Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 11, Nov- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Cybercrime Awareness among the Belagavi City Citizens and their Attitudes towards Filing Complaint to Police

*Suleman Choudhri

**Prof. R N Mangoli

Abstract

Cyberspace represents the national environment in which communication occurs over computer networks. A virtual realm that has fostered human activities, from education to commerce and currency exchange. Yet, this dependence has given rise to certain negative consequences, because many users lack awareness of the dangers and best practices for the use of the internet. As a result, this has created an opportunity for cyber criminals to exploit innocent individuals, resulting in global victimization.

This particular study focuses on the issue of cyber victimization in Belagavi City. The study sample includes 200 participants who were selected through non-probability convenient and snowball sampling methods, via a survey questionnaire. The study adopts a quantitative approach, utilizing survey research methods.The findings of this study will be invaluable in informing future efforts aimed at mitigating the impact of cyber victimization in Belagavi and beyond.

Key Words: Familiarity, Cyberspace, cybercrime, victimization, Attitude

*Research Scholar, Department Research Scholar, Department of Criminology and Criminal Justice, Rani Channamma University, Belagavi Karnataka, India., Email: sulemanchoudhary1@gmail.com

**Professor and Research Guide, Department of Criminology and Criminal Justice, Rani Channamma University, Belagavi Karnataka, India. Email ID: drmangoli.rn@gmail.com

Introduction

The term "cyber" is typically associated with electronic communication networks and virtual reality. These concepts involve the use of electronic devices, such as computers and mobile phones, as well as the internet. Electronic communication refers to the transmission of information through electronic gadgets, with the information typically being encrypted and decrypted digitally. Popular examples of electronic communication include email, Facebook, and websites. These tools allow for the transmission of information in the virtual world or reality created on computer networks. It is important to note that each individual, group, or society has their own domain to explore the virtual world. To facilitate this computer-generated experience, the internet or network is essential. The internet is a computer network that provides communication and information services using standard communication protocols. This allows for easy and accessible communication to occur across the world. The internet has revolutionized the way we communicate and interact with one another, and it has become an integral part of our lives.

As our reliance on cyberspace continues to grow, it's become increasingly apparent that this dependence can sometimes lead to deviant behavior. Deviance, in this context, refers to actions that go against the cultural norms that are recognized and accepted by the majority. One of the most severe forms of deviance is committing a crime, which involves violating the laws that society has formally created. However, not all deviant behaviors are equally severe. For instance, failing to show respect for elders is considered a deviant behavior, but it's not generally punished. Every society has its own set of norms, and deviant behavior can vary depending on the society. Modern societies are often pluralistic, made up of people from different backgrounds with varying values and beliefs. This diversity can create conflicting norms and values, which can contribute to deviant behavior.

In recent years, it has become apparent that every society possesses unique characteristics. The society on the internet has caused people to rethink the structure of society, as individuals from across the globe are connecting with one another without any geographical boundaries. However, cybercrime has become increasingly prevalent, which is defined as crime committed on the internet. As the incidence of cybercrime continues to rise, a study was conducted to determine whether victims of cybercrime were aware of the concept and whether they reported the crime to law enforcement agencies, if they had been victimized.

Methodology

The study is quantitative, as the primary data collected is in the form of numeric values directly obtained from the respondents. The self-administered questionnaire has been used as a tool for data collection. The sample used for the study was selected using a non-probability type convenient and snowball method of sampling, with a total sample size of 200. The collected data has been presented in tables, and the analysis has been performed accordingly.

Results and Discussion

Demographic information of respondents indicates that most of the respondents belong to the age category of 25- 40 years at 122 followed by 55 were 18-24 years and23 were 40 above and of age. Most of the respondents were male at 133 while 67 were females. 78 were graduates, 26 were postgraduates, 52 were cleared PUC or 12th class and 44 were cleared SSLC or 10th. Most of them were job holders at 94, 43businessmen followed byhomemaker at 27 and 36 unemployed.

Table No: 01

No	*ajor cybercrimes*	*amiliarity with terms*	
		es	o
	ocial Engineering	59	1
	alicious codes attack	14	5
	poofing attacks	1	29
	entity theft	06	4
	yber stalking	16	4
	yber abuse or Trolling	78	2
	hreatening or Hate message/call	50	0
	ob frauds	33	7
	vestment/ lottery fraud	02	3
	ocial media frauds	44	5

The table above shows information regarding whether citizens are aware of the terms and commission of major forms of cybercrimes. In many cases, people are not aware of the laws or lack legal knowledge in our country. This makes it essential to understand the level of awareness citizens have regarding cybercrimes, as they are becoming more common than traditional methods of committing crimes. The research conducted in the city of Belagavi in Karnataka state aimed to determine the level of awareness among citizens of cybercrimes. However, it is important to note that the findings may differ if the research is conducted in rural areas, as the focus of this research was on the urban population. During the data collection process, specific terms related to cybercrimes were explained to respondents, since they were not familiar with them. The responses were then collected based on this explanation.

