International Journal of Recent Trends in Engineering & Research
ISSN (ONLINE) : 2455 – 1457
IMPACT FACTOR : 4.101

A Study of Cyber Crime Awareness for Prevention and its Impact

Dr. Manisha Kumbhar[1],Dr. Vidya Gavekar[2]
[1]Professor, Sinhgad Institute of Management, Pune-41
[2]Asso. Professor, Sinhgad Institute of Management, Pune-41

Abstract: In the current era of online processing, maximum of the information is online and prone to cyber threats. Cyber crime is emerging as a very serious threat in today's world. The internet brings joy to our lives but at the same time it has some negative sides too. The cyber criminals are always in a search to find out the new ways to attack the possible internet victims. Today, everybody is using the computers i.e. from teenagers to adults. Cyber attacks may have some motivation behind it or may be processed unknowingly. Restriction of cyber crimes is dependent on proper analysis of their behaviour and understanding of their impacts over various levels of society. So this research manuscript provides the understanding of cyber crimes and their impacts over society along with victims of cyber crime. It also studies various precautions while using internet and its impact.

Keywords: Cyber Attacks, Cyber Crimes, cyber threats, Precautions etc.

I. INTRODUCTION

Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is cyber crime by the use of Internet. The term cyber crime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represents the cyber crime as ―Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or disrupt of equipment and data. The Internet space or cyber space is growing very fast and as the cyber crimes.

The term cyber crime refers to a variety of crimes carried out online, using the internet through computers, laptops, tablets, internet-enabled televisions, games consoles and smart phones. Cyber Crimes are a new class of crimes rapidly increasing due to extensive use of Internet and Information Technology (IT) enabled services. The Information Technology (IT) Act, 2000, specifies the acts which are punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of IT, certain omissions and commissions of criminals while using computers have not been included. Several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC with the legal recognition of Electronic Records and the amendments made in several sections of the IPC vide the IT Act, 2000.

II.NEED & SIGNIFICANCE

Because of lack of time in today's world, respondent are more like to work online. There is gateway to make a payment for online transaction, but hackers may hack their accounts and make online frauds. Social websites also have more preference by the respondent. There are also respondent made some cyber crime such as hacking others social accounts. Respondents are also a victim of pornography. This is also one of the offences of Cyber Crime. To prevent this Cyber crime in social life there is government act as "Cyber Crime Act 2000".

This research gives brief information about "*cyber crime"* .The research is depend upon the awareness about cyber crime. So this research gives the way to not being victim of "*cyber crime"*. Also this research gives the information about cyber laws. Adults are the most victim of "*cyber crime"*, so this research takes the adult age grout to study, which can help then to not be victim of "*cyber crime"*. In other age group also it's help to not being victim.

III. SCOPE OF THE SYSTEM

The scope of the research is citizen of Pune city.

IV. RESEARCH DESIGN & METHODOLOGY

A research design is the arrangement of conditions for collection and analysis in a manner that aims to combine relevance to the research purpose with economy in procedure. In fact the research design is the conceptual structure within research is conducted; it constitutes the blue print for the collection, measurement and analysis of data.

4.1 Objectives of the research:

Researcher has conducted descriptive research work on the basis of set objectives, the objectives are as follows;

1. To study the awareness about cyber crime and victim of it .
2. To study various precautions taken by user while using Internet

4.2 Research Hypothesis:

In consistence with the objectives, following hypotheses has formed by the researcher.

H_1: **U**sers are highly aware about hacking while using internet

H_2: Cyber crime gives insecure feeling about internet usage for safe transaction

4.3 Sampling Design and method: -A simple design is a definite plan for obtaining a sample from a given population it refers to the technique or the procedure would adopt in selecting items for the sample. Sample design may as well lay down the no. of items to be included in the sample i.e.; the size of the sample. As this is an academic research this research is restricted to very small sample size and due to time constraints the research is carried out research in Pune city only with 200 respondents from different parts of city. For study purpose we have considered respondents from age group between 15-30 years those used internet facility. We have used convenience sampling method for collection of primary data and it has collected from Student/Educated/Working class by using questionnaire.

