International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 11
ISSN: 2454-4248
323 – 337

E- Crime Behaviour of Internet Users

Gagandeep Kaur Rosha[1], Mukhdeep Singh Manshahia[2*]

Department of Economics, Punjabi University Patiala, Punjab, India.
Department of Mathematics, Punjabi University Patiala, Punjab, India.
*Corresponding author email: mukhdeep@gmail.com**

***Abstract*—** Electronic crime or cyber crime refers to crimes that can only be committed using information technology such as phishing, data theft and payment fraud. Software called crime ware makes it easy to find and target the victims. E-commerce websites in particular are often seen as the "sweet spots", especially by organized criminals. Whilst some one-off attacks may be the result of disgruntled customers and organized attacks are more likely to be undertaken internally by staff or externally by organized criminals. This paper compiles e-crime nature, types, provides detailed review of work done in e-crime prevention and gives analysis of e-crime behavior of internet users based on a primary survey.

Keywords- *E-crime, Cybercrime, Information Technology, Internet users.*

*****

1. Introduction

Computer and the Internet are used by many people, governments and several organizations. Each of these entities has different goes in regard to ethical and moral values. Everyone aims at maximum satisfactions, by least involvement and also by gaining maximum benefits in returns. Each technical area presents new ethical challenges, which are needed to be seriously considered. Through good cooperation and common desire to achieve a healthier computing environment, a general ethical policy can be made [20].

Many street crimes has taken a tilt in past decade and also the time has gone when criminals committed crime by bribing employees, photocopying the documents and conducting surveillance on company personnel. Some more constraints/characteristics of cyber crime are [20]:

1. Low marginal cost of online activity due to global reach.
2. Lower risk of getting caught.
3. Catching by law and enforcement agency is less effective and more expensive.
4. New opportunity to do legal acts using technical architecture.
5. Official investigation and criminal prosecution is rare; not very effective sentences.
6. No concrete regulatory measure.
7. Lack of reporting and standards
8. Difficulty in identification
9. Limited media coverage.
10. Corporate cyber crimes are done by group of persons.

2. Frequent Cyber Crimes & Types of Crimes

Though criminals use many cyber crimes, some frequent cyber crimes are:

(1) **Financial Crimes:** Marketing the product through fake web site and through responses obtaining the credit card numbers and later misusing them. : Criminals use e-commerce (design websites) for fraudulent sales like soliciting fund for charitable institution or for bogus investment as they enjoy direct access to millions of prospective victims.

(2) **Cyber Pornography:** Spread of Child pornography and sexually implicit material.

(3) **Marketing Strategy for Illegal Articles**: Selling narcotics, weapons etc. through bogus web sites.

(4) **Intellectual Property Crimes:** This includes software piracy, copyright, infringement, trademarks violations, theft of computer code. New product plans, and product description, research, marketing plans, prospective customer lists etc.

(5) **Email Spoofing:** A copying / hacking e-mail and password, criminal send unwanted e-mails to one's acquaintances and spoils the image of the original person.

(6) **E-Murder:** By manipulating medical prescription in a hospital.

(7) **Political Crime:** Abusive Management of public funds by altering computer data. Bribery and corruption by manipulating data, Manipulation in election by adding more votes or denial of voting rights.

(8) **Theft of Telecommunication Services:** The criminals gain access to dial in/out circuits of an organization and then make their own calls like framing duplicate calling cards.

(9) **Information Piracy and Forgery:** Digital technology permits perfect reproduction of the original documents, examples are birth certificates, passport,

 ISSN: 2454-4248
323 – 337

false identity, counterfeiting of currency, negotiable instruments etc.

(10) **Money Laundering and Evasion:** Emerging technologies greatly assist in online gambling and concealing the origin of ill-gotten money. Legal money can also be concealed from taxation authorities. Due to the volume of electronic fund transfers the criminals bypass the banking system.

(11) **Electronic Terrorism**: Criminals use electronic intruding in government websites causing inconvenience by bringing them down within no time.

(12) **Electronic Funds Transfer Fraud:** Financial institutions are using electronic fund transfer systems. Criminals intercept them and divert the funds. Valid credit card numbers are intercepted electronically and data stored on a card can be forged.

(13) **Hacking:** Information theft from computers hard disk, removal storage etc. Data theft, data destroy, stealing and altering information.

(14) **E- Mail/Logic Bombs:** These are event/date dependent programs and are created to do something, only when a certain event occurs. Some viruses also act as logic bombs because they lie dormant throughout the year and become active on a particular date. Criminals send large number of e-mails to the victim till their server crashes.

(15) **Internet Time Thefts:** By stealing user name and password, criminals use for themselves and steal the internet time allotted to the purchaser.

(16) **Hate/Communal Crimes:** As building a web page is inexpensive and it reaches to billions of people to spread disgust or communal information or rumors.

(17) **Altering Websites:** The hacker deletes some pages of a website, uploads new pages with the similar name and controls the messages conveyed by the web site.

(18) **Spreading Computer Virus:** Criminals uses malicious software for spreading computer virus. A virus program then attaches to a computer or to file and then circulates to other file or to other computers on a network.

3. Cyber Criminals

Some known cyber criminals are [20]:

(1) **Kids:** Kids take pride in hacking into a computer system or a web site and commit the crime unknowingly without knowing implications.

(2) **Organized Hacktivists:** Social, political and religious activism attacks major web sites for diplomatic motives.

(3) **Disgruntled Employees:** Instead of going on strike previously they commit computer related crimes due to automation process and this brings entire system to collapse.

(4) **Professional Hackers:** Business Organizations store all information in their computers and the employees of rival organizations hack or steal the secrets for their benefit.

4. Cyber stalking

Cyber stalking is when a person is followed and pursued online. Their privacy is invaded, their every move watched. It is a form of harassment, and can disrupt the life of the victim and leave them feeling very afraid and threatened [17].

Stalking or being 'followed' are problems that many people, especially women, are familiar with. Sometimes these problems (harassment & stalking) can occur over the Internet. This is known as cyber stalking. The internet mirrors the real world. That means it also reflects real life & real people with real problems. Although it is rare, Cyber stalking does occur. A cyber stalker does not have to leave his home to find, or harass his targets, and has no fear of physical violence since he believes he cannot be physically touched in cyberspace. He may be on the other side of the earth or a neighbor or even a relative! And a stalker could be of either sex.

Typically, the cyber stalker's victim is ignorant about the rules of netiquette & internet safety. Their main targets are the mostly females, children, emotionally weak or unstable, etc. It is believed that Over 75% of the victims are female, but sometimes men are also stalked. The figures are more on assumed basis and the actual figures can really never be known since most crimes of such natures go unreported. Following factors motivate the cyber criminals [18]:

a) **Sexual Harassment:** This should not surprise anyone, since sexual harassment is also a very usual occurrence offline. The internet reflects real life and internet communications also makes it convenient for a stalker on the internet do cyber stalking without any personal presence

b) **Obsession for love:** It could start from an online romance and the rejected lover is not ready to accept the end of the relationship. Obsession stalking can start from real life or online and there is personal information sharing between the persons involved. This makes it effortless for the cyber stalker to annoy the victim [18].

c) **Revenge & Hate:** This could be an argument that leads to a hate & revenge relationship. Revenge vendettas are the result of arguments and actions which may have insulted someone. Sometimes you have been chosen as a random target by an unknown person to let out his frustrations online [18].

d) **Ego & Power Trips:** Sometimes stalkers use their online skills to “show off” power to their friends and you may become their random for fun and power “show off” [18, 21].