When the question was asked pertaining to their awareness or familiarity with terms used for cybercrimes, data indicates that 169 citizens out of 200 were familiar with the social engineering these crimes are most familiar to everyone as almost every individual have received such calls, followed with 114with malicious codes,71 individuals were having knowledge pertaining to spoofing attacks, 106 knew about the identity theft, 116 about cyber stalking, Cyber abuse and trolling by 178, threatening or hate messages call by 150, job frauds by 183,investment fraud and lottery frauds by 102, and social media frauds by 144 respondents.

If we consider the responses in current research in Belagavi city, highlights that citizens are most familiar with social engineering, cyber abuse or trolling, and job frauds as types of cybercrime. These crimes are prevalent due to the increasing use of social media platforms and online job portals. However, it is concerning to note that citizens are least aware of spoofing attacks, which are becoming more sophisticated and difficult to detect. Investment fraud and identity theft are known by approximately half of the respondents, which indicates that they have some knowledge of cybercrime trends. Nevertheless, it is important to note that many citizens still lack awareness of the various types of cybercrime, which could lead to severe consequences. As cyberspace is continuously evolving and criminals are using advanced techniques to commit crimes, it is crucial for citizens to stay informed about the latest trends in cybercrime. This can be achieved through awareness campaigns, workshops, and training programs, which can help citizens protect themselves and their digital assets.

Table No:02

Sl No	*ajor cybercrimes*	*ave been victimized ever*	
		es	o
1	ocial Engineering	19	1
2	alicious codes attack	03	7
3	poofing attacks	6	24
4	entity theft	9	11
5	yber stalking	38	2
6	yber abuse or Trolling	24	6
7	hreatening or Hate message/call	3	27
8	ob frauds	2	08
9	vestment/ lottery fraud	06	04
10	ocial media frauds	9	31

Above data consists details of the victimization of the respondents, as it was explained to the respondents the meanings of the terms used in the questions, further the details of their victimization have been collected in the particular query for which responses are as follows, out of 200 respondents 119 had been the victims of social engineering attacks (which consists Phissing, Vishing and Smishing) followed with 103 victims of malicious codes, 76 with spoofing attack, 89 with identity theft, 138 cyberstalking, 124 cyber abuse or trolling 73 threatening or hate messages 82 with job frauds, 106 with investment or lottery fraud and 69 with social media related frauds.

Upon scrutinizing the aforementioned data, it is quite evident that cyberstalking, cyber abuse, and trolling are the most commonly faced crimes by the respondents. The surge in social media activity among individuals has made these platforms one of the major mediums of communication. However, this has also led to instances where individuals form groups to troll or follow individuals without their knowledge, leading to a surge in cybercrimes. Moreover, the respondents have also been victims of social engineering, malicious attacks, and investment or lottery scams, which have a direct correlation with economic loss. According to a Hindustan Times article, India stands third in the world in terms of phishing attacks. This could be attributed to the fact that, in the earlier days of these attacks, there was less awareness among the citizens, and many fell prey to such attacks. However, people have become more aware of such attacks and are taking necessary precautions to avoid them.

Table No: 03

Sl No	*ajor cybercrimes*	*ave been reported*	
		es	o
1	ocial Engineering	5	4
2	alicious codes attack	7	6
3	poofing attacks	4	2
4	entity theft	6	3
5	yber stalking	1	7
6	yber abuse or Trolling	2	02
7	hreatening or Hate message/call	6	7
8	ob frauds	0	2
9	vestment/ lottery fraud	3	3
10	ocial media frauds	5	4

When enquired about the reporting of the cybercrime to the law enforcement agencies, the revelation was quite surprising as most of the victims were not reported their victimization. Out of 119 social engineering attack victims only 65 respondents have reported their victimization which is the highest number of reported offenses in the present research, if we look at every victimization in the research it is visible that most of the reported victimizations are related to economic losses that is 65 social engineering, 40 job frauds and 38 investment fraud, which indicates that respondents were more worried about their economic loss rather than any other, as it indicates in the above data where only 14 reported for spoofing attack followed 17 in malicious code attack, 15 in social media frauds, 22 cyber abuse or trolling, 26 identity theft, and 36 in threatening or hate messages. As technology continues to rapidly evolve, the number of cybercrimes is increasing at an alarming rate. Despite this, it is concerning that many individuals are not reporting such offenses. It is crucial that a safe and secure environment be established for everyone, and this can only be achieved if victims of cybercrime come forward and actively participate in the Criminal Justice System. By doing so, not only can they help bring the perpetrators to justice, but they can also help prevent further cybercrimes from occurring in the future.

