Awareness among Internet Users towards Cyber Crimes

Sushma Rani,
Assistant Professor, Department of Commerce, Hansraj College, University of Delhi.
E mail sushmaharikot@gmail.com

Abstract

Cyber crime is vastly growing in the world of technology today. Criminals of the World Wide Web exploit internet users' personal information for their own good. This study seeks to explore the awareness among the internet users regarding various cyber crimes. It also examines their views about cyber security tools and methods. The research method used for this study was the survey method. It was a set of structured questions which were distributed to a number of participants using social media and personal contacts. This survey was completed by 119 respondents. Approximately 70% of the respondents have either an 'Average' or 'High' knowledge about these security measures. It is interpreted that only a small percentage i.e. 24% of the respondents has 'High' degree of awareness. 76 % are either in the 'Low' or 'Average' category. It is observed that approximately 62% views are on the positive side being indicated by 'Agree' or 'Strongly Agree' but still the percentage is low in to be a smart user. Though the results of chi square test indicated that there is no significant association between gender and cyber crime victims but the result was found significant between age and cyber crime victims since p value (0.0093021) was less than the significance level. It was also observed that the group 18-30 was most adversely impacted from the cyber crimes.

Keywords- *Cyber crimes, security, online, cyber attacks, internet.*

Introduction

In recent years, information and communication technologies and digitalisation has remarkably increased the demand for internet connectivity. According to reports of Global Digital Insights, the number of internet users in India increased by 128 million (+23%) between 2019 and 2020. Digital India is the result of many innovations and technology advancements. The idea of digitalisation was to use it as a boon for the country, but it has also led to an increase in the cyber crimes. The Kaspersky Security Network (KSN) report showed that its products detected and blocked 52,820,874 local cyber threats in India between January to March 2020. Cyber criminals are

undoubtedly using this as a chance to commit crimes. This study aims at examining the awareness of internet users towards various cyber crimes.

Cyber Crime is vastly growing in the world of technology today. Criminals of the World Wide Web exploit internet users' personal information for their own good. Cybercrime is a crime where a computer is used to commit a crime. A cybercriminal may use any device to access a user's personal information, private business information, government information, or to disable a device.

According to a report (https://purplesec.us/cyber-security-trends-2021) cybercrime as a whole has increased by 600% since the beginning of the global pandemic. An Economic Times report says that cyber attacks within India rose multiple times during the Covid-19 pandemic and reveals that threat actors targeted the States with Covid-19 themed attacks which aimed at exploited user trust. These attacks aimed to compromise computers and mobile services to get access over the user's confidential data and banking details. Thousands of people lost their hard earned money because of these instances. A majority of the recorded attacks were phishing attacks. They were using sophisticated campaigns so even the most educated users failed to identify whether it was a fraud. Users were encouraged to visit fake links.

'Prevention is better than cure' holds true in the case of cyber crimes.

Statement of the Problem

The cybercrime in India has increased amidst the country's unprecedented pandemic lockdown. The extreme measures have been accompanied by a vivid rise in cybercrimes across the country. Attacks have gone up by 86% in the four weeks roughly between March and April, 2020. According to a recent Reuters report quoting Indian Home Ministry officials and detailing "fake offers that Reliance Industries telecom arm Jio and streaming service Netflix Inc were offering discounted services" during the lockdown.

Personal data also continues to be an attractive target to the cybercriminals. Indian officials have reported that malware and phishing schemes operating under the pretext of COVID prevention efforts have similarly seen a steep rise since the outbreak. The so-called "coronavirus malware" is intended at stealing bank account details, password and other sensitive information from users.

The recent chaos on the change of privacy policy of What's App also brought attention to the topic of data security among users of social networking sites. The users must be aware about their data security while using internet as it is the most attractive target for cyber crimes. This study seeks to explore the awareness among the internet users regarding various cyber crimes. It also examines their views about cyber security tools and methods.

Review of Literature

Cyber crime is understood as the illegal activity

committed using the internet which is now a big threat to the nation. As the use of internet is increasing by which any information can be accessed easily from anywhere, so various illegal activities basing upon the internet are also increasing. Criminals are taking benefit of the fast internet speed and convenience provided by the internet to perform large and different 'against the law' activities. It becomes the duty of all the internet users to be aware of cyber crime and cyber law which are in place to deal with it. Here are some glimpses of research work already done in this area.

