International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Study on Cybercrime Awareness and Security

Harshadkumar Baluji Thakor

Research Scholar (Law), Gokul Global University

ABSTRACT:

The use of the Internet has become a daily routine for most of the people for daily transactions. The number of Internet users has grown enormously, as has cybercrime. Cybercrime is the crime that is carried out using the computer and the network. The threat of cybercrime is an ever-present and growing reality in both the private and professional sectors. With the advent of the Internet, old crimes have taken on a new look. The purpose of this research is to raise awareness about cybercrimes that are occurring in today's world and also to raise awareness about increasing cyber security. This article attempts to analyze cybercrime awareness among Internet users with different age groups and educational levels. The linear regression model has been applied to analyze both objectives. This document finds that there is a relationship between the age groups and the educational qualification of the respondents. Therefore, it is the duty of each and every netizen to be aware of cybercrime and security and also to help others by raising awareness among them.

KEYWORDS: Cyber-crime, Cyber criminals, Cyber security, Internet, IT Act, Awareness.

INTRODUCTION:

Internet in India is growing rapidly. It has given rise to new opportunities in the field of entertainment, business, sports, education and many more. With the advent and increasing use of the Internet, companies have crossed the barriers of local markets and are reaching customers located in all parts of the world. Computers are widely used in business not only as a tool to process information, but also to gain strategic and competitive advantage. Computers can be used for both constructive and destructive reasons.

The abuse of the Internet has given rise to new age crimes that are addressed in the Information Technology Act of 2000. As information around the world becomes more accessible, it also becomes more vulnerable to misuse. India is on the radar of cybercriminals with increasing cyber attacks against Indian establishments. India ranks third as a source of malicious activity on the Internet after the US and China, second as a source of malicious code, and fourth and eighth as a source or origin of web attacks and network attacks.

According to the Computer Emergency Response Team of India (CERT-In), 27,482 cases of cybercrime were reported between January and June (2017). These include phishing, virus or malicious code, defacement, scanning or probing, site intrusion, ransomware, and denial of service attacks.

It has been shown that in the first six months of 2017, at least one cybercrime was reported every 10 minutes in India, which is higher as compared to every 12 minutes in 2016. India has seen a total of 1.71 lakh crimes. cyber crimes in the last 3.5 years and the number of crimes so far this year has been 27,482, indicating that the total number is likely to exceed 50,000 in December. Analysis of data from 2013 to 2016 shows that 6.7% of all cases accounted for network scanning and probing, while viruses or malware accounted for 17.2%.

According to the latest report from the National Crime Records Bureau (NCRB), a total of 11,592 cases were registered under cybercrimes (including cases under the Information Technology Act, crimes under related sections of IPC and crimes under the Special and Local Laws (SLL)) compared to 9,622 cases registered during the previous year (2014) which shows an increase of 20.5% compared to the previous year. Uttar Pradesh has reported the highest number of such crimes, followed by Maharashtra and Karnataka.

The increasing rate of Internet usage has created a problem for people who spend long hours browsing the cyber world. In 2017, the number of mobile internet users grew by 12.49 percent compared to the previous year and 23.93 percent of the population accessed the internet from their mobile phone. This figure is expected to grow to 34.85% in 2022. (statista.com, 2017). Therefore, the increased use of the Internet has opened the door for cybercrime to flood. Lack of awareness on these issues will lead to emotional, moral or ethical financial damage.

Under such an alarming scenario, apart from tackling cybercrime, another issue that needs to be targeted at higher priority is raising awareness of "cybercrime and security" among internet users. Therefore, the current study focuses on finding the answers to alarming questions, that is, "Are people really aware that they are vulnerable to various cybercrimes?" “If they are aware, to what extent?”, and “If they are not aware, then what steps can be taken to make them more aware and up-to-date?

Understanding the Cyber Crimes:

Cybercrime refers to any crime involving a computer or network. It is an illegal act in which the computer is a tool, a target, or both. These are criminal activities committed through the use of electronic means of communication. It's taking something from the computer over the internet.

The term Cyber Crime has not been defined either in the Indian Parliament or in the Information Technology (IT) Act 2000. In India, the IT Act 2000 deals with offenses related to cyber crime. Cyber crime registration in India is carried out under the three general headings which are IT Act, Indian Penal Code (IPC) and Other State Level Legislation (SLL). Several Cyber Cells have been established to exclusively handle the cases that are registered under cyber crimes in India.

It is a fast growing crime area. Cyber criminals are exploiting the Internet to commit a wide range of criminal activities. In the past, cybercrime was mainly committed by individuals or small groups, but now cybercriminals constitute various groups/categories, such as professional hackers, organized hackers, children and adolescents between the age group of 6-18, scammers, phishers. , insiders, malware authors, spammers, etc.

Categories of Cyber Crimes:

The main categories of cybercrime can be broadly classified into the following four groups based on their objective and impacts:

1. Crimes against people:

These types of crimes are committed to harm private individuals. These include hacking, cracking, email harassment, cyberstalking, cyberbullying, defamation, disseminating obscene material, email spoofing, SMS spoofing, carding, deception and fraud, child pornography, threatening assault, denial-of-service attack, forgery, and spoofing.