 ISSN: 2454-4248
323 – 337

Most people who receive threats online imagine their harasser to be large and powerful. But in fact the threat may come from a child who does not really have any means of carrying out the physical threats made.

Cyber stalkers can be categorized into 3 types:

a) **The common obsessional cyber stalker:** The common obsessional stalker refuses to believe that their relationship is over. Do not be misled by believing this stalker is harmlessly in love.
b) **The delusional cyber stalker:** The next type is the delusional stalker. They may be suffering from some psychological sickness like schizophrenia etc. A delusional stalker is generally an outsider & most often select sufferers who are married woman, a celebrity or doctors, teachers, etc. Delusional stalkers are hard to shake off [19].
c) **The vengeful cyber stalker:** These cyber stalkers are annoyed at victim due to real or imagined reasons. These stalkers may be stalking to take revenge for their imagined victimization. Ex-spouses and disgruntled employees can be vengeful cyber stalkers [17].

Two different kinds of cyber stalking situations can occur:

a) Online harassment & cyber stalking that occurs & continues on the internet.
b) Online harassment and stalking that begins to be carried on offline too. This is when a stalker may attempt to trace a telephone number or a street address. Always be careful what details you give out over the web and to whom.

5. Economic Crimes Under the Indian Penal Code (IPC)

The Indian Penal Code contains provisions to check economic crimes such as Bank Fraud, Insurance fraud, Credit card fraud, stock market manipulation, etc. The local police deal with the IPC crimes falling under the broad categories of 'Cheating' (Section 415-424), 'Counterfeiting' (Coins & Stamps Section 230- 263A and Currency Section 489A-489E) and 'Criminal Breach of Trust' (Section 405-409) **[15].**

6. Review of Literature

J Govil [1] made a study some of the preventive measures are also suggested under the title Ramifications of cyber crime suggestive preventive measure, for corporative house and law enforcement agency. Computer is developed as a new crime tool the information on computer is used a lot in a negative aspect and leading to several crime against computer and is as well commanding attention of various nations. The excessive uses of Internet and computer have put a threat to problem of cyber crime proliferations. More over the existing laws and present preventive measure are not at all effective to control crime. It further leads to laws of steal deny access destroy access to value information.

Shabana Kabeer et al.[2] studied about this relationship and they come to the conclusion that there is a relationship between e-crime and the mental illness among people. It will create awareness among people regarding e-crime and as well as on the crime ability due to psychological sickness.

Arthur K. K. et al. [3] concluded that that due to growth in both the computer and information technologies the field of digital forensics faces a number of upcoming challenges. It also involves a considerable human interpretation in order to reconstruct any particular sequence of news or events.

Gianluigi M. et al. [4] analyzed that In our society information represent a very important assets of both management & business, so a reliable information is very crucial in order to prevent & detect possible abuse & misuse if information. Several theories, methods & techniques should be applied or formulated enough in order to stop the increasing e-crimes. Majority of methods & techniques applied are based upon the experience of IT Professional & practitioners'. Here a new framework is being introduced based upon social, psychological & organizational theories. Here focus is done upon human behavior instead of upon IT, to better understand e-crime & to offer substantial overview of IT security.

A.B Patki et al. [5] proposed that Cyber civilization considers knowledge as an in legal part of society & human system. Along with the facilities, the evils of cyber should also be equally paid attention & also tackled through both technological & social network. Efforts on the lives of centralized and as well as globally sharable resource & support infrastructure appear to be the need. Here the consideration & case for United Nations is taken into account.

Peter M. Bednar et al. [6] put forward that on the several challenges the computer forensic investigators face in regard to the collaborative decisions making, communication & coordination… The opportunities, operational environment & the set of action of cyber criminals are being considered have in order to respond to the respective threat factors. The published framework for systematic thinking can be fit for purpose for supporting the collaborative enquiry & decision-making process.

Kwan l. et al. [8] Gamed a study that the future of e-business & e-commerce depend upon the ability of our legal institute that how they protect general users from the prevalence of cyber crime. While the development have new outgoing for the implementation of tools and techniques for cyber crime / attack, but there still lack of effective and absolute methodologies to be develop in order to procure the offended ones (cyber criminals).Several criminals remain unpunished and much detection goes unutilized. So the need of the law is to develop such an appropriate method that can help the organization to collect legal valid evidence from cyber crime, so that hassle / strict actions can be stepped towards cyber criminals.

Deng- Yiv Chiu et al. [9] conducted a systematic dynamic simulation model from both-crime attacking and defending side respectively. Several decision variables related

 ISSN: 2454-4248
323 – 337

to both the behavior and psychology of victim and the offended are included as well. Influence of simulation result and some suggestion are also proposed to reduce e-crime behavior. Cyber is the most worsening and the terribly developing problems that can lead to the loss of both financial and as well as personal information. However, another problem related to E-Crime as compared to other is that it's limitless; its boundaries are indefinite, so that the collection of evidence /proofs is also a very hard nut to crack.

Clay Wilson [10] analyzed that the attack by cyber criminals are quite similar to that of cyber terrorist because both had to loss national infrastructure. Cyber security should be enlarged in order to curb Computer crimes. Appropriate (federal) data about crime indicate that the growth in prosecution of computer crime is comparatively lower then that of growth of computer incidents. The current policy also doesn't provide an embayed effect on the attitude and activities of college students. Current policy as expressed in computer fraud and Abuse act doesn't hold any organizational management accountable, where the computer is being hacked by hackers. Severally organization also says that most of the computers intension takes place due to the lack of the host operating system that has latest fixes applied for hacker's volubility information through informal group linked by internet. While Govt. and private industry are reluctant to do so provide and advantage to the attackers. A recommendation is there to hold managers in the Govt. and private sectors, more accountable for keeping their computer system updated with the latest operating systems fixes to improve computer security.

Gregory B. White [11] made a model the whole work of the state, community nation depends upon the computer systems and networks so they have to suffer cyber crime / cyber attack in return of their interdependent usage. Some of the communities understand their responsibilities to prevent detect and respond to most natural & manmade disasters, but only few try to get involved in order to defend themselves from cyber attacks. Model which states and represent that structure in which it says that which communities and state can use to determine their land of prepare dues and to create a plan to improve their security posture , and as a result to developed a successful preventing or detecting related to cyber attack.

Neil C. Rowe [12] proposed a theory and according to him there have been exploring delegate deception in defensive tactics which are useful enough for military strategies by information system under cyber attack as during information warfare... Development of a tool "counter plan" on finding ways to foil a particular attack plan has taken place. Firstly the findings of all atomic ploys that interface with the plan have to take place. Ploys are simple deciles the operating system can d such as laying about the status of a file. The degree of difficulty the ploys cause is defined and then the "counter planning" is done by selecting the most cost effective tool (ploy) and assigning then the most appropriate presentation method to them. We should remain very careful enough else the attackers will realize, they are being derived and will terminate * game with them. It can be affected by a modified operating system.

