/ order s of certifying authority	_	_	_	_	_	_	_	_	_	_
2. To assist in decrypting the information intercepted the Govt. Agency	_	4	6	9	7	_	1	38	8	3
Unauthorized access/ attempt access to protected computer system	_	2	0	2	2	_	1	0	2	0
Obtaining licence or Digital Signature certificate by mispresentaions/ suppression of fact	_	1	2	5	9	_	1	1	5	2
Publishing fake Digital Signature Certificate	_	170	78	87	149		31	49	35	43
Fraud Digital Signature Certificate	56	3466	3953	6233	10396	12	614	844	1120	1688
Breach of Confidentiality	35	247	389	812	742	4	105	122	219	603
Others	713	1503	980	2720	1017	109	379	390	491	320
Total	8613	13635	18495	30729	29643	1438	3169	4414	5852	9194

Table 1: Cybercrime/Cases Registered and Person Arrested Under IT Act during 2016 – 2020 (Source: ncrb.nic.in)

Note- The table data shows increase in cybercrime cases in every field from past few years where number of people get reported and people get arrested still maintain large gaps.

12. CONCLUSIONS

Nobody could argument the many ways in which the Internet has altered our culture, society, and way of life over the last 20 years. In fact, the whole phenomena are still so young that we have not yet figured out precisely how it affects us and how it will continue to affect us in the future. We are unsure of what new technological developments, creative forms, social classes, or subcultures the internet will give rise to. Additionally, we are unable to foresee every hazard that it poses. Additionally, cybercrime is still very new. As soon as the internet existed, thieves started using cutting-edge technologies to exploit it. To defend ourselves, we must make every effort to stay one step ahead of cybercrime. We cannot afford to lag behind too much, at the very least.

13. REFERENCES

1. Yarovenko, H., & Rymar, V. (2023). DEVELOPMENT OF MODERN CYBERCRIME PROFILES. Grail of Science, 23, 267–268. https://doi.org/10.36074/grail-of-science.23.12.2022.40

2. Choi, S., & Parti, K. (2022). Understanding the Challenges of Cryptography-Related Cybercrime and Its Investigation. CrimRxiv. Published. https://doi.org/10.21428/cb6ab371.10db84c3

3. Mohsin, K. (2021). The Internet and its Opportunities for Cybercrime – Interpersonal Cybercrime. SSRN Electronic Journal. Published. https://doi.org/10.2139/ssrn.3815973

4. Kovtun, K. A. (2021). Banking Cybercrime as One of the Main Problems of Modern Society. Theoretical and Applied Law, 1(7), 94–97. https://doi.org/10.22394/2686-7834-2021-1-94-97

5. Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2021). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. Policing and Society, 32(1), 103–124. https://doi.org/10.1080/10439463.2021.1883608

6. Meena Y, Sankhla MS, Mohril S, et al. Cybercrime: youth awareness survey in Delhi NCR, India. Forensic Res Criminol Int J. 2020;8(5):177-180. DOI: 10.15406/frcij.2020.08.00325

7. Agarwal, V., & Verma, C. (2018). An Analysis of Indian Spirituality in Modern Society: A Short Review. Journal of Advances and Scholarly Researches in Allied Education, 15(4), 175–179. https://doi.org/10.29070/15/57401

8. NWOYE, C. J. (2015). Cybercrime Prevention in Online Transaction Using Biometric Access Control. International Journal of Information Security and Cybercrime, 4(2), 61–72. https://doi.org/10.19107/ijisc.2015.02.06

9. PARODI, F. (2013). The Concept of Cybercrime and Online Threats Analysis. International Journal of Information Security and Cybercrime, 2(1), 59–66. https://doi.org/10.19107/ijisc.2013.01.07

10. Koops, B.-J. (2010). The Internet and its Opportunities for Cybercrime. SSRN Electronic Journal. Published. https://doi.org/10.2139/ssrn.1738223

11. Wall, D. S. (2008). CYBERCRIME AND THE CULTURE OF FEAR. Information, Communication & Society, 11(6), 861–884. https://doi.org/10.1080/13691180802007788