The International Journal of Indian Psychology
ISSN 2348-5396 (Online) | ISSN: 2349-3429 (Print)
Volume 11, Issue 3, July- September, 2023
DIP: 18.01.026.20231103, DOI: 10.25215/1103.026
https://www.ijip.in

Research Paper

A Study on People's Opinion on Awareness about Cybercrime in India

Dr. Jamuna KV[1], Ms. Janvi Jaiswal[2]*, Ms. Sanjana Santosh[3], Ms. Sneha Baiju[4]

ABSTRACT

Today, cybersecurity is as important as economic security". Like many other crimes, cybercrime is on the increase these days. Using computers and the Internet to steal a person's identity or to import illegal or malicious programs. Cybercrime is very harmful for everyone., because it directly includes stealing their personal data, which damages their respect in the society, cybercrime has a huge-negative impact on our society, our economy and our business, because for our society, cybercrime can play a role in bullying, identity theft, cyber-stalking and cyber-defamation, resulting in a very uncomfortable position for victims of these attacks. Cybercrime affects the economy and business, and recent years have seen many cases of data theft another cyberattacks against some large companies. Companies spend millions of dollars each year to protect their systems from any form of cyber theft, misuse of their files. Not only does cybercrime affect any individual financially, but it also affects them spiritually like women who irritate their modesty by sharing photos of themselves on the internet, but it also hampers the spiritual growth of anyone teenager today, because many teenagers are in This cyber traits & over. And end their lives with suicide and depression. To protect everyone from cybercrime, there are many laws related to cybercrime prevention like: 1. Information and Technology Act 2000 & 2. Indian Penal Code 1860.

Keywords: *Cybercrime, India, People's Opinion, Awareness.*

Cybercrime, or computer crime, is a crime involving computers and networks. The computer may have been used to commit or be the target of a crime. Cybercrime is the use of computers as a weapon to commit crimes such as fraud, identity theft or invasion of privacy. Cybercrime, especially on the Internet, has become increasingly important as computers have become central to everything from business to entertainment to government. Cybercrime can endanger the security and financial health of individuals or nations.

Cybercrime covers a wide range of activities, but generally falls into two categories:

[1]Programme Head BSc Forensic Science & Assistant Professor, Department of Forensic Science Jain (Deemed-to- be-university) Bangalore, Karnataka, India.
[2]Student, Department of Forensic Science Jain (Deemed-to-be-university) Bangalore, Karnataka, India
[3]Student, Department of Forensic Science Jain (Deemed-to-be-university) Bangalore, Karnataka, India
[4]Student, Department of Forensic Science Jain (Deemed-to-be-university) Bangalore, Karnataka, India
*Corresponding Author

Received: May 20, 2023; Revision Received: July 09, 2023; Accepted: July 12, 2023

1. A crime against a computer network or device. These types of crimes involve different threats (such as viruses, vulnerabilities, etc.) and denial of service (DoS) attacks.
2. Offenses using computer networks to commit other criminal activities. These types of crimes include cyberstalking, financial fraud or identity theft.

Cybercrime Challenges

1. **People don't know their rights online -** Cybercrime usually affects illiterate people around the world who don't understand the cyber rights enforced by the government of that particular country.
2. **Anonymity-** Those who commit cybercrimes are anonymous to us, so we cannot do anything against that person.
3. **Less Recorded Cases-** Every country in the world is facing the challenge of cybercrime and the cybercrime rate is increasing day by day because even people who have not recorded cybercrime cases are a big challenge for us as well than for the authorities.
4. **Mainly perpetrated by educated people -** Cybercrime is not everyone's cup of tea. A person who commits a cybercrime is very technical, so they know how to commit the crime without getting caught by the authorities.

REVIEW OF LITERATURE:

Cezar V. (2012) "Cyber-attacks to understand "
This paper explores the concept of cyber-attack as a concept for understanding contemporary conflict. Elaborating a conceptual theoretical framework, the authors state that there is no internationally accepted definition of the subject for cyberattack, cyberwarfare, and cyberdefense. The authors develop a process for clearly distinguishing between events (cyber-attack, cyber-warfare, and cyber-crime or cyber-terrorism) and maintain a process for conducting legitimate military/civilian cyber response operations for the country. This suggests that special attention should be paid to it.