Miles A. M. et al. **[13]** proposed that the Control system security defense mechanism may employee deception in the behaviors of human system & their interaction in order to make it more difficult for the attackers to plan and then execute successful planning & attacks. These deceptive defensive measures are just of all organized & then initialized to explore , according to based upon a deception taken my (which may be self induced or accidental) , and then the seven abstract dimensions of security , already proposed as a framework for the cyber security of control system.

Henry C. Lee [14] reveals that the rapid and the even increasing development in the usage of the computer technology and the integration of computer and communication technology have lead number of human information activities... Due to efficient and effective power of information processing, Now a days the computer has become the most effective and popular tool for the processing of data. Because of its large storage, a huge amount of data can be stored in it. Now a day Computer is being used in every field of modern technology, with the help of internet the several activities like shopping, getting service enable, and as well as communication and sharing information can be done without even getting face to face with others. Information technologies {IT} have enabled global business to flourish, but lead enables for several individuals to commit or perform crime and escape from law enforcement agencies. It is the largest and the overwhelming challenge for law enforcement agencies to curb the cyber attackers and to develop research direction for the e-crime investigations & computer forensics.

7. Analyses and Discussion

Total 100 respondents have been interviewed with help of a questionnaire. Detailed analysis of e-crime behavior of internet user is presented below: (*Source: primary survey)*

TABLE1: AGE

S. N.	ITEMS	NO.OF RESPONDENTS	PERCENTAGE
1.	BELOW 20	10	10%
2.	20- 30	68	68%
3.	30-45	14	14%
4.	ABOVE 45	8	8%
5.	TOTAL	100	100%

 ISSN: 2454-4248
323 – 337

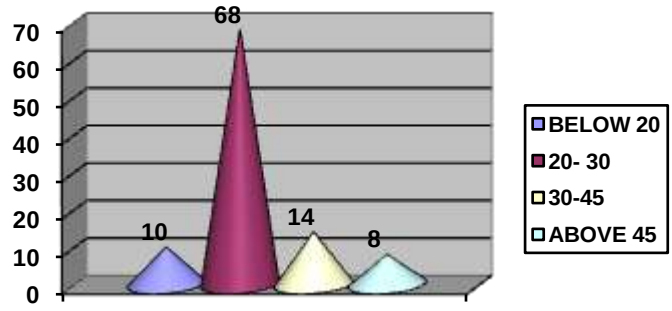


Table 1: linearly depicts that 68% of the respondents belong to the age group of 20-30 yrs, then 14% belong to age group of 30-45 yrs and 10% belong to the category of below 20 yrs and lastly 8% belong to the age group above 45 yrs.

TABLE 2: GENDER

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1	MALE	63	63%
2	FEMALE	37	37%
3	TOTAL	100	100%

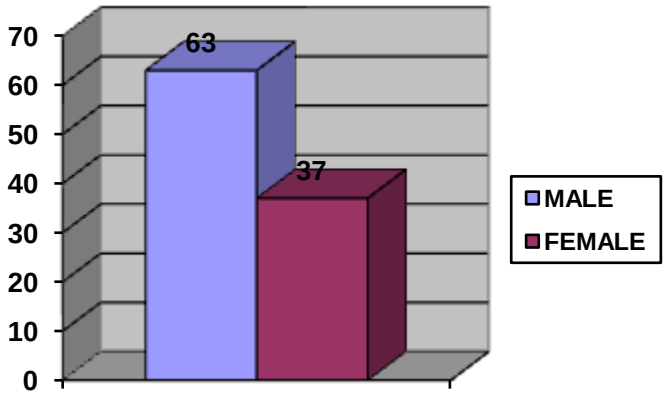


Table 2: explains that 63% i.e. majority constitute to be male and 37% constitute to be of female category

TABLE 3: EDUCATIONAL QUALIFICATIONS

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	MATRIC	2	2%
2.	DIPLOMA	10	10%
3.	UNDER GRADUATE	6	6%
4.	GRADUATE	28	28%
5.	POST-GRADUATE	41	41%
6.	DOCTRATE	13	13%
7.	TOTAL	100	100%

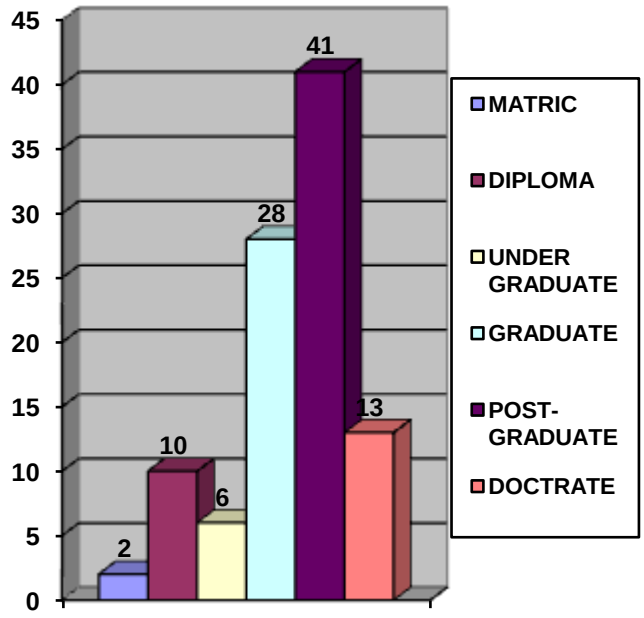


Table 3: clearly explains that regarding educational qualifications majority of 41% belong to post graduates section and 28% in graduate section, 10% are the diploma holders 13% are doctorate or done PhD then further 6% belong to under graduate group and 2% have done metric.

TABLE 4: EMPLOYMENT STATUS

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	WORKING	39	39%
2.	NON-WORKING	61	61%
3.	TOTAL	100	100%

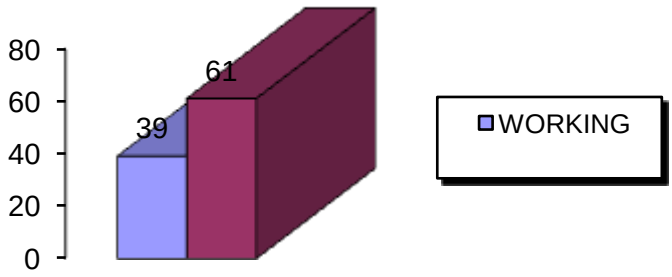


Table 4 shows regarding employment status, 61% are non - working so they don't have any income and 39% are working.

 ISSN: 2454-4248
323 – 337

TABLE 5: INCOME PER MONTH

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	WORKING		
	BELOW 7,000	2	5.13
	7,000 - 14,000	7	17.94
	15,000 - 25,000	9	23.08
	25,000 – 50,000	13	33.33
	ABOVE 50,000	8	20.52
2.	TOTAL	39	100%

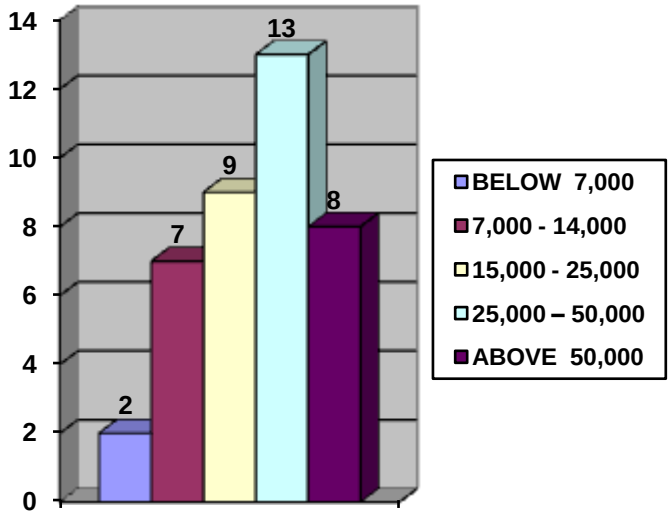


Table 5: depicts that 33.33% belong to the income group of 25000-50000, then 23.08% belongs to 15000-25000, 20.52% are earning income of above 50000, 17.94% earn income in between 7000-14000, lastly 5.13% are below 7000...