The objective of the study was to explore the level of familiarity that respondents had with cybercrime, their experiences with victimization and their attitudes towards reporting such incidents. However, the research did not delve into the underlying reasons for the reluctance of individuals to report instances of cybercrime that they may have been victimized by. Identifying such reasons could provide valuable insights into how to encourage more people to report cybercrime and improve the effectiveness of prevention and response strategies.

Conclusion

The advent of technology has revolutionized the way we live our lives. With the proliferation of wireless networks and advancements in computer equipment, citizens have enthusiastically adopted technology to make their daily chores of life easier. However, with this advancement in technology, the threat of cybercrime victimization has also risen significantly. Unfortunately, most victims are not aware of the negative aspects of technology, making them vulnerable to cybercrime. Research indicates that many citizens lack basic knowledge about cybercrime, making them unaware of the potential dangers of using technology. Furthermore, most victims do not report their victimization to law enforcement agencies, which only exacerbates the problem.

After analyzing the data presented above, it becomes evident that individuals must be vigilant and cautious of their online activities, as cybercriminals are constantly lurking online to exploit any vulnerabilities. The consequences of cybercrime can be devastating, including identity theft, financial loss, and reputational damage. Therefore, every individual must prioritizetheir privacy and stay updated on the latest technological advances to safeguard themselves against such threats.

In addition to individual responsibility, law enforcement agencies and the government have a crucial role in combating cybercrime. They must enact new laws and policies that focus on protecting individuals from cybercrime victimization. This will ensure that the perpetrators of cybercrime are held accountable for their actions and that the victims receive the necessary support to recover from any damages caused by these crimes.Overall, every individual needs to take proactive measures to protect themselves from cybercrime, while also urging the government and law enforcement agencies to take necessary actions to ensure the safety of individuals online.

References

- Ahuja Ram (2005) Criminology, Rawat Publication ISBN 81-7633-609-0
- Appelbaum Richard & Chambliss William (1995) Sociology, Harper Collins College publisher New York
- Macionis John (2005) Sociology, Pearson Education Inc, Dorling Kindersley (India) pvt. Ltd ISBN 81-317-0385-1
- Rawat H K (2010) Sociology: Basic Concept, Rawat Publication ISBN 81-7033-0054-8
- https://www.vedantu.com/commerce/introduction-to-cyberspaceRetrieved on 15th April 2022
- https://www.techopedia.com/definition/2493/cyberspaceRetrieved on 15th April 2022
- https://www.britannica.com/topic/cyberspaceRetrieved on 15th April 2022
- https://www.jigsawacademy.com/blogs/cyber-security/cyber-space/Retrieved on 15th April 2022
- https://www.yourdictionary.com/cyberspaceRetrieved on 15th April 2022
- https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Social%20engineering%20is%20the%20term,in%20one%20or%20more%20steps. Retrieved on 1st September 2022
- https://www.veracode.com/security/malicious-codeRetrieved on 1st September 2022
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3217699/#:~:text=Intellectual%20property%20rights%20(IPR)%20refers,a%20given%20period%20of%20time. Retrieved on 1st September 2022
- https://www.geeksforgeeks.org/intellectual-property-in-cyberspace/Retrievedon 1st September 2022

- https://blog.hootsuite.com/how-to-deal-with-trolls-on-social-media/Retrieved on 1st September 2022
- https://www.malwarebytes.com/spoofingRetrieved on 03rd September 2022
- https://www.techopedia.com/definition/1655/email-bombRetrieved on 03rd September 2022
- https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/Retrieved on 03rd September 2022
- https://www.securitymagazine.com/articles/96510-salami-attacks-small-deposits-resulting-in-significant-lossesRetrieved on 04thSeptember 2022
- https://www.computerhope.com/jargon/d/data-diddling.htmRetrieved on 04th September 2022
- https://www.malwarebytes.com/spam#:~:text=Spam%20is%20any%20kind%20of,phone%20calls%2C%20or%20social%20media. Retrieved on 04th September 2022
- https://www.hindustantimes.com/cities/mumbai-news/india-third-most-targeted-country-by-phishing-campaign-report-101670179300520.html retrieved on 04th September 2023