Debarati H and K Jaishankar (2010) "Cyber Victimization in India"
The authors of this article describe the growth of India's IT sector from the 1990s to the present, with almost all households living in middle-to-higher economies. I live in an income group. , have internet access, and people in the age group 13-70 access the internet regularly, but at the same time they are being harmed. There are some monopoly laws on cyberspace, but they do little to curb the ever-increasing amount of personal harm in Indian cyberspace.

M. Herzog-Evans (2010) "Internet and Cybercrime"
The Internet and its Opportunities for Cybercrime the Internet deserves special attention in criminology as well as in criminal law and politics because it is global, instantaneous, cross-border in nature, digital and capable of automating the processing of information. Because of these characteristics, the Internet offers special opportunities for the commission of cybercrime: crimes that target computer networks or use hardware tools. This chapter offers a brief review of the literature examining how and why the Internet offers exceptional opportunities for crime, and what this means for the management of (cyber)crime. It describes some types of cybercrime and lists twelve Internet risk factors that, taken together, provide a unique pattern of opportunity for crime. The chapter then discusses what is misunderstood about cybercriminals, organized cybercrime and cybervictims, and briefly discusses the challenges and limitations of law enforcement and other countermeasures. Although there is little empirical research on cybercrime, the theoretical ideas and hypotheses

presented in the literature support the conclusion that the Internet modifies crime. Cybercrime is seen as organized, large-scale and diverse, with an increasing division of labour, and is expected to be increasingly intertwined with offline organized crime. Also, for some crimes, there appears to be considerable overlap between offline and online victimization. Now that Internet use has become a daily activity in everyday life, criminology, as well as law and criminal policy, should integrate Internet and cybercrime into their own daily activities, while paying attention to specificities and complexities of this unique phenomenon that is the Internet.

Bradford W. Reyns (2017) "Routine Activity Theory and Cybercrime"
This chapter discusses some new challenges that arise when applying theory to cybercrime, potential solutions to these challenges, and an overview of the current state of the domain. Routine activity theory is part of the opportunity view of criminology, which views criminal opportunities as the ultimate cause of criminal events. Its central premise explains that crime occurs when circumstances conducive to crime lead to opportunities for crime. According to routine activity theory, a motivated offender responds to opportunity when confronted with a suitable target that lacks effective guard. In terms of routine activity theory, cybercrime relies on computer networks to connect motivated perpetrators to potential victims in the absence of effective custody. Cyber-lifestyle routine theory suggests that the temporal separation of motivated perpetrators and appropriate targets can be reconciled by viewing their interactions as "delayed" times.

Zarina Shukur, Rozilawati Razali "Commentary on Cybercrime Affecting Portable Devices"
The popularity of mobile devices in the market is impressive, but the influx of different products makes it difficult for users to protect their infrastructure from possible data breaches. As the number of exposures and attacks increased, so did the security solutions provide by researchers. This article reviews the literature on preventing cybercrime from affecting portable devices, particularly smartphones with the Android operating system. Existing research was analysed and opportunities for future research were identified. Four research questions were asked and 33 of the 493 articles found were selected for analysis. Through our analysis, we found that data breaches due to lost or stolen devices, accidental data disclosures, and phishing attacks were the most common among attackers. Security researchers have certainly emphasized the importance of protecting confidential personal data residing in Android portable devices. They propose to use a permission-based security model and behaviour-based detection methods to protect confidential information. As a result, we found that the Android operating system can manage and enforce a built-in protection model, but we still have opportunities to improve personal data security.

METHODOLOGY

The Research Design is Qualitative Research, Sample was the Population Aged between 18 and 50 irrespective of their gender & ethnicity.

The objectives of the study were to study the level of awareness amongst people, and to study the measures taken by people to prevent cybercrime.

The sample size consists of 125 general public opinion both males and females and the Sampling Method was Purposive Sampling Technique for this research.