TABLE 6: INTERNET USAGE

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	1 – 2 hrs / DAY	29	29%
2.	5 hrs / DAY	8	8%
3.	3 – 5 hrs / DAY	24	24%
4.	MORE THAN 10 hrs / WEAK	7	7%
5.	LESS THEN 1 hrs	32	32%
6.	TOTAL	100	100

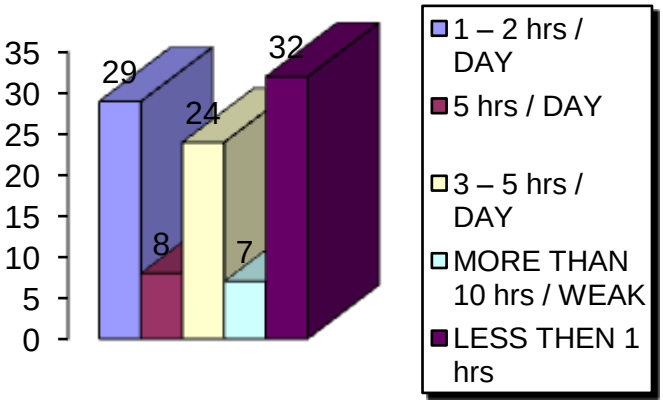


Table 6: shows that regarding the usage of internet , 29% use it for 1-2 hrs per day, 24% for 3-5 hrs per day, 8% for 5hrs per day , 7% for more than 10hrs per week and maximum is in the case of 32% i.e. less than 1hr .

TABLE 7: PURPOSE OF USAGE OF INTERNET

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	PRODUCTIVE	30	30%
2.	NON-PRODUCTIVE	21	21%
3.	BOTH	49	49%
4.	TOTAL	100	100%

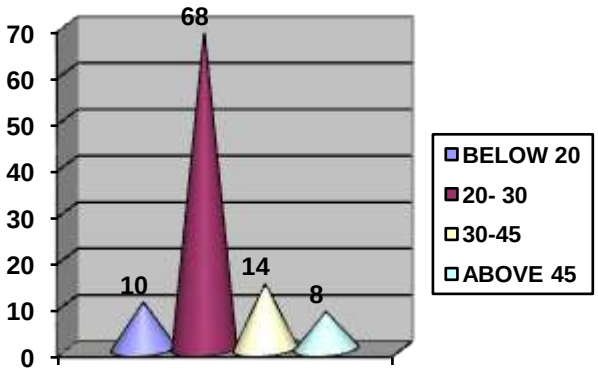


Table 7: depicts the purpose of using internet, and 49% of the respondents make the most of it for both the productive and non productive usage, 30% use it for the sake of productive purposes, lastly 21% make its use for unproductive purposes.

TABLE 8: AWARE OF NON- PRODUCTIVE INTERNET USAGE

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	72	72%
2.	NO	28	28%
3.	TAOTAL	100	100%

 ISSN: 2454-4248
323 – 337

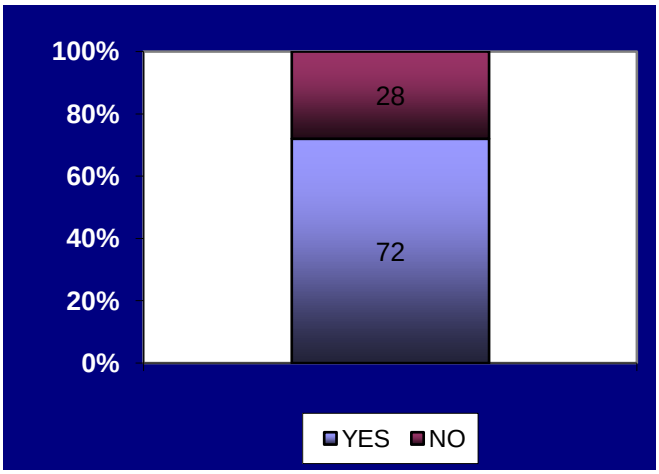


Table 8: depicts the awareness of the effect of unproductive internet usage, and 72% of respondents are aware of it and still 28% are not aware about it.

TABLE 9: ATTENTED ANY WORKSHOP REGARDING PROS AND CON OF INTERNET

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	30	30%
2.	NO	70	70%
3.	TOTAL	100	100%

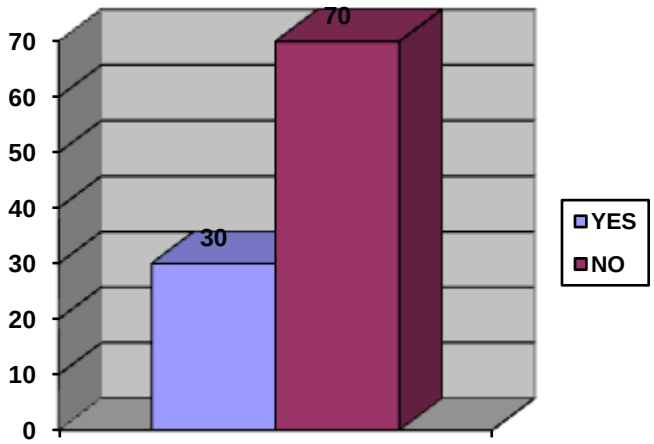


Table 9: deals with that have the respondent ever attended any workshop regarding the pros and cons of internet, then 70% which is a majority have never done so and only 30% have attended this kind of workshop.

TABLE 10: INTERNET'S ADVERSE USAGE LEADS TO CREATION OF SEVERAL CRIMES

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	64	64%
2.	NO	12	12%
3.	LITTLE BIT	24	24%
4.	TOTAL	100	100%