2. Crimes against Property:

There are cyber crimes carried out to damage the property of an individual. They can be classified into: crimes against intellectual property, cybersquatting, cybervandalism, computer hacking, computer vandalism, computer forgery, transmission of viruses and malicious software to damage information, Trojan horses, cyber intrusion, theft of Internet time, theft or theft of money. while money transfers etc.

3. Offenses against the State/Business/Company/Group of people:

These types of crimes include cyberterrorism, possession of unauthorized information, pirated software distribution, web jacking, salami attacks, logic bombs, etc. The criminals in these want to terrorize the citizens of the country.

4. Offenses against the Company:

All the aforementioned crimes have their direct or indirect influence on society in general. Therefore, all such crimes are included in this one, such as pornography, online gambling, counterfeiting, selling illegal items, phishing, cyber terrorism, etc..

RESEARCH METHODOLOGY:

To test the awareness of cyber-crime and security, the following methodology has been applied:

a) Objectives of the study:

1. Examine the relationship between the respondent's level of education and cybercrime and security awareness.

2. Examine the relationship between different respondent age groups and cybercrime and security awareness.

3. To find out the internet use of the respondents.

4. Know the level of awareness about security in the use of personal computers and the Internet among Internet users in relation to cybercrime.

b) Sampling Design:

A structured questionnaire for the purpose of research was administered to 160 respondents. It was divided into four sections:

Section A deals with the demographic characteristics of the respondents.

Section B deals with respondents' Internet use.

Section C deals with the level of awareness of cybercrime and security.

Section D dealt with the level of security awareness when using personal computers and the Internet.

All data was collected using a 5-point Likert scale. (1 = Strongly disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly agree). Samples are drawn from various regions of Delhi-NCR.

c) Methods of Data Collection:

Primary data was collected from respondents through a questionnaire to analyze whether people are actually aware that they are vulnerable to various cybercrimes or not.

Secondary data: Substantial data was collected from various books, published national and international magazines, various websites, etc.

d) Research Tools:

For the findings of the study, Linear Regression technique was performed using SPSS Software version 23.

e) **Hypotheses:**

Based on the aforementioned objectives, the present study aims to test the following hypothesis (null hypothesis):

1. H01: There is a relationship between the educational level of the respondent and the awareness of cybercrimes among them.

2. H02: There is a relationship between the different age groups of the respondent and the awareness of cybercrimes among them.

CONCLUSION AND SUGGESTIONS:

With the increase in internet users, you can also see the increase in cyber crimes. There are various types of cybercrime that occur in everyday life. But people are not aware of all those types. Most people only know about hacking and viruses/worms. They are not aware of phishing, slander, identity theft, cyber bullying, etc. It is the need of today's world to be aware of these crimes that are associated with the Internet. The study shows that 48% of respondents share their personal data with other people, even if they don't know them closely. 55% of respondents agree that their PCs are often damaged by viruses. Internet users struggled with spam emails, phishing calls, and emails asking for their sensitive information such as mobile phone number, bank account, address, etc. It is the duty of each of us to know basic cyber security. Cyber security refers to the technologies and processes that are designed to protect computers, networks, and data from unauthorized access and attacks carried out over the Internet by cybercriminals. People should be aware of basic cyber security, such as:

a) Install security suites like Avast Internet Security, Kaspersky antivirus, McAfee antivirus, Norton Antivirus, etc. to protect the computer against threats such as viruses and worms.

b) Activate network threat protection, firewall and antivirus.

c) Always use secure passwords, preferably alphanumeric.

d) Communicate personal information only by phone or secure websites.

e) Do not click on links, download files or open attachments in emails from unknown senders.

f) Beware of links in emails that ask for personal information or pop-ups.

g) Verify that all antivirus software and computer operating system are up to date.

h) Double check the spelling of a website, URL, HTTP addresses, etc.

The government is also making efforts to control cybercrime. He has made cyber laws to help people learn about various cyber crimes and cyber security. The Information Technology (IT) Act 2000 deals with cyber-related crime. Not only the government but also the people need to work hand in hand to catch the criminals. People who have been victims of any of these cybercrimes must come forward and file a complaint against them in the special cybercrime cells. This will definitely help in tackling cyber crimes. Therefore, cybercrime and security awareness is a one hour must.

REFERENCES:

1. Aggarwal, Gifty (2015), General Awareness of Cybercrime. International journal of advanced research in computer science and software engineering. Vol 5, Number 8.

2. Aparna and Chauhan, Meenal (2012), Cybercrime Prevention: A Study of Cybercrime Awareness in Tricity. International Journal of Enterprise Computing and Business Systems, January, Volume 2, Issue 1.

3. Archana Chanuvai Narahari and Vrajesh Shah (2016).Cybercrime and Safety: A Study on Awareness Among Young Internet Users in Anand.International Journal of Advanced Research and Innovative Ideas in Education.Vol-2, Issue 6.