International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s, 2025
https://theaspd.com/index.php

A Study Of Cyber Crime Awareness

Japan Babu[1], Dr. Vikalp Shrivastava[2]
[1]Research Scholar, Department of Law, Christ (Deemed to be University)
[2]Asst. Professor, School of Law, Christ (Deemed to be University) Delhi NCR, Ghaziabad, Uttar Pradesh

Abstract:
Nowadays, most information is handled online, leaving it open to cyber threats. Cybercrime has seriously harmed people, businesses, and even the government. In the modern world, cybercrime is becoming a very severe concern.A variety of laws and procedures have been put in place to prevent it, and those who engage in cybercrime are subject to sanctions. Our lives are made better by the internet, but there are also some drawbacks. Cybercriminals are always looking for novel methods to target active online victims. Everybody uses computers nowadays, regardless of age. An accurate understanding of cybercriminals' behavior and the impact they have on people from different socioeconomic strata is necessary to prevent cybercrimes. Therefore, this study publication offers insight into cybercrimes, their impacts on society, and victims of cybercrime. Additionally, it examines the effects of several online safety measures.
Keywords: *Cyber Attacks, cyber threats, Cyber Crimes, Precautions, etc., financial crimes, cyberstalking, telecommunication frauds, cybercriminals, email-related crimes, email bombing, emailspoofing.*

I. INTRODUCTION

The pace of modern life is too quick to take advantage of time as a performance enhancer. Only the usage of the Internet makes it feasible. The Internet is a network of electrical connections connecting a large number of computers, numbering in the millions.The internet is connecting to millions of computers. Although everyone appreciates using the Internet, there is a drawback to it: online criminal activity. Any breach of a law that forbids or mandates it, whether it is performed out or not, and for which a penalty is given upon conviction is referred to as 'cybercrime.' Cybercrime includes, among other things, unlawful access to another person's computer system or database, the modification or theft of material that has been stored locally or online, and the disruption of hardware and data. The area of the Internet known as 'cyberspace' is growing swiftly, as are the crimes committed there.

Cybercrime is the umbrella word for a wide range of offenses committed online using devices such as computers, laptops, tablets, internet-enabled TVs, gaming consoles, and smartphones. Due to the widespread use of services made possible by the Internet and information technology (IT), a new category of crimes known as 'cyber crimes' is growing quickly. The crimes that may be punished are listed in the Information Technology (IT) Act of 2000. This Act does not cover all illegal acts that are committed while using computers since its main goal is to establish an environment that facilitates their usage commercially. With the acceptance of electronic records by the law and the revisions to numerous IPC sections made by the IT Act, of 2000, a number of offenses with a bearing on the cyber-arena are also recorded under the relevant parts of the IPC.

II.NEED & SIGNIFICANCE

In today's world, there isn't enough time and due to the Novel Coronavirus, we are supposed to work online from Home. There are a ton of payment gateways available for online purchases, but hackers might compromise those accounts and commit online fraud. Additionally, social media sites have more preferences for us. We are also pornographic victims. This is yet another cybercrime offense. The 'Information Technology Act, of 2000' is a government law that aims to avoid this cybercrime in social interactions.

This study provides some basic information on 'cybercrime.' The study depends on people being aware of cybercrime. Thus, this study provides a means of avoiding being a victim of 'cybercrime.' This study also provides information on cyber regulations. Since adults are the most common 'cybercrime' victims, this study focused on adults in hopes of preventing 'cybercrime' victims among them. It is beneficial to avoid becoming a victim in other age groups as well.

III. RESEARCH DESIGN & METHODOLOGY

In order to balance procedural efficiency and relevance to the study's purpose, a research design is a framework of rules for analyzing as well ascollecting data. The research design acts as the study's conceptual framework and as a guide for gathering, measuring, and analyzing data.

3.1 Objectives of the research:

Based on preset goals, the researcher carried out a descriptive study; these aims are as follows.;

1. To study the awareness about cybercrime and victims of it.

2. To study various instances of cyber crimes experienced by users while using the Internet

3.2 Research Hypothesis:

The researcher has developed the following hypotheses, all of which are consistent with the goals.
Internet users are well aware of the risk of hacking.

3.3 Sampling Design and Method: - A simple design is a clear strategy for choosing a sample from a certain population; it describes the method or process that would be used in choosing the sample's components. The design sample might also consist of information about the size of the sample, or the number of items that would also include in the sample. Due to time restrictions, the study can only be conducted at Christ University since it is academic in nature and can only use a very small sample size.For research reasons, we took into account respondents who accessed online resources from all age categories. For the main data gathering, we utilized Google Forms, and we used an online questionnaire to get information from the students.

IV. DATA PRESENTATION, ANALYSIS AND INTERPRETATION

The goal of this study is to examine cybercrime awareness among Christ University students. This study also intends to raise awareness about cybercrime prevention strategies. This also provides advice on safety measures to adopt while working online.

