A STUDY OF AWARENESS OF CYBER CRIME AMONG COLLEGE STUDENTS WITH SPECIAL REFERENCE TO KOCHI

Sreehari A, KJ Abinanth, Sujith B, Unnikuttan P.S, Mrs.Jayashree
Department of Commerce and Management, Amrita School of Arts and Sciences
Amrita Vishwa Vidyapeetham, Amritapuri, Kollam, India
sree97hari@gmail.com
unnikutanps@gmail.com
abinath2010@gmail.com
sujitbbhanuvikraman@gmail.com
jayashrees@am.amrita.edu

Abstract- People dependence and behaviour towards information security and internet deeply affect the way they intend to use information technology. The increased dependence of people on internet has led to the rise in cybercrime. Problems such as lack of proper training and education, the poor awareness of cybercrime among Indians have also contributed to the growth in cybercrime. Even the law enforcement has faced huge problems in tackling cybercrimes due to the high rate of cybercrime. The paper intends to understand the awareness level of cybercrime among various college students of Kochi. The paper also intends to find out the college students' awareness on the types of cyber crimes and the various government schemes. The paper also finds out the various precautions taken by a student while using the internet. A questionnaire survey was conducted among 200 college students of Kochi in the state of Kerala to collect the required data.

Keywords: Cyber Crime, Youth, Awareness, Government Schemes, Precautions,

I. INTRODUCTION

The internet helps us in providing information as well as storing our data. It has become so crucial that it has become a vital part in people’s lives. However, due to the rapid increase in our modern technology, it has become very difficult in keeping our private information safe. Classified data are becoming easily available to people. This has lead to the increase in crimes as practically anyone can access one’s personal data without the victim’s knowledge. Internet has become a relief for the modern age, yet it also causes a burden on the people. The Internet has also bred a new kind of crime; cyber crime. Common internet users are unaware of cybercrimes. They are not aware of the proper precautionary methods to prevent such attacks from taking place. Many individuals have been a victim to cybercrimes around the world. For a cybercrime to occur, the criminal only requires a computer and access to internet. Cybercrimes have led to the creation of hacking, identity theft, Credit/debit card frauds, cyber terrorism and many more crimes. Cybercrimes can occur to anyone if their information or data is stored in the network.

Cybercrimes create a nuisance for the law enforcement. This is because these crimes are extremely difficult to trace back to the criminal. Also the digital footprints of these criminals are also easily wiped by these criminals. Also the rate of the cybercrimes have increased at an alarming rate that it has practically become impossible to prevent a cybercrime from occurring.
II. LITERATURE REVIEW

Saroj Mehta and Vikram Singh’s (2013) research paper focuses on the awareness of cyber crime laws in India. It states that even though there exist firewalls, antivirus and many other effective measures to control cybercrime, India is still far behind in combating cybercrime. It was found out that there lies a significant difference between the awareness level of male users and female users.

Jagvinder Singh’s (2012) research paper is on cyber crime awareness among XII students in Bathinda, Punjab. It was found out that the gender of the students does not create a difference in the level of awareness of cybercrime. The stream chosen by the students also do not play a part in the awareness level.

Bijoy Saima’s research paper states that people's attitude towards information technology is a major cause for cybercrime awareness. This paper intended to find the level of awareness of among Law students. It was found out that there was a moderate levels regarding cybercrime awareness among the students. However a few percent of students knew and had proper knowledge regarding types of cybercrime which were listed under Information Technology Act, 2000.

Teena Jose, Y.vijayalakshmi, Dr.Suvanam and Sasidhar Babu researched on the cyber crimes in Kerala. With the advancement of technology, cybercrimes increases. The Kochi city in Kerala was the highest state in the cybercrime attacks. The various cybercrimes and the popular mobile crimes are stated here.

P.S. Dowland, S.M. Furnell, H.M. Illingworth and P.I. Reynolds researched on the public attitudes and awareness towards computer crime and abuse. It was found that the environment affects the public attitude. The media have been helpful in informing the public regarding cybercrime however it did a poor job in providing the proper remedies and corrective actions to counter cybercrime.

Sukanya K.P and Raju C.V. (April 2017) research paper focuses on the awareness of cybercrime among youth of Malappuram district. The youth of Malappuram district are aware of IT Act, 2000. Yet, they are ignorant about it. Basic ethics and the proper usages on IT applications must be introduced in schools. Also the media must provide proper information regarding cybercrime. The study found out that the youth have an idea regarding the security measures for combating cybercrime.