Mehta and Singh's (2013) study focused on cyber-crime awareness in India. It was found that there is a significant difference between the awareness level of male and female users, male users are more aware as compared to females. It finds that even though there exists antivirus and many other effective measures to control cybercrime, India is still far from combating cybercrime.

Sukanya and Raju 's (2017) research paper targeted on finding the awareness about the cybercrimes among youth of Malappuram district. The youth of the district are aware of IT Act 2000. Yet, they are ignorant about it. The study found that the youth have an idea regarding the security measures for combating cybercrime.

The study conducted by Norton (2013) which focused to understand the scenario of global cybercrime, found that India stands at the top position when it comes to spam attacks, at second position in case of virus attacks, and at third position in case of all kinds of threats.

Abdurrahman and Jibril's (2017) research paper found that having a sound socio-economic and technological environment is necessary to evade the existence of cybercrime. The study further pressed the need for a massive campaign awareness and action for all. Kandpal and Singh's (2013) research paper concluded that criminals have changed their method and have started using advanced technology. In order to deal with the needs of the society, the legal and law enforcement authorities will also have to come up with new policies and updated regulations. This is the duty of government, print media to educate the people about dangerous areas of the cyber world because prevention is better than cure.

Sarathchandra, (2016) conducted studies on risk perceptions, awareness and practices regarding cyber security amongst US college students. Study found that the students spend long times on the internet and have the wrong perception about cyber risks. The students have higher anxiety with the false things on online platform.

Research Methodology

The research method used for this study is the survey method using an online questionnaire. This method was considered most appropriate because it is a method involving search for opinions and views. Our survey method is an online questionnaire prepared for gathering data to get the results for user's awareness level. It is set of structured questions which were distributed to a number of participants

using social media and personal contacts. This survey was completed by 119 respondents. The sample was obtained using convenience method. This data is collected from primary sources.

This survey questionnaire was created by the use of google forms. There were total thirteen questions, out of which four questions were targeted to obtain demographic profile of the respondents. All the questions were multiple-choice questions.

Objectives and Hypotheses of the Study

The objectives of the study are as follows:

1. To understand the level of awareness of cybercrime among participants.
2. To know the most preferable web browsers.
3. To know the various anti-virus software used by them and various safety measures taken by them.
4. To study level of understanding of the users regarding causes and consequences of cybercrime.

Hypotheses

H_1: There is no significant association between gender and cyber crimes.

H_2: There is no significant association between age and cyber crime victims.

H_3 : There is no difference in the level of knowledge among various types of cyber crimes.

Data Analysis and Discussion

The present study aims at examining the 'Cyber Crime' and 'Cyber Security Awareness' among individuals of different age groups among different cities in India. An online questionnaire survey was used as the major tool for collecting the required data about the sample. The total sample size of the study was 119.

The data showed that large percentage of the sample 65.5% was male and rest of them were females (39.5%). There were 72 males and 47 females. 107 out of 119 total respondents belonged to 18-30 age groups. So we had young internet users as our sample in majority i.e. 90%. Only 9.2% of the sample was of the age group 30 -50.

Table 1 : Demographic Profile of the Respondents	
	Frequency
Gender	
Male	72
Female	47
Age	
Below 18	1
18-30	107
30-50	11
50 above	0
Employment Status	
Student	83
Self employed	6
Salaried employee	22
Other	8

As it is shown in Table 1, almost 88% of the respondents belonged to either students or the salaried employees group. Students are one

of the most active categories of internet users now a days. In the times of Covid-19 coronavirus more and more youth are taking benefit through online mode only.

Table 2: Have you ever been a cyber crime victim?	
Yes	12
No	107

The first question of the questionnaire was targeted to know the experience of the respondents of being a cyber crime victim or not. Out of the total respondents, 107 (89.9%) respondents have never been the victim of cybercrime and 12 (10.1%) have been the victim of such attacks.

Table 3: How often do you change your password?	
Daily	0
Weekly	5
Monthly	28
Annually	25
When forced	35
Never	26

Table 3 represents how often the respondents are changing their password. Password is one of the important tools to stop hacking and other online attacks. Ideally we shall change our passwords regularly. It is clear from the responses that out of the total respondents, no one is actually changing the passwords daily, and a handful of them (5) are changing them weekly. 28 people change their password monthly, 25 of them annually. A large percentage of the respondents i.e. 51.26% are almost never changing their passwords. These people are vulnerable to cyber crimes. It is important to be alert and aware while using online mode.