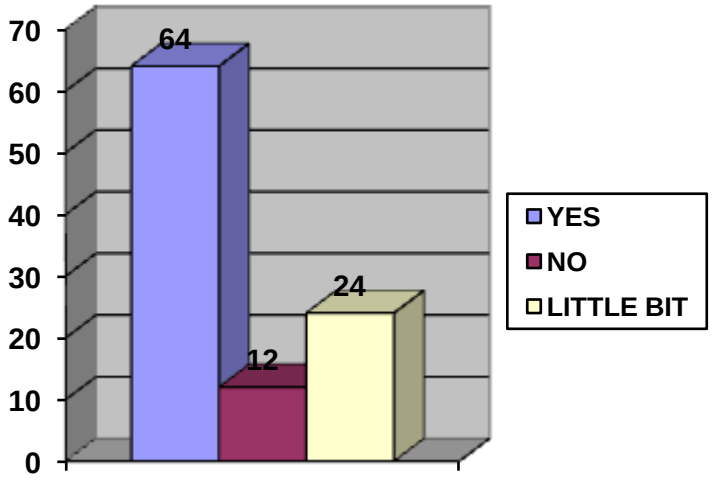
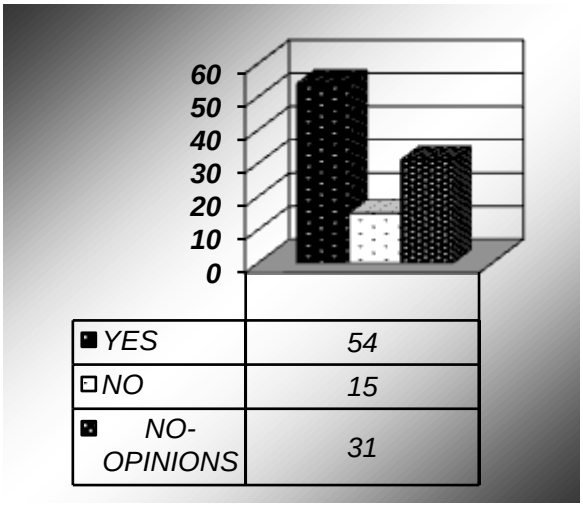


Table 10: explains that the adverse usage of internet may lead to the creation of several crimes then only 64% of respondents are aware of this fact and 24% have little knowledge regarding it and 12% do not have any knowledge about it at all.

TABLE 11: E-CRIME CREATES MENTAL ILLNESS

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	54	54%
2.	NO	15	15%
3.	NO-OPINIONS	31	31%
4.	TOTAL	100	100%



 ISSN: 2454-4248
323 – 337

Table 11: shows the analysis of, that e-crime creates mental illness depicts that 54 per cent of the respondents are aware of it and 31 per cent are having no opinion which is a shameful % whereas only 15% respondents are not at all aware of this thing that crimes committed on internet leads to mental illness as well.

TABLE 12: PREVENTIVE MEASURES DURING THE USAGE OF INTERNET

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	68	68%
2.	NO	20	20%
3.	OCASSIONALLY	12	12%
4.	TOTAL	100	100%

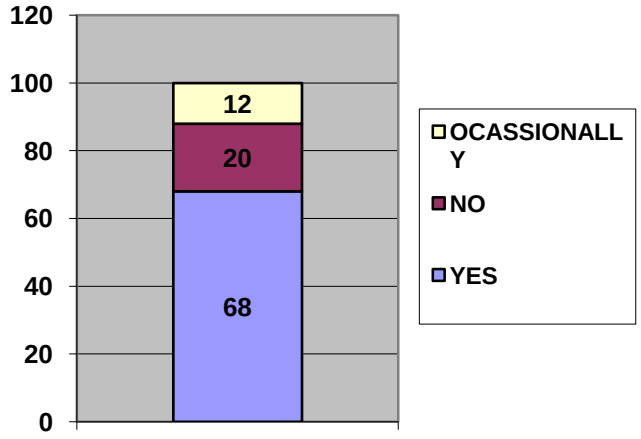


Table 12: shows that the preventive measures used during internet usage like security check, anti viruses installation by the users is 68 per cent of the respondents, and 20 per cent of the respondents do not use it at all whereas 12 per cent of the respondents occasionally use them, this no should be rose as fast as possible, in case of definite usage of preventive measures and even there updating should take place on a defined time interval.

TABLE 13: HAVE YOU EVER SENT ANY FAKE MAIL TO THE STRANGER

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	PUROSELY	12	12%
2.	BY – MISTAKE	24	24%
3.	NEVER	64	64%
4.	TOTAL	100	100%

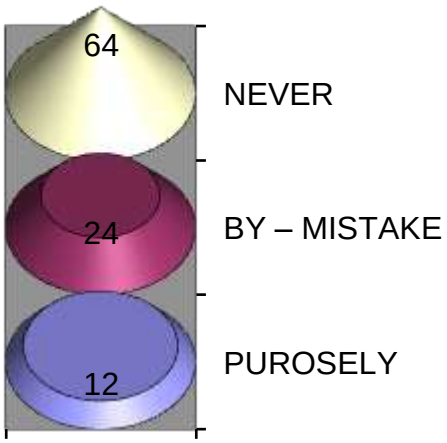


Table 13: studies about the sending of fake mails to the strangers I mean to the people never acquainted before, revealed that 64 per cent of the respondents does not do so, followed by 24 per cent may send those mails but not intentionally rather by mistake, 12 per cent of the users purposely send them which is a crime in itself.

TABLE 14: SENDING FRIEND REQUEST ON ANY SOCIAL NETWORKING WEBSITE TO THE STANGER

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	30	30%
2.	NO	15	15%
3.	JUST FOR YOUR FRIENDS	55	55%
4.	TOTAL	100	100%

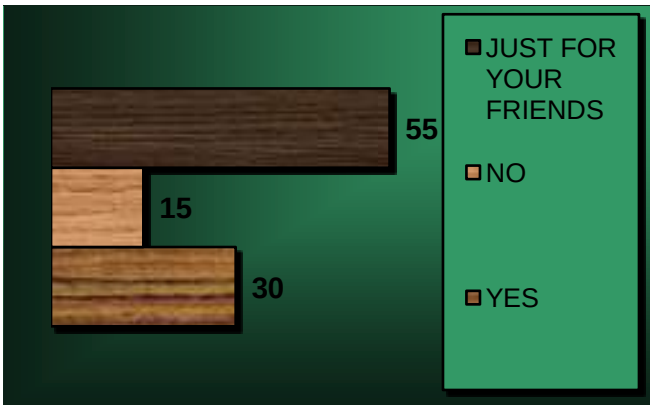


Table 14: depicts that 55 per cent of the respondents say that they send friend requests to their friends only, on any social networking site. The numbers of respondents who intentionally send these friend requests to strangers reveal that 30 per cent of the respondents, 15 per cent of respondents do not send these kinds of request to strangers.

 ISSN: 2454-4248
323 – 337

TABLE 15: DO U TRIED TO SPREED ANY VIRUSE, THROUGH FORWARDING CORRUPTED DATA

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	10	10%
2.	NO	74	74%
3.	UN-INTENTIALLY	16	16%
4.	TOTAL	100	100%

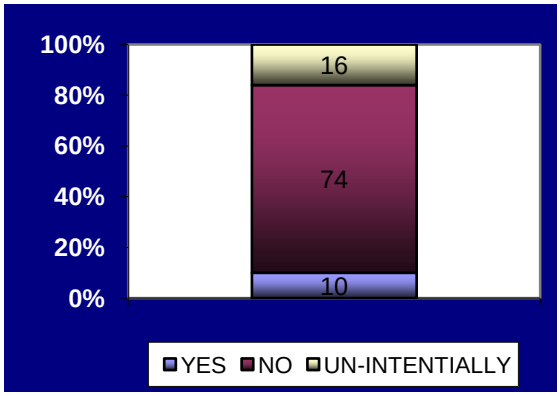


Table 15: shows that how many respondents tried to spread viruses through forwarding corrupted data then 74% majority said that they never did so and then 16% agreed that may be unintentionally it is done and 10% said yes they have forwarded this corrupted data and done the crime.