V. DATA PRESENTATION, ANALYSIS AND INTERPRETATION

This research is aims to study the cyber crime and awareness about it among the citizens in Pune city. This research also aims to make aware respondent about cyber crimes and preventive methods about cyber crime. This also tells some precautions to take while working online.

5.1 To study the awareness about cyber crime and victim of it

First objective of the study is, "To study the awareness about cyber crime and victim of it". Now a day, most of the respondent does online transactions for their daily needs and that's why it becomes part of their routine life. They use internet by using their mobile, computer, laptop etc as per their needs.

5.1.1 Cyber Crime Awareness: During the transactions, various types of cyber crime may be happens every day like hacking, Trojan attack, virus attack, email spamming etc. To identify the awareness about cyber crime among the respondent and to study this objective, we have asked the various

questions to the respondents. Table No.1 shows the ratio of cyber crime awareness among the respondent.

Table No.1: Cyber Crime Awareness

Types of Attack	Yes
Hacking	182(92.50)
Trojan Attacks	43(21.50)
Virus And Worm Attack	23(11.50)
Email Spamming	16(08.00)

Note: Values in Bracket indicates percentages

Table No. 1 shows the types of various cyber crime attacks and its awareness among the respondent. From above table, it clears that most of the respondent are aware about cyber crime. It is observed that 92.50 percent respondent are aware about hacking followed by 43 percent respondent are aware about Trojan attack. Further it is observed that 11.50 percent are aware about Virus and worm attacks followed by 8 percent respondent are aware about email spamming.
So it clears that ratio of awareness among the respondent regarding cyber crime is high.

5.1.2 Victim of cyber crime

Cyber crimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime. There are various types of cyber crime and out of which few of them are considered for study purpose as an all of they are part of our routine life. Following Table No. 2 shows the Victim of various cyber crimes like Bank Account Hacking, Piracy, Pornography and Social website hacking etc.

Table No. 2: Victim of Cyber Crime

Cyber Crime	No. Of Respondents
Bank Account Hacking	62(31.00)
Piracy	39(19.50)
Pornography	51(25.50)
Social website hacking	51(25.50)
Online Identity Theft	31(15.50)
Hacking	69(34.50)
Instruction into Computer	18(09.00)
None	50(25.00)

Note: Values in Bracket indicates percentages

Table No.2 shows the victim of the cyber crime in Pune city. From the table we can conclude that 62 respondents that is approx 31 percent respondents are victim of bank account hacking and 51 each

respondents that is approx25 percent respondents are victim of pornography and social website hacking. Further 19.50 percent respondents are victim of Piracy and 15.50 percent respondent are victims of online identity theft. It is also observed those 34.50 percent respondents are victim of hacking and 9 percents respondent are victim of instructions into the computer.

It's observed that most of the respondent are victim of bank account hacking. Due to this reason they are not doing any online transaction. As per the primary data, we observed that out of 62, 23 respondents stopped online transactions.

5.2 Precaution while using Internet

Second objective of the study is, "To study various precautions taken by user while using Internet." While using Internet, need to take care of cyber attacks. Those respondents are aware about cyber attack and cyber crime they take care about it. But as per the awareness, most of the respondent doesn't know about precautions and also about IT act during Internet usage.

For this objective, we have asked the respondents that whether they take precaution during internet usage like Protect Identity, Changing login details frequently, assess link of file before click on a unknown origin, Checking security settings while post on social website, Use of or turn on Firewall, Use of Antivirus, Shopping at secured website and Changing login details frequently etc. For collection of data, we have used five point scales. For analysis of these data, we calculate Average value and identify the conclusion accordingly.