Table 4: Do you use two-step verification on social media/ payment platforms?	
Yes	92
No	11
Not aware	16

Out of total respondents, 92 (77.3%) use two step verification process, 11 (9.2%) don't use while 16 (13.4%) are not aware of two step-verification process. Two-step verification tool has been introduced by most of the payment platforms. It works as a check-post at the user's end. So on the basis of Table-4, we can conclude that most of the respondents are using this smart tool to protect against probable cyber attacks.

Out of total respondents 13 (10.9%) use Microsoft Internet Explorer, 9 (7.6%) use Mozilla Firefox, 109 (91.6%) use Google Chrome, 11 (9.2%) use Apple's Safari and 1 (0.8%) use Opera.

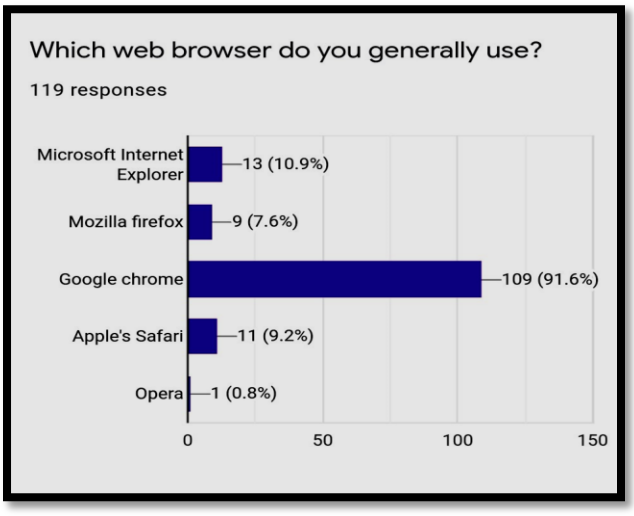

Figure 1: Most Popular Web Browser

So 'Google Chrome' was found a most popular web browser among our respondents. A good web browser shall provide a shield against cyber-attacks. The next question was besieged to know the same. The responses are being presented in Table 5.

Table 5: Do you think your browser have enough safeguard against cyber-attacks?	
Yes	42
No	18
Not sure	59

Out of the total respondents 42 (35.3%) think that their browser has enough safeguard against cyber attacks whereas 18 (15.1%) don't think so, while 59 (49.6%) people are not sure about such safeguards. It may be possible that they are using 'Google Chrome' because of its convenience or only because others are also using it (generally it is automatically uploaded). They might not be having knowledge about its security features.

Table 6: Level of knowledge to use IT-security measures.					
Options	Very low	Low	Average	High	Very high
Anti virus	8	13	59	31	8
Anti spyware	10	40	57	10	2
Anti spam	13	29	61	14	2
Software updates	0	10	52	47	10
Secure password practice	5	9	52	39	14
Back ups	3	16	56	31	13
Security measures on mobile devices	4	14	51	35	15
Firewall	15	29	55	14	6
Total Score (Points)	**58**	**160**	**443**	**221**	**70**

The next question tried to know the degree of knowledge about various security measures. The respondents were asked to rank themselves on a five point scale. The results are being given in Table 6. The last row shows the grand total of points. There were eight security measures and the respondents were required to select one level of knowledge from each measure. So the total points will be 952(119 x 8). Looking at the data it is quite obvious that approximately 70% of the respondents have either an 'Average' or 'High' knowledge about these security measure which is a positive symbol.

While last question revealed how much aware the respondents are about the security measures, the next question tried to understand their level of awareness about the various types of cyber crimes happening all around. The responses are being reported in Table 7.

Table 7: Degree of knowledge regarding the following types of cyber crimes			
Types of Cyber crimes	Low	Average	High
Phishing	33	58	28
Espionage	55	48	16
Stalking	19	47	53
Cyber pornography/ Childpornography	19	58	42
Cyber Terrorism	28	60	31
Sabotage	47	53	19
Programming a computer virus	49	50	20
Spoofing	54	48	17
Total Score	**304**	**422**	**226**

Table 8: Views on Statements related to Security						
Statements	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree	Total
I don't open attachments in mails from an unknown source.	**18**	**17**	**10**	**51**	**23**	119
If I see an unsolicited pop-up, I click on it to see what the website contains.	45	44	16	12	2	119
I look for a security icon, trust mark or HTTPS to verify that a website is secure before logging onto it.	**19**	**18**	**23**	**37**	**22**	119
I click on links in emails that request me to confirm my personal details.	43	40	13	15	8	119
I am concerned that the information I submit to online companies could be misused.	**14**	**14**	**28**	**38**	**25**	119

Total score has been taken the same way it was done for earlier question. But this time only three categories are provided to know their level of knowledge about various cyber crimes. It is interpreted that only a small percentage i.e. 24% of the respondents has 'High' degree of awareness. 76 % are either in the 'Low' or 'Average' category.