TABLE 16: HAVE U EVER DONE ANY UNAUTHORIZED LOG IN

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	BY INTENTION	15	15%
2.	BY MISTAKE	30	30%
3.	NEVER	55	55%
4.	TOTAL	100	100%

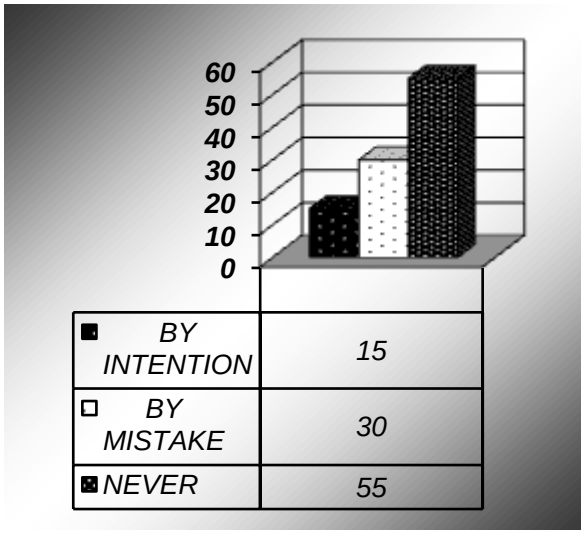


Table 16: shows the number of respondents who have unauthorized log in, is done by 15 per cent of the respondents intentionally , 30 per cent do it by mistake , 55 per cent of respondents never did so.

TABLE 17: HAVE YOU EVER STOLEN DATA & READY MADE MATERIAL PREPARED BY SOME ELSE

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	50	50%
2.	NO	30	30%
3.	NEVER	20	20%
4.	TOTAL	100	100%

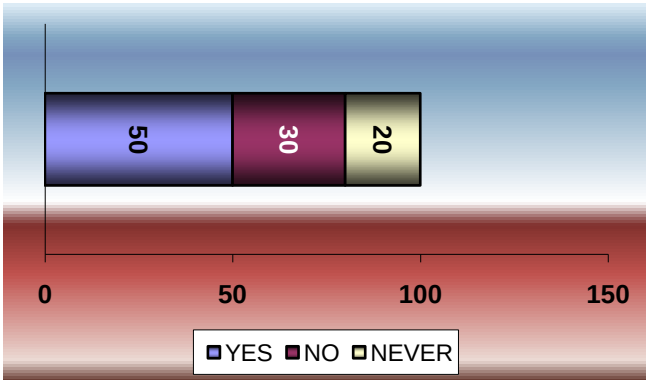


Table 17: studies about that, the usage of readymade material prepared by someone else, means ever stolen data shows that 50 per cent of the respondents do so, whereas 30 per cent of the respondents do not use it ever, 20 per cent of the respondents are of the opinion that they never stole readymade material prepared by someone else.

TABLE 18: DO YOU KNOW E-CRIME HAVE EFFECT ON E-COMMERECE

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	45	45%
2.	NO	31	31%
3.	NO – OPINION	24	24%
4.	TOTAL	100	100%

 ISSN: 2454-4248
323 – 337

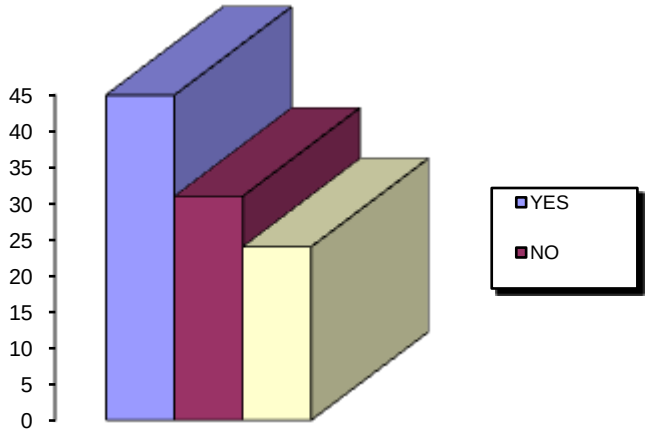


Table 18: defines that amongst the internet users, only 45 per cent of the respondents agree that e-crime have any effect upon e-commerce whereas 31per cent are not agreeing with these views and a huge percentage of 24% do not put any opinion regarding that e-commerce and e-crime are interrelated.

TABLE 19: HAVE U EVER PURCHASED ANY GOOD ONLINE

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	34	34%
2.	NO	50	50%
3.	PLANNING FOR IT	16	16%
4.	TOTAL	100	100%

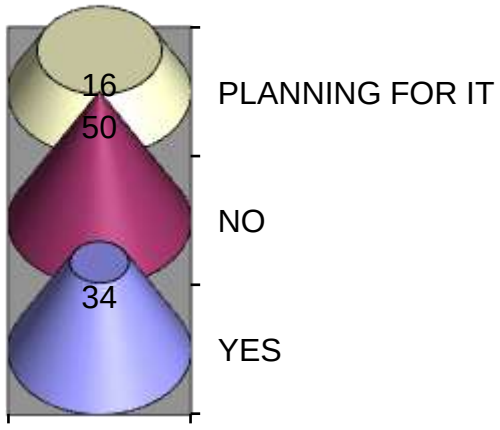


Table 19: reveals that 50 per cent of the respondents are never brought any product online and only 34 per cent of the respondents are making the purchases online; a large percentage 60 people are planning to make a purchase in the coming future.

TABLE 20: IF PURCHASE DONE ONLINE, MODE OF CONDUCT WAS

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	DIRECT ACCOUNT NO	9	26.47%
2.	CREDIT CARD	15	44.12%
3.	DEBIT CARD	10	29.41%
4.	TOTAL	34	100%

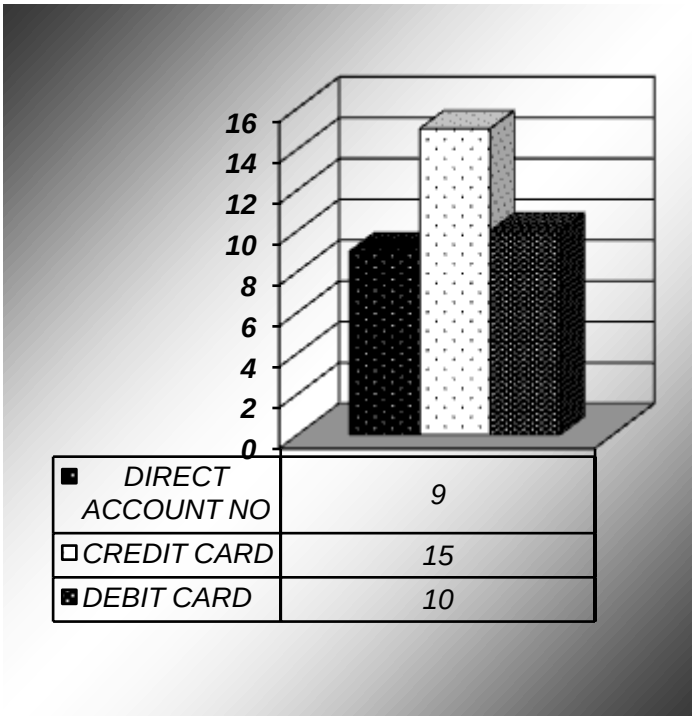


Table 20: shows that the respondents reply regarding the purchase made by them, the mode of purchase is mostly 10 of respondents i.e. 29.41% make the payment through master or debit cards i.e. 44.12% make the payment by credit card a whereas only 26.47 per cent i.e. 9 uses' payment mode is direct account number of the banks.