III. OBJECTIVES

1. To understand the awareness of cyber crime among college students in Kochi
2. To analyze the awareness of the various government schemes and programmes to combat cyber crimes among college students in Kochi.
3. To find out the various precautions taken by user to prevent cyber crime.

IV. RESEARCH METHODOLOGY

Using random sampling, this research was carried out in Kochi with 200 respondents. The respondents Are college students who are either undergraduates or postgraduates. The data was collected using online surveys which were sent to the students.

V. CYBERCRIME AND THE TYPES OF CYBERCRIMES

Cyber-crime can broadly be defined as criminal activities carried out by means of computers or Internet on unsuspecting victims. The various types of cyber crimes are:

- **Online Harassment**: It involves sending harassments letters, messages etc. via emails. This form of cybercrime usually occurs in social media.
- **Cyber-Stalking**: It means tracking a personal whereabouts and creating a sense of invading a user’s personal space and also creating a sense of insecurity on the person.
- **Hacking**: It means unauthorized control/access over computer system. It involves unauthorized access and use of a person’s computer and collecting private data and deleting personal data.
- **E-Mail Spoofing**: It refers to sending fake emails to random internet users with fake sender address.
- **SMS Spoofing**: Spoofing is a blocking through spam which means the unwanted uninvited messages. In this case, an offender sends out false messages to the victim to steal his identity and personal data such as bank information.
- Carding: It means use of false ATM cards i.e. Fake Debit and Credit cards used by criminals which is used by them to withdraw money from the victim’s bank account.
- Virus attacks: It involves the criminals releasing harmful viruses into the victims’ computer with the intention of damaging and deleting his personal data and also to extract information from the computer.
- Email spamming: It involves sending thousands of emails to various users with the intention to get personal data.
- Illegal download: It means download of the latest movies via torrent and downloading the latest games. All these falls under cybercrimes.
- Identity theft: This refers to a crime where the criminal uses the victims’ names to conduct online transactions for his personal gain.

VI. CYBER LAWS IN INDIA

1. IT Act of India, 2000
The IT Act of India was passed by the Indian Government in May 2000, it contains the various cyber laws of the state. It is the law that deals with cybercrime and e-commerce. The Act was based on the United Nations Model Law on Electronic commerce. The Act aims to provide legal structure for all electronic transactions in India. Chapter IX of the Act states about the various penalties for cybercrime offences. The Act also talks about the compensation for the victims affected by cybercrime which does not exceed Rs. 100, 00,000. The Act talks about the various offences that can be classified as cybercrime.

This act was formalized by the Indian Government in 2013. It was taken as a step to counter cybercrime. The purpose of this document is to ensure a secure a safe cyberspace for the citizens of India. The Cyber Security Policy ensures protection of information in cyberspace, reduce vulnerabilities, and minimize the threats of cyber incidents and also to minimize the damage from cybercrimes. The policy states that education and training programmes are required for reducing the cybercrime rate. The policy aims to create 500,000 professionals within 2018 through advanced training and skill development programs. The policy plans to launch various national awareness programs across the country with a view to increase cybercrime awareness. The policy calls for a public and private partnership in order to tackle the cybercrimes.

3. Cyber Swachhta Kendra
The Cyber Swachhta Kendra is an initiative taken up by the Government of India to create a secure cyberspace by detecting botnet infections and to enable cleaning and securing systems of users so as to prevent further infections. This policy is set up in accordance with the objectives of the ‘National Cyber Security Policy’. The policy operates in close coordination with various internet service providers and antivirus companies to notify the users regarding the bot infection in their computer and also provides them assistance to clean their systems. The policy also aims to provide awareness regarding botnet, malware infections and measures to be taken to prevent malware infection.

VII. FINDINGS

The present study titled ‘A study of awareness of cybercrime among the college students with special reference to Kochi’ used a questionnaire survey as the major tool for collecting required data. The total sample size of the study was set at 200. The respondents of the survey was college students and the age group ranged from 18-27. The respondents were of different colleges: Rajagiri, Amrita Vishwa Vidyapeetham, SCMS, Maharaja’s College, SNGIST, St. Xavier’s college for women etc.

<table>
<thead>
<tr>
<th>TABLE 1. RESPONDENT’S GENDER</th>
<th>FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>110 (55%)</td>
</tr>
<tr>
<td>female</td>
<td>90 (45%)</td>
</tr>
</tbody>
</table>
The data showed that large percentage of the sample (55%) was male and rest of them female (45%). There were 110 males and 90 females.