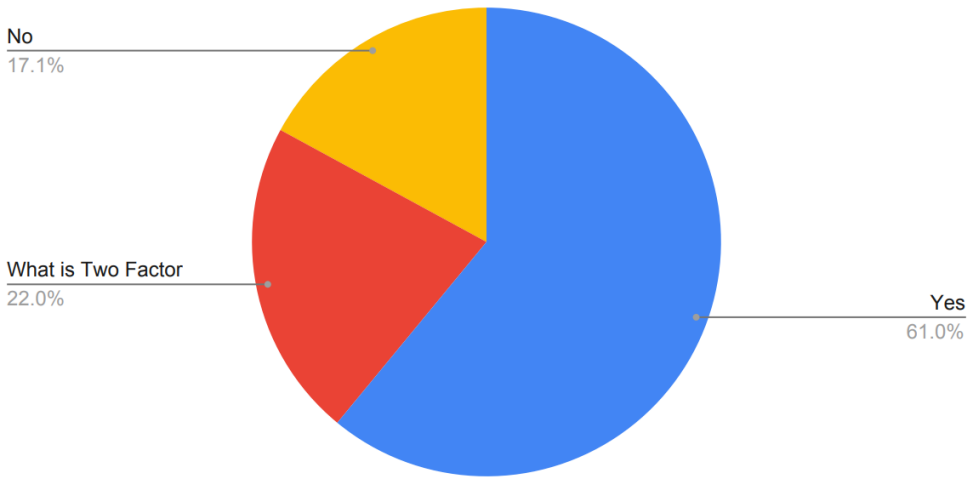
The data was collected from people all across India with the help of the Tools that is A Questionnaire of 15 questions that was developed with the help of an expert was used.

The data was concluded as Descriptive Statistics-percentage analysis.

DATA ANALYSIS & DISCUSSION

The survey aimed to understand the level of awareness and preparedness among respondents regarding cyber threats and whether they have experienced any cyber-related incidents in the past. The survey questions cover various aspects such as online safety, the government's efforts in preventing cybercrime, the use of antivirus and two-factor authentication, experiences with cyberbullying and cybercrime incidents, and more. The responses collected from the survey can help in identifying areas of improvement and developing effective strategies to combat cybercrime.

Figure 1: showing people's awareness on two Factor Authentication for online accounts.

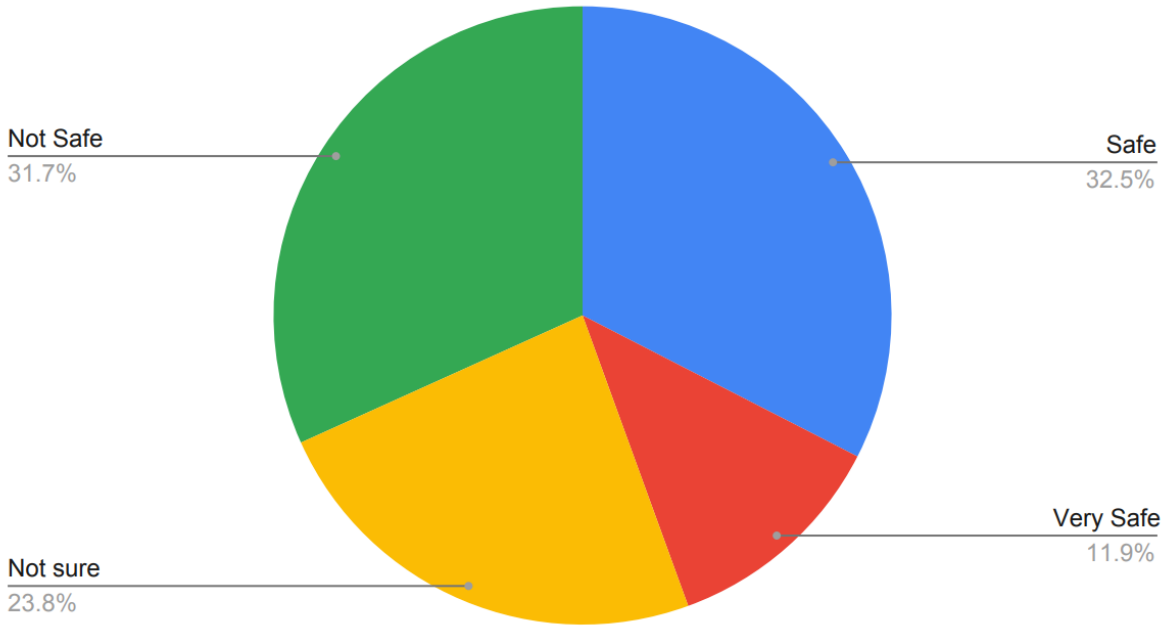


According to the survey, the majority of respondents have enabled Two-factor authentication (2FA) for their online accounts. Out of all the respondents, 61.0% have opted for this added layer of security to protect their sensitive data from potential cyber-attacks. This is a positive trend as 2FA provides an additional layer of security and makes it more difficult for hackers to gain unauthorized access to accounts.