TABLE 21: ARE YOU SATISFY WITH THE DELIVERY OF GOOD PROCESSED THROUGH ONLINE PURCHASE

S. N.	ITEMS	PERCENTAGE
1.	YES	70.59%
2.	NO	29.41%
3.	TOTAL	100%

 ISSN: 2454-4248
323 – 337

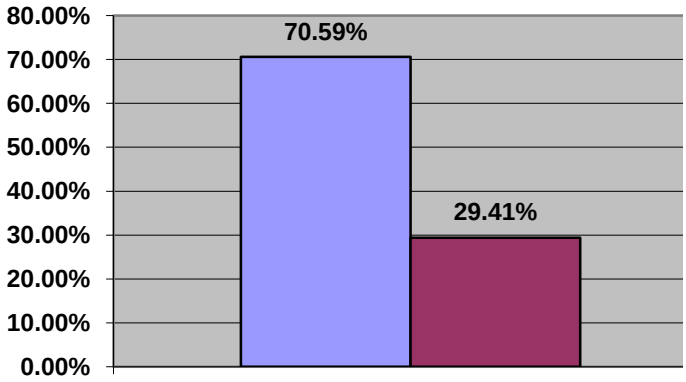


Table 21: reveals the, respondents reply regarding satisfaction of delivery of goods processed through online purchase depicts that 70.59 per cent of the respondents i.e. 24 people are satisfied, and 10 persons i.e. 29.41% are not satisfied through their purchase.

TABLE 22: ARE YOU VICTIME OF CYBER CRIME DURING ONLINE SHOPPING

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	9	26.47%
2.	NO	25	73.53%
3.	TOTAL	34	100%

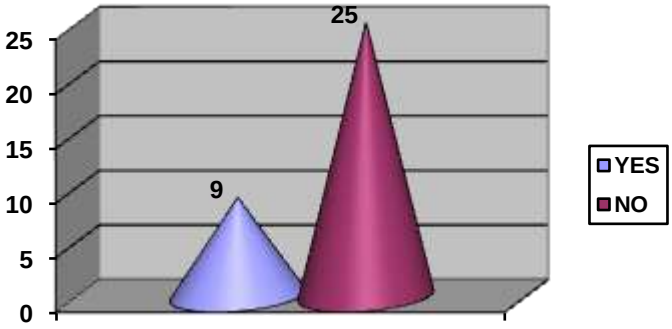


Table 22: depicts the respondent's opinion regarding that are they the victim of cyber crime during online shopping reveals that 26.47 per cent of the respondents i.e. 9 customers amongst the total of 34 are the victim of cyber crime and 25 customers i.e. 73.53% are of good opinion about that they were never the victim of cyber crime during their online purchase.

TABLE 23: HAVE THE HACKERS SUCCED IN BREAKING YOUR ID/PROFILE'S PASSWORD

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	ONCE	16	16%
2.	TWICE	13	13%
3.	NEVER	58	58%
4.	MANY TIMES	13	13%
5.	TOTAL	100	100%

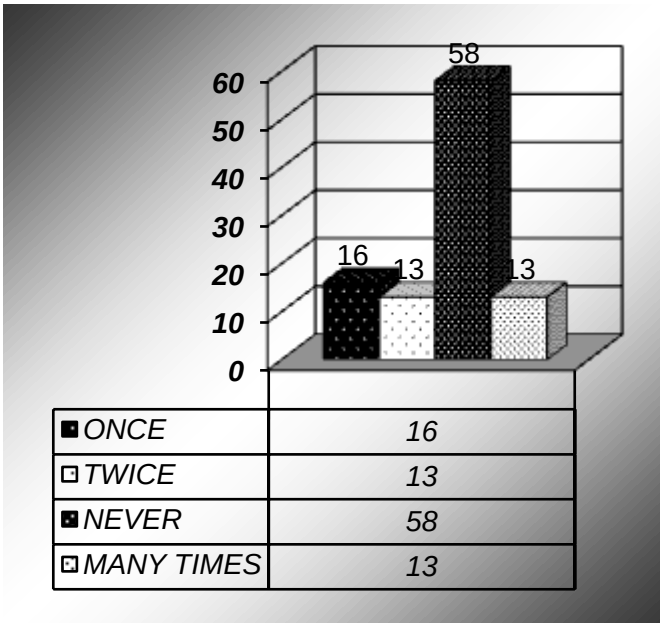


Table 23: made a study on respondents opinion about , that whether the hackers ever succeed in breaking their id or profile's password reveals that 58 per cent of the respondents never came across with these kind of difficulties , 13 per cent of the respondents are unsatisfied and their profile got hacked twice according to them and 13 per cent of the respondents are of the opinion that their profile or id got hacked many times, which made them face a lots of difficulties and still 16% respondent's are of the opinion that their id or profile got hacked once till now.

TABLE 24: HAVE OFTEN YOU UPDATE PASSWORD

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	WEEKLY	22	22%
2.	MONTHLY	29	29%
3.	ANNUALLY	22	22%
4.	NEVER	27	27%
5.	TOTAL	100	100%

 ISSN: 2454-4248
323 – 337

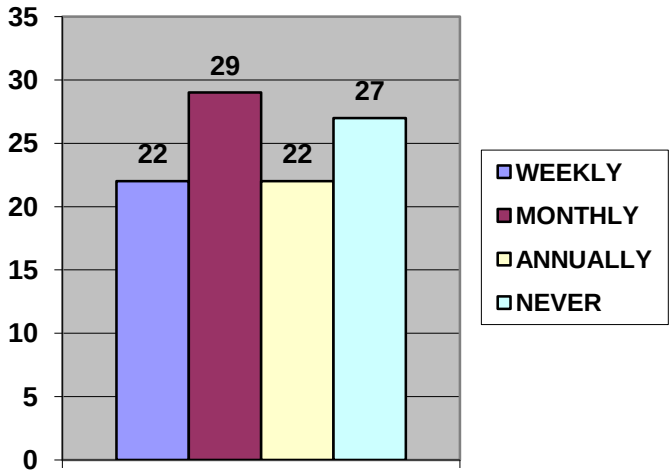


Table 24: made a study Regarding the updating of their password's refer to that 29% of the internet users do change it monthly and 27% of the users never did it, which is an alarming % rather password should be renewed frequently to avoid various further difficulties and 22% of the users change it annually which should also be improved and 22% of the users update it weekly which is a very nice practice and should definitely be carried on further.