Table No. 3: Precaution while using Internet

Precaution	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Average Value
Changing login details frequently	87(43.50)	100(50.00)	5(02.50)	4(02.00)	4(02.00)	**4.31**
Protect Identity	88(44.00)	79(39.50)	16(08.00)	15(07.50)	2(01.00)	**4.18**
Use of or turn on Firewall	80(40.00)	91(45.50)	5(02.50)	18(09.00)	6(03.50)	**4.11**
Use of Antivirus	66(33.00)	88(44.00)	16(08.00)	20(10.00)	10(05.00)	**3.9**
Shopping at secured website	61(30.50)	94(47.00)	13(06.50)	20(10.00)	12(06.00)	**3.86**
assess link of file before click on a unknown origin	67(33.50)	78(39.00)	18(09.00)	30(15.00)	7(03.50)	**3.84**
Checking security settings while post on social website	58(29.00)	83(41.50)	12(06.00)	20(10.00)	27(13.50)	**3.63**
alert while using public Wi-Fi Hotspots	44(22.00)	84(42.00)	16(08.00)	31(15.50)	25(12.50)	**3.46**

Note: Values in Bracket indicates percentages

Above table shows various precautions taken by respondents while using Internet. It is observed that highest average value is 4.31 is for Changing login details frequently followed by 4.18 is for Protect Identity, 4.11 is for Use of or turn on Firewall, 3.90 is for Use of Antivirus. Also it is observed that while online shopping respondent are aware about their transaction with average value 3.86. Average value for assess link of file before click on a unknown origin is 3.84. Checking security settings while

posting any data on social website with average value is 3.63 and alert while using public Wi-Fi Hotspots average value is 3.46.

So its concludes that most of the respondent takes precaution while using internet for factors like Changing login details frequently, Protect Identity and Use of or turn on Firewall as compared to other factors.

VI. TESTING OF HYPOTHESES

Various statistical tools used to test the hypotheses. If the replies of a majority of the respondents support a hypothesis then that hypothesis will be considered as confirmed. Otherwise it will be considered as rejected. The data connected with the hypotheses and obtained from respondents has been used for this purpose.

6.1 Hypothesis 1: The first hypothesis of the study is **"Users are highly aware about hacking while using internet."**

H_0 Null Hypothesis: 92 % or more user have positive attitude towards awareness of hacking. (H_0: p = .92)

H_1 Alternate Hypothesis: <92% user have positive attitude towards awareness of hacking (H_1= p < .92)

This hypothesis is tested by using the awareness of hacking while using internet. It is seen that majority of the users (92.50 percent) are aware about hacking.

Table No. 4 Z – Statistics of awareness of hacking

Respondents	Sample size	Proportion	Standard error	z - statistic
Users	200	.9250	1.92	**0.2604**

As the sample sizes are >= 30 therefore normal approximations is satisfied. In this case Z-test and as one proportion is involved. As alternative hypothesis is in terms "if less than" hence rejection area is towards only one side hence it is one tail test at 5 Percent level of significance is considered. Table value for one tail test is 1.64. The decision rule is that if the calculated value of z is greater than 1.64, and then rejects the null hypothesis and if z is less than 1.64, do not reject the null hypothesis, accept it.

Standard Error (S.E.) for percentage = **1.92** and **Z = 0.2604.** As Z_{Cal}= |Diff| /S.E. is less than 1.64.
Z statistics of awareness of hacking is 0.144462 < 1.64 hence accept Null hypothesis at 5 Percent level of significance. Thus it is seen that 92 percent users have positive attitude towards awareness of hacking while using internet means "As a security reason, users are highly aware about hacking" and hence **the hypothesis is accepted.**

6.2 Hypothesis 2: Cyber crime gives insecure feeling about internet usage for safe transaction".
This hypothesis is tested by using 5 point scale with average value. The percent and average scale of responses were calculated by using the ratings. Following Table No. 5 shows the Percent value of Insecure feeling of Security of Online Transaction and its average value.

Table No. 5: Insecure feeling of Security of Online Transaction

Insecure feeling of Security of Online Transaction	No. of Respondent	percent	Avg. Scale
Strongly Agree	84	42	4
Agree	70	35	
Neutral	17	8.5	
Disagree	20	10	
Strongly Disagree	9	4.5	
Total	**200**	**100**	

It is clear that 77 percent respondents were agreed about the insecure feeling of Security of Online Transaction. Also the calculated value of average point rating scale is 4 represent the majority of the respondents are agreed about the enhancement insecure feeling of Security of Online Transaction. Therefore, it is to be concluded that, the hypotheses which is stated in the present study is **positively accepted.**

VII. FINDINGS, CONCLUSION & SUGGESTIONS

This research paper presents the important findings of the study; conclusion and suggestion arising out of the study are presented. It was observed during the course of the published research material on the subject of the study was strictly limited and a no. of areas and aspects required wider and in-depth research in future.