The last question of the questionnaire wanted to know the respondents' views on Security based on their personal behaviour while using the online mode. This will give a more real picture of how do they behave when encountered with some real life cyber attacks. Usually we all encounter such texts, messages, fake links, fraud emails etc. The responses to this question are being presented in Table 8.

Table 9.1 - Compiled scores after adjustments					
	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Statement 1	18	17	10	51	23
Statement 2	2	12	16	44	45
Statement 3	19	18	23	37	22
Statement 4	8	15	13	40	43
Statement 5	14	14	28	38	25
Total Score	61	76	90	210	158
Percentages	10.25	12.77	15.13	35.29	26.55

This table interestingly has both negative as well as positive questions. In case of 1st, 3rd and 5th statements 'Agree' or 'Strongly Agree' will give the positive indication. But in case of 2nd and 4th statements 'Strongly Disagree' or 'Disagree' are indicating a positive. So for the analysis these two statements were given a 180 degree rotation. The table finally was took the shape as Table 9.1. It is concluded from this table that approximately 62% views are on the positive side being indicated by 'Agree' or 'Strongly Agree' but still the percentage is low in terms of being a smart user. More and more users shall use all of these security measures to ensure online safety.

Testing of Hypotheses

Chi Square test can be used to test if the two variables are statistically associated with each

other significantly. The first two hypotheses are based on chi-square test and the third one uses the ANOVA.

H_1: There is no significant association between gender and cyber crimes.

p value for chi square = 0.6451354

MS Excel was used to apply chi square test by using the cross tabulation (by calculating the observed and expected frequencies) as given in Table 10.

Table 10: Cross Tabulation of Gender and Cyber Crimes

Gender/ Cyber Crime Victims	Male	Female	Total
Yes	4	8	12
No	43	64	107
Total	47	72	119

We fail to reject the null hypothesis at 5% level of significance and we conclude that there is no significant association between gender and cyber crime victims since p value (0.6451354) is more than the significance level. So we conclude that both males and females got affected from such crimes in almost a similar manner.

H_2: There is no significant association between age and cyber crime victims.

p value for chi square =0.0093021

A detailed Table 11 shows the observed and expected frequencies of age groups and cyber crime victimisation. We shall reject the null hypothesis at 1% level of significance and we conclude that there is a significant association between age and cyber crime victims since p value (0.0093021) is less than the significance level. So we conclude that not all groups are affected in a similar way. By observation it is clear that the group 18-30 was most adversely impacted from the cyber crimes. So this age group needs to be more careful as they are most vulnerable. They shall use various security measures to safeguard against such incidents.

Table 11: Cross Tabulation among Age Groups and Cyber Crimes

	Observed Frequencies					Expected Frequencies		
Age Group/ Cyber Crime Victims	Below 18	18-30	30-50	Total	Percentage out of Total	Below 18	18-30	30-50
Yes	0	8	4	12	0.100840336	0.2016807	10.68908	1.109244
No	2	98	7	107	0.899159664	1.7983193	95.31092	9.890756
Total	2	106	11	119				

Anova Test- is a statistical technique used to test the equality of three or more samples means and thus make inferences as to whether the samples come from population having same means or not.

H_3 :There is no difference in the level of knowledge among various types of cyber

crimes.

Table 12: Cross Tabulation between Level of Knowledge about Cyber Crimes versus Really being a Cyber Crime Victim

Level of knowledge/Cyber Crimes	Low	Average	High
Phishing	42	58	28
Espionage	56	48	16
Stalking	18	48	52
Childpornography	18	58	42
Cyber Terrorism	28	60	22
Ssabotage	45	52	20
Programming A computer virus	48	50	20
Spoofing	52	48	18

Table 12.1 Summary output

Groups	*Count*	*Sum*	*Average*	*Variance*
LOW	8	303	37.875	233.839286
AVERAGE	8	422	52.75	26.2142857
HIGH	8	227	28.375	172.267857

Single Factor Anova across different degrees of knowledge was applied. Since the calculated value of F is higher than critical value of F, we shall reject the null hypothesis and thus conclude that there is a difference in the level of knowledge among various cyber crimes. Looking at Table 12.1 it can be interpreted that majority of respondents are either low or average category which further makes them more exposed to fall prey to cyber attackers.