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-21</td>
<td>154 (77%)</td>
</tr>
<tr>
<td>21-23</td>
<td>34 (17%)</td>
</tr>
<tr>
<td>Above 23</td>
<td>12 (6%)</td>
</tr>
</tbody>
</table>

The age group of samples was 18-25, where the majority of the respondents were of the age group of 18-21 (77%). Only 17% of the sample was of the age group 21-23 and 6% of the age group 23-25.

Findings on internet usage

- 47.8% respondents spend less than 2 hours on the internet. 23.2% respondents spend between 2-5 hours on the internet. 13.5% respondents spend between 5-7 hours on the internet while 15.5% spend more than 7 hours on the internet.
- 86% of the total respondents spend their time on the internet in social media websites. 55.1% of the total respondents spend their time watching videos. 42.5% of the total respondents spend their time surfing the web while only 24.6 of the total respondents use the internet for leisure.
- 94.25% respondents download various content from the internet, while only 5.8% do not download anything.
- 68.1% of the total respondents admitted that they downloaded movies, 85.3% of the total respondents download music, 66.25 downloaded various study material while only 39.2% downloaded general content such as Apks, books, software, games etc.
- 27.5% respondents download content very frequently. 43% respondents download quite often. 20.3% respondents download less frequently. 7.7% rarely download any content while only 1.4% never downloads anything.

Findings on Cybercrime awareness and safety

- 25.1% respondents are very aware about cybercrime. 51.7% know about cybercrime. 21.7% don’t know very well about cybercrime, while only 1.4% doesn’t know anything about cybercrime.
- 87.8% of the total respondents know about hacking. 71.8% of the total respondents know about virus attacks, 53.7% of the total respondents know about identity theft, 59.6% of the total respondents know about credit/debit card fraud.
- 80.3% have never been a victim to a cybercrime scam while 12.5% have been a victim once. 4.3% have been a victim to cybercrime scam 2-5 times and 2.9% have been a victim more than 5 times.
- 63.9% respondents strongly agree that it’s essential to be safe to be online, 22.1% agree to it, while 5.8% disagree to it. 1% strongly disagree that it is necessary to be safe while a user is online. 7.2% are neutral.
- 4.3% feel very safe about their information while being online, 20.7 are comfortable about their information while online. 52.4% have no idea whether they are safe or not. 18.3% don’t feel safe and 4.3% do not feel safe at all.
- 5.8% of the total respondents were overcharged and have lost money due to cybercrime. 2.4% respondents have had fraud transactions. 3.8% have lost money from their bank accounts. A majority of respondents i.e. 76% have not lost money due to cybercrime.
- 40.9% respondents’ friends/family members got affected by cybercrime scam. 35.1% do not know whether their friends/family got affected by cybercrime scam. 24% respondents are sure that none of their family members/friends got affected by a cyber crime scam.

Findings on awareness on anti cybercrime schemes by government
- Only 5.3% respondents are very well aware of the anti cybercrime schemes. 18.3% just know about it. 31.3% have heard about it. 30.8% don’t know very well and have little information regarding it. 14.4% don’t know about it.
- 53.4% of the total respondents know about the Information Technology Act, 2000. 48.1% of the total respondents know about the National Cyber Security policy, 2013. 18.8% of the total respondents know about the Cyber Swachhta Kendra.

Findings on the precautions taken by a college student
- 64.9% respondents use antivirus for their personal mobile phones and computers. The remaining 35.1% don not use any kind of antivirus for their computers.
- 59% of the total respondents use password for their mobile phones and computers. 47.3% of the total respondents use number pin. 46.8% of the total respondents use fingerprint for security. While only 6.8% use face recognition as their security measure.
- 58.9% respondents rarely change their passwords. Only 3.6% respondents change their passwords weekly. Also 3.6% change their passwords once every two weeks. 19.4% change their passwords monthly. While the remaining 13.5% never change their passwords.
- 12.6% checks the verification of a website before entering it. 31.5% respondents check it sometimes. 22.1% checks the website’s verification occasionally. 21.6% only checks the website’s verification only when it looks suspicious and the remaining 12.2% checks the website’s verification only when it looks suspicious.
- 42.3% respondents never open any unwanted/unknown messages such as spam. 36.5% opens these unknown messages only when they are curious. 16.7% respondents opens these spam messages most of the time. The remaining 4.5% open these spam messages all the time.
- 81.1% respondents failed to report a spam call to the cyber police. Only 18.9% took the initiative to inform the cyber police regarding the spam calls.
- 47.7% respondents do not accept any unknown friend request received by them via social media websites such as Facebook, Instagram etc. 33.3% only accepts these requests if only if they have a mutual friend between them. However 18.9% accepts these unknown friend requests all the time.