7.1 Findings

- According to this research; the findings we have gathered from this research are that the usage internet is quite high in youth generation.
- Out of these internet users 92.50 percent have response for the hacking have been occurred during online transaction.
- 43 percent respondents are aware about Trojan attack.
- It is observed that 11.50 percent are aware about Virus and worm attacks followed by 8 percent respondent are aware about email spamming.
- 62 respondents that is approx 31 percent respondents are victim of bank account hacking and 51 each respondents that is approx 25 percent respondents are victim of pornography and social website hacking.
- 19.50 percent respondents are victim of Piracy and 15.50 percent respondents are victims of online identity theft. It is also observed those 34.50 percent respondents are victim of hacking and 9 percents respondent are victim of instructions into the computer.
- 83.50 percent respondents changing login details frequently.
- 83.50 percent respondents protect their identity while using internet.
- 85.50 percent respondents Use of or turn on Firewall
- 77 percent respondents used Antivirus and Shopping at secured website
- 72.50 percent respondents assess link of file before click on a unknown origin
- 70.50 percent respondents Checking security settings while post on social website
- 64 percent respondents are alert while using public Wi-Fi Hotspots
- It is clear that 77 percent respondents were agreed about the insecure feeling of Security of Online Transaction.

VIII . CONCLUSION

This research proved that there are most users of internet. Due to less time during working hours they prefer most online transaction. But they are not feeling secure while making online transaction. Maximum respondent give response in the favor of neutral, so we can conclude that they are not feel secure about online banking transaction. It clears that ratio of awareness among the respondent regarding cyber crime is high for hacking as compared to the others. There are many ways of cyber crime happened as pornography, social account hacking, bank account hacking, etc. Among those respondents are victim of any of those cyber crime. Users feel insecure about Security of their details during Online Transaction.

IX. SUGGESTION

The respondents have put forward certain suggestions which have been summarized into a more organized form by the researcher:

- Cyber crime cell should provide some preventive measure for online transaction.
- Online banking system should provide secure mechanism for secure transaction
- Cyber crime should solve as soon as possible pending cases
- Respondent should have to check whether they work on fishing site or not. They should prevent fishing page bay some anti-fishing technique.
- In rural area there are not awareness about cyber crime so aware them by some advertisement.
- Students are most victim of cyber crime, so make them aware about cyber crime.
- Pune City should have to provide some strong mechanism for prevent cyber crime.

REFERENCES

I. http://www.icai.org/resource_file/19132comp_sugans_pe2_it_cp13.pdf
II. http://www.icai.org/resource_file/19132comp_sugans_pe2_it_cp13.pdf
III. http://www.icai.org/resource_file/19132comp_sugans_pe2_it_cp13.pdf
IV. http://www.euro.who.int/__data/assets/pdf_file/0006/74463/E89486.pdf
V. http://www.who.int/peh-emf/meetings/archive/fox_bsw.pdf
VI. http://www.dailymail.co.uk/news/article-1318992/Mobile-phone-health-risk-Phone-giants-accused-burying-warnings-handsets-small-print.html
VII. http://well.blogs.nytimes.com/2011/05/31/cellphone-radiation-may-cause-cancer-advisory-panel-says/
VIII. http://www.huffingtonpost.com/devra-davis-phd/cell-phones-and-brain-can_b_585992.html
IX. http://www.ccst.us/projects/smart/documents/072010Summary%20of%20the%20Literature-Cell%20%26%20Health.pdf
X. http://www.hindustantimes.com/Entertainment/Wellness/Is-mobile-phone-tower-radiation-a-health-hazard/Article1-889268.aspx