So, the first hypothesis concluded that there is no significant association between gender and cyber crime victims. Second hypothesis concluded that there is a significant association between age and cyber crime victims. And the third hypothesis concluded that there is a difference in the level of knowledge among various cyber crimes.

Conclusions and Suggestions

Approximately 70% of the respondents have either an 'Average' or 'High' knowledge about these security measures. It is interpreted that only a small percentage i.e. 24% of the respondents has 'High' degree of awareness. 76 % are either in the 'Low' or 'Average' category. It is observed that approximately 62% views are on the positive side being indicated by 'Agree' or 'Strongly Agree' but still the percentage is low in terms of being a smart user. Though the results of chi square test indicated that there is no significant association between gender and cyber crime victims but the result was found significant between age and cyber crime victims since p value (0.0093021) was less than the significance level. it was also observed that the group 18-30 was most adversely impacted from the cyber

Table 12.2 Anova Results

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	2415.08	2	1207.54	**8.37947129**	**0.00211**	3.4668
Within Groups	3026.25	21	144.107			
Total	5441.33	23				

crimes. On the basis of ANOVA results it can be said that the respondents have different level of knowledge about various types of cybercrimes. In other words it can be concluded that the respondents are not equally aware about these different types of crimes.

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.

1. Educating the student, right from school level about the dangers of cybercrime has to be given prior importance.
2. The same strategy can be done in college level where workshops can be presented on cybercrime.
3. Government should bring out awareness campaigns in various places of the state to bring more awareness among the people.
4. Internet users are recommended to use strong and unique passwords for their social media websites. Passwords should be changed regularly at least weekly.
5. Social media websites can be used to bring more awareness regarding the crimes such as identity theft and fake user profiles.
6. Rules and regulations that deal with cybercriminals should be strengthened so as to bring a sense of safety among the internet users.
7. The cyber cell departments should be increased throughout the state to control the increasing cybercrime rate in the state.
8. The internet users must strictly use antivirus software for their computers and update it on a regular basis.
9. It is recommended that internet users use firewalls in their computers.
10. The cyber cell must advise and recommend that the public shall inform them of the spam calls when they receive it.
11. It is recommended that people should install intrusion detection software so as to provide a warning to the user regarding any breach.

Bibliography

- Abdurrahman, U, A. and Jibril, A. U. (2017), "Perception of Cybercrime among Nigerian Youths" ISSN: 2394-4404, Volume- 4 Issue-12.
- Kandpal V. and Singh R. K. (2013), "Latest face of Cybercrime and its Prevention in India", *International Journal of Basic and Applied Sciences*, Vol-2, Issue-4, pages 150-156.
- Mehta, S. and Singh, V. (2013), "A study of awareness about cyber laws in the Indian society" ISSN (online): 2229-6166, Volume-4 , 2013
- Norton Cybercrime Report, Mountain View: Norton by Symantec, 2013.
- Sarathchandra, D., K. Haltinner and N. Lichtenberg, (2016) "College Students' Cybersecurity Risk Perceptions, Awareness and Practices", Cybersecurity Symposium, 2016.
- Sukanya, K.P. and Raju, C.V. (2017), "Cyber Law Awareness among Youth of Malappuram District", Volume -22, Issue-

4.

- https://ciso.economictimes.indiatimes.com/tag/kaspersky accessed on 8th June, 2021
- https://ciso.economictimes.indiatimes.com/tag/local+cyber+threats accessed on 8th June, 2021
- https://www.pandasecurity.com/en/mediacenter/panda-security/business-email-compromise/ accessed on 8th June, 2021
- https://economictimes.indiatimes.com/tech/internet/hackers-using-coronavirus-malware-to-steal-data-cyber-cops/articleshow/74842435.cms

https://www.reuters.com/article/us-health-coronavirus-india-fraud/scammers-try-selling-worlds-tallest-statue-as-pandemic-boosts-indias-cyber-crime-idUSKBN21P0KH

This would mitigate the anxieties and pains of the students making them skilled and employable. This would also attract more firms for recruitment thus making it a win-win situation for all the stakeholders leading to the economic growth of the nation.

References:

[1] AISHE 2018-19 report from MHRD
[2] Placement Cell data from Hansraj College
[3] National Education Policy (NEP) 2020, Ministry of Human Resource Development