4.1 To study the awareness about cybercrime and victim of it

Studying public awareness of cybercrime and its victims is the researches' initial goal. Most respondents now do the bulk of their daily business online, making it a regular part of their life.Depending on what they want,they utilize their cellphone, computer, laptop, etc. to access the internet.

4.1.1 Cyber Crime Awareness: Every day, several sorts of cybercrime, such as hacking, Trojan assaults, virus attacks, email spamming, etc., may occur throughout the transactions. We posed a number of questions to the respondents to gauge their knowledge of cybercrime and to research this goal. The percentage of respondents who are aware of cybercrime is shown in Table No. 1.

Table No.1: Cyber Crime Awareness

Types of Attack	Yes
Hacking	54.5%
Trojan Attacks	13.6%
Virus And Worm Attack	13.6%
Email Spamming	18.3%

The sorts of different cybercrime assaults and respondents' knowledge of them are shown in Table No. 1. It is evident from the above table that the majority of respondents are aware of cybercrime. 54.50 percent of respondents reported knowing about hacking, while 13.60 percent reported knowing about Trojan assaults. Furthermore, it is shown that 18.3 percent of respondents are aware of email spam, followed by 13.60 percent who are aware of virus and worm threats.
Therefore, it is evident that a high level of knowledge about cybercrime exists among the respondents.

4.1.2 Victim of Cybercrime

Cybercrime is the term used to describe any crime that makes use of a computer and a network.The computer might be the targetfor crime in some instances or may have been used to conduct it in others.There are many different forms of cybercrime, and just a handful of them are taken into consideration for research since they all affect our daily lives. The victims of numerous cybercrimes, such as hacking into bank accounts, piracy, pornographic social media websites, etc., are shown in Table No. 2 below.

Table No. 2: Victim of Cyber Crime	
Bank Account Hacking	18.2%
Piracy	22.7%
Pornography	9.1%
Social website hacking	27.3%
Online Identity Theft	22.7%

The victim of cybercrime in New Delhi is shown in Table No. 2. We may infer from the data that 18.2% of participants are victim of bank account hacking, 9.1% of respondents are victims of pornography, and 27.3% of respondents are victims of social website hacking. Furthermore, 22.7 percent of respondents have experienced online identity theft and 22.7 percent have encountered piracy.
It's observed that most of the respondents are victims of Piracy and Online Identity Theft.

V. TESTING OF HYPOTHESES

The hypothesis underwent many statistical tests. A hypothesis will be regarded as confirmed if the responses of the majority of the respondents do so.If not, it will be seen as being rejected. For this, information related to the hypotheses that were collected from respondents was employed.

5.1 Hypothesis The "hypothesis of the study is **'Users are highly aware of hacking while using the internet.'**

54.5 % or more usershave a positive attitude toward awareness of hacking. (H0: p = .54)

The awareness of hacking when utilizing the internet is used to test this notion. Most users(54.50 percent) are regarded to be aware of hacking.

Table No. 4 Z – Statistics of awareness of hacking

Respondents	*Sample size*	*Proportion*	*Standard error*	*Z – statistic"*
Users	22	.54.5	1.92	**0.2604**

As the sample sizes are >= 20 Consequently, the usual approximations are fulfilled.

Thus, the finding that 54.5% of users have a favorable attitude toward knowledge of hacking when using the internet indicates that 'Users are quite aware of hacking for security purposes, and this supports the idea.

VI. FINDINGS & CONCLUSION

This research report covers the key results from the study, as well as the conclusions and recommendations that resulted from it. The study's topic's published research was determined to be quite limited, and a number of areas and elements called for further investigation that would be more extensive and in-depth.

6.1 Findings

- This study has shown that the young generation uses the internet at a very high rate, according to the data.
- 54.50 percent of these internet users replied to the hacking incidents that happened during online purchases.
- The Trojan Attack is known to 13.6 percent of the respondents.
- It is shown that 13.60% of respondents are aware of viruses and worm attacks, whereas just 8% are aware of email spamming.
- 18.2 percent of respondents are victims of bank account hacking and approx 9.1 percent of respondents are victims of pornography and 27.3 are victims of social website hacking.
- 22.7% of respondents report being victims of online identity theft, while 22.7% of respondents report

being victims of piracy.

VII. CONCLUSION

This research proved that more than 95% of users are aware of cybercrime. Due to the pandemic and less time throughout the workday, they prefer most online activities. However, they do not feel safe while doing business online. It is evident that among the respondents, knowledge of cybercrime is highest for hacking when compared to the other types.Cybercrime may occur in a variety of ways, including via social media account hacking, pornography, bank account hacking, etc. Any such cybercrimes have affected some of the responders. Users worry about the security of their personal information while making online purchases.

REFERENCES

https://cybercrime.gov.in/Webform/Crime_OnlineSafetyTips.aspx
http://www.hcbam.org/article/cybercrime-awareness-among-the-people
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/defeating-cybercrime-with-awareness-and-good-habits/
https://economictimes.indiatimes.com/topic/cyber-crime-awareness
https://en.wikipedia.org/wiki/Cybercrime