Findings on trust on the existing Cybercrime laws
- Only 9% strongly agree that the cybercrime laws are strong enough to cybercriminals. 39.6% respondents agree that they are effective to control cybercriminals. 18.5% respondents disagree that the laws are effective while 6.3% strongly disagree that the laws are powerful enough to control and stop the cybercriminals. 26.6% respondents are on both sides, they are neutral.
- 15.8% strongly agree that the cybercrime can be completely eliminated in Kerala. 41.9% agree that the cybercrime can be eliminated in Kerala. However 14.4% disagree to it and 2.7% strongly disagree to the belief that the cybercrime can be eliminated in Kerala. The remaining 25.2% are neutral to this thought.
VIII: CONCLUSION

The research shows that only most users are just aware about cybercrime. It is clear that the ratio of awareness among the respondents regarding cybercrime is high for hacking when compared to other types. However it also shows that the most of these respondents are not properly aware of the cybercrime laws. Most of the respondents spend more than 2 hours on the internet. Also maximum respondents stated that they have no idea about the safety of their information while being online. It is clear from this that the respondents do not know the proper steps in ensuring that they keep their data safe. It was also found that a minority of the respondents have lost money during online transactions. Also a large percentage of the respondents rarely change their password for accounts which is also a safety threat. It is also clear that the respondents even though they are just aware about cyber crime still download various content such as movies, games etc. which falls under cybercrime. The study also found out that most of the respondents occasionally receive spam messages and spam calls but hardly anyone of these respondents failed to report it to the cybercrime police in order it to prevent it from occurring again.

IX: SUGGESTIONS

These are some of the suggestions based on the overall conclusions of the study. Few suggestions were made which can be helpful for all internet users as well the Government.

- Educating the students, right from school level about the dangers of cybercrime has to be given prior importance.
- The same strategy can be done in college level where workshops can be presented on cybercrime.
- Workshops and orientations from hackers and experts should be presented in order to get a clear idea of the cyber scam.
- Government should bring out awareness campaigns in various places of the state to bring more awareness among the people.
- Internet users are recommended to use strong and unique passwords for their social media websites.
- Social media websites can be used to bring more awareness regarding the crimes such as identity theft and fake user profiles.
- Rules and regulations that deal with cybercriminals should be strengthened so as to bring a sense of safety among the internet users.
- The cyber cell departments should be increased throughout the state to control the increasing cybercrime rate in the state.
- Changing of passwords every now and then is recommended in order to keep up with the high cybercrime rate.
- The punishment and penalties to the cybercriminals should be implemented as soon as they are caught.
- The internet users must strictly use antivirus software for their computers and update it on a regular basis.
- It is recommended that internet users use firewalls in their computers.
- The cyber cells must block all websites that potentially harm the internet users.
- The cyber cell must advise and recommend that the public inform them of the spam calls when they receive it.
- The cyber cells also must provide support and relief to the people who have lost money due to cybercrime scam, even if the amount is very low.
- It is recommended that people install intrusion detection software so as to provide a warning to the user regarding any breach.
- Internet users and businesses must back up their information daily so as to avoid data loss.

X: REFERENCES

2. Cyber Crime in the Society: Problems and Preventions
3. Evaluation of cyber crime growth and its challenges as per Indian scenario
   ISSN (online): 2347-1697 Volume 2 Issue 9 May 2015
4. To analyze cyber crime awareness of class 12 students- Jagvinder Singh
   ISSN- 2278-8808
5. Cyber Crime Awareness amongst students of Government Law College, Trivandrum – Bijoy Saima
6. A Study of Cyber Crime Awareness for Prevention and its Impact- Dr. Manisha K, Dr. Vidya G ISSN (Online) - 2455-1457
7. Cyber Crime and Security – A study on awareness among young netizens of Anand (Gujarat State, India)
8. Cyber crimes in Kerala: A study - Teena Jose, Y.vijayalakshmi, Dr.Suvanam, Sasidhar Babu