However, it is concerning to note that 17% of the respondents have not enabled 2FA for their online accounts. This suggests that there are still some people who are not taking adequate steps to protect their online accounts, which could lead to potential security breaches.

Furthermore, it is alarming to see that 22.0% of the respondents were not familiar with what 2FA is. This indicates a need for further education and awareness on this topic. It is essential for people to understand the importance of 2FA and how it works to secure their online accounts, while it is encouraging to see that a majority of respondents have enabled 2FA, it is essential to continue educating people about the benefits of this security measure to ensure the safety of their online accounts.

Figure 2: Showing peoples opinion on their information safety online.



As per the survey, a considerable percentage of respondents are not confident about the safety of their online information. Approximately 31.7% of the respondents do not feel safe about the security of their online data, which could be a result of previous data breaches and cyber-attacks. This is a worrying trend as online data is becoming increasingly crucial, and a lack of confidence in its security could lead to people avoiding online activities altogether.

Additionally, 23.8% of the respondents were not sure about their level of safety, indicating a lack of knowledge or awareness about online security. This lack of awareness highlights the need for further education and awareness programs to educate people about online security measures and the importance of protecting their personal information online.

However, the survey also revealed that a significant proportion of respondents reported feeling safe or very safe about the security of their online information. 32.5% of respondents reported feeling safe, while 11.5% reported feeling very safe. This suggests that not many people are confident in their ability to protect their online data and maintain their privacy, possibly due to implementing online security measures such as using strong passwords and enabling two-factor authentication.

The survey results indicate that while some people lack confidence in the security of their online information, there is also a significant proportion of people who are aware of the risks and taking measures to protect their online data. However, there is still a need for continued education and awareness programs to improve people's understanding of online security and the importance of protecting their personal information online.

Major Findings of the Study:

- According to a recent survey, when asked about their level of safety regarding their personal information while online, 28.6% of respondents reported feeling "not safe," while 19% reported feeling "not sure." In contrast, 33.3% of respondents reported feeling "safe," and 19.0% reported feeling "very safe." These results suggest that a significant portion of the population has concerns about the safety of their personal information while online.

- when asked whether they have antivirus software installed on their PC/Mac, 38.1% of respondents reported not having antivirus software installed, while 61.9% reported having antivirus software installed. These results suggest that the majority of the population surveyed have taken steps to protect their devices from potential cyber threats by installing antivirus software.
- when asked about whether they have been a victim of email or SMS bombing/spamming, 52.4% of respondents reported not having been a victim, while 47.6% reported having been a victim. These results suggest that nearly half of the population surveyed has experienced email or SMS bombing/spamming, highlighting the prevalence of this form of cyber threat.
- when asked about the relationship between the responsible use of data/information on their devices and the prevention of cybercrime, 11.9% of respondents reported disagreeing with the statement, while 88.1% reported agreeing with the statement. These results suggest that the overwhelming majority of the population surveyed believe that responsible use of their personal data and information can help prevent cybercrime.
- According to the results, approximately 28.6% of the respondents do not feel safe about their online information. This could be due to a variety of factors, such as concerns about hacking, data breaches, or identity theft. Additionally, 19% of the respondents were not sure about their level of safety, which may indicate a lack of knowledge or awareness about online security. On the other hand, 33.3% of the respondents reported feeling safe about their online information, while 19% reported feeling very safe. This suggests that a significant proportion of respondents are confident in their ability to protect their online data and maintain their privacy.
- when asked whether they were aware that victims of fraud and cybercrime should report it to the national Cyber Crime Reporting Portal, 28.6% of respondents reported that they were aware and had used/would use the service, 19% reported that they were aware but would not use the service, and the majority of respondents (52.4%) reported that they were not aware of such a reporting portal. These results suggest that while there is some level of awareness of the existence of the national Cyber Crime Reporting Portal, many respondents are still unaware of this resource for reporting cybercrime.
- when asked whether respondents believed that antivirus software can protect their systems from cyber-attacks, 21.4% of respondents answered in the affirmative, 23.8% answered in the negative, and the majority of respondents (54.8%) reported that antivirus software can sometimes protect their systems from cyber-attacks. These results suggest that while many respondents believe that antivirus software can provide some level of protection against cyber-attacks, a significant portion of respondents are not convinced that it is a reliable means of defence against such attacks.
- when asked whether respondents have ever lost money due to cybercrime, 9.5% of respondents were unsure or could not say, 2.4% reported being overcharged, 9.5% reported that money was deducted from their account without authorization, 11.9% reported being a victim of fraud involving merchandise, and the majority of respondents (66.7%) reported that they have never lost money due to cybercrime. These results suggest that while some respondents have been victims of cybercrime and lost money, the majority of respondents have not experienced any financial losses due to cybercrime.

- when asked whether respondents have ever received a call from someone asking for bank, account, or other sensitive details, the majority of respondents (42.9%) reported that they have not received such calls, 23.8% of respondents reported receiving such calls multiple times, and 33.3% of respondents reported receiving such calls at least once. These results suggest that a significant number of respondents have received unsolicited calls from individuals attempting to obtain their sensitive personal or financial information, indicating the need for increased awareness and caution when sharing such information over the phone.
- when asked whether cyberbullying or harassment is a major cybercrime, 4.8% of respondents disagreed, 35.7% of respondents agreed, and a significant majority of 59.5% of respondents strongly believed that cyberbullying or harassment is a major cybercrime. These results suggest that there is a widespread recognition of the seriousness of cyberbullying or harassment as a form of cybercrime, which highlights the need for continued efforts to prevent and address this issue.
- When asked whether anyone ever experienced as a situations Out of the responses provided, 16.6% of the respondents have experienced Trojan or malware, 19.1% have received auto-generated mails to their inbox, 7.2% have had obscure material published on their profiles, and 4.8% have had confidential reports or information hacked. The majority, at 52.4%, have not experienced any such situation.

CONCLUSION

Cybercrime prevention: Here are some key points we can use to prevent cybercrime:

1. **Use strong passwords –**Keep a different username and password combination for each account and resist the temptation to write them down. Weak passwords can be easily cracked by brute force, rainbow table attack and other attack methods. So, make it complicated. It represents a combination of letters, numbers and special characters.
2. **Use reliable antivirus software on your devices –**Always use reliable and highly advanced antivirus software on mobile and personal computers. This results in protection against various virus attacks on the device.
3. **Keep social media private -** always keeps your social media account data private and only available to your friends. Also, be sure to only make friends you know well.
4. **Keep your device software up to date –** Whenever you get system software updates, update them as well, as older versions are sometimes vulnerable.
5. **Using secure networks –** Public Wi-Fi is vulnerable. Avoid financial or business transactions on these networks.
6. **Never open attachments in spam emails -** computers are infected with malware attacks another form of cybercrime via attachments in spam emails. Never open an attachment from a sender you don't know.

REFERENCES

Cybercrime (no date) *INTERPOL*. Available at: https://www.interpol.int/en/Crimes/Cybercrime (Accessed: April 19, 2023).

Kaspersky (2023) *What is cybercrime? how to protect yourself from Cybercrime, www.kaspersky.co.in*. Available at: https://www.kaspersky.co.in/resource-center/threats/what-is-cybercrime (Accessed: April 19, 2023).

Literature review on cybercrime (no date) *Bartleby*. Available at: https://www.bartleby.com/essay/Literature-Review-On-Cyber-Crime-PJP6L3WT26 (Accessed: April 19, 2023)

Literature review on cybercrime (no date) *Bartleby*. Available at: https://www.bartleby.com/essay/Literature-Review-On-Cyber-Crime-PJP6L3WT26 (Accessed: April 19, 2023)

Literature review on cybercrimes and its prevention mechanisms (no date). Available at: https://www.researchgate.net/publication/331010726_Literature_review_on_Cyber_Crimes_and_its_Prevention_Mechanisms (Accessed: April 19, 2023).

Acknowledgement

The author(s) appreciates all those who participated in the study and helped to facilitate the research process.

Conflict of Interest

The author(s) declared no conflict of interest.

How to cite this article: Jamuna, KV, Jaiswal, J., Santosh, S. & Baiju, S. (2023). A Study on People's Opinion on Awareness about Cybercrime in India. *International Journal of Indian Psychology*, *11(3),* 287-294. DIP:18.01.026.20231103, DOI:10.25215/1103.026