TABLE 25: HAVE YOU MISUSED ANY STRANGER'S CREDIT CARD

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	8	8%
2.	NO	92	92%
3.	TOTAL	100	100%

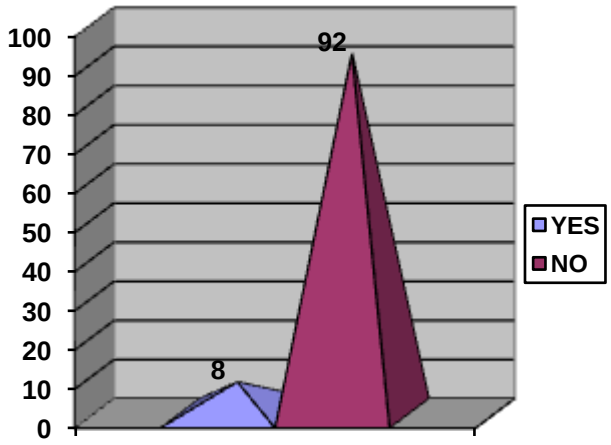


Table 25: made a study which reveals that whether the internet user ever misused any strangers credit card then 8% of the respondents agree that yes they did so and 92% per cent of the respondents are do not agree that means they never did so.

TABLE 26: HAVE YOU PUT ANY CONTRIBUTION FAR FOILING / STOPPING CYBER ATTACKS

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	24	24%
2.	NO	48	48%
3.	NEVER HEARD OFF	28	28%
3.	TOTAL	100	100%

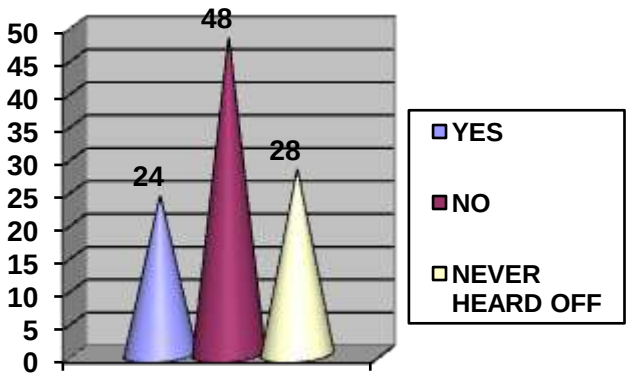


Table 26: made a enquiry which was that, have the user ever contributed for foiling or stopping cyber attacks then, 48 per cent of the respondents are disagree that they never contributed and 28 per cent of the respondents are neither agree nor disagree means they don't provide any opinion about the statement and further 24% of the user say that yes they have contributed for stopping cyber attacks.

TABLE 27: IS E- COMMERCE PLAYING AN IMPORTANT ROLE IN ECONOMICE DEVELOPMENT

S. N.	ITEMS	NO. OF RESPONDENTS	PERCENTAGE
1.	YES	82	82%
2.	NO	18	18%
3.	TOTAL	100	100%

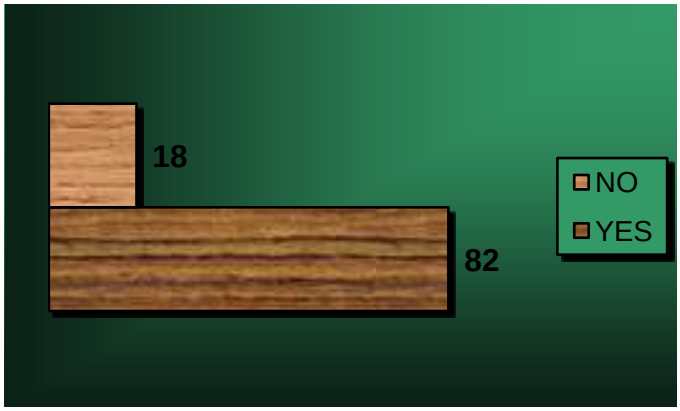


Table 27 made a study which lastly reveals that 82 per cent of the respondents have a strong opinion that, yes; e-commerce is playing an important role in economic development of the

 ISSN: 2454-4248
323 – 337

economy whereas only 18 per cent of the respondents don't agree to the above said statement.

8. Summary and Conclusion

E-crime, or computer crime and refers to criminals activities where a computer or network is at the source, tool or target or place of a crime and is generally defined as a criminals activity involving information technology infrastructure. THERE are several ethics of internet like arts, crime, software ownership& intellectual property, computer security, social behavior, role of government, the digital divide, computer enhanced information. ALSO ramifications of cyber crime and several suggestive measures are mentioned here along with criminals as well. A methodology is also being defined for profiling cyber criminals.

The attacking and defending perspective of e-crime and the psychology of criminals are also defined. Cyber law is explained along with the challenges faced during crime investigation is also illustrated.

The relationship between e-crime and mental illness also holds a great importance. In the present study, information regarding e-crime behavior of e-consumers has been collected from 100 consumers during April 2010 and May 2010 in Patiala city of Punjab. The sampling size includes 63 male and 37 female internet users form different areas, age groups, occupations as well as different income background. The Sex wise analysis shows that male internet users constitute 63% per cent and female internet users constitute 37% per cent of the total respondents. Age composition of the respondents reveals that maximum percentage that is 68% per cent belongs to the age group of 20 to 30 years, followed by 14% per cent belongs the age group of 30-45years, 10%percent belongs to the age group of below 20 years, 8 per cent falls in the age group of above 45 years.

Educational qualification of the respondents reveals that maximum percentage i.e. 41 per cent of the respondents are post-graduates, followed by 28 per cent are graduates, 13 per cent are doctorates or PhD, 10 per cent are diploma holders, 6 per cent are under graduates, 2 per cent are metric. The employment status of the respondents shows that 61per cent of the respondents are non- working and 39 percent are working.

This study further reveals that 33.33 per cent of the respondents having per month average family income of Rs. 25000 to Rs. 50000 and are 13 in number, followed by 23.08 per cent having the income level of Rs. 15000 to Rs. 25000 and the number is 9, 20.52 per cent having the income level of Rs. 50000 and above and the number is 8 people, 17.94 per cent having the income level of Rs. 7000 to Rs. 14000 and the no of people are 7, 5.13 per cent having the income level of Rs. below 7000 and 2 people fall in this category.

It reveals that regarding the usage of internet, i.e. 32% use it for less than 1 hour, 29% use it for 1-2 hrs per day, and 24 users use it for 3-5 hrs per day, then 8 people for 5 hrs per day, 7 users for more than 10 hrs per week.

This study states that maximum users use internet for both the productive and unproductive usages and is i.e. 49 per cent , 30% are using for the productive basis like study ,job, shopping, searching, e-mail and the non productive users i.e. 21 per cent, they make the most of it for chatting, scraping etc.

This study reveals that 72 per cent of the respondents are aware of the effects of the unproductive usage of internet and 28 per cent are still not aware about it, it's very essential and alarming to have awareness about the effects of unproductive usage... It means that people still require having more and better knowledge about computer and its usage. Respondents who are not at all attended any workshop raga are rdEng the pros and cons mean the advantages and disadvantages of internet (i.e.70percent) and have attended workshop are (i.e. 30 percent) which is quite low in number. The major reasons cited for this is lack of awareness and curiously amongst the internet users.

The results of this study further infer that 64 per cent of the respondents having the knowledge that internets adverse usage may lead to several crimes , followed by 24 per cent of the respondents have little bit hint of it and 12 per cent of the respondents have no knowledge regarding it , which should be essentially acquired.

The analysis of that e-crime creates mental illness depicts that show that 54 per cent of the respondents are aware of it and 31 per cent are having no opinion which is a shameful % whereas only 15% respondents are not at all aware of this thing that crimes committed on internet leads to mental illness as well.

The preventive measures during internet usage like security check, anti viruses installation by the users is 68 per cent of the respondents, and 20 per cent of the respondents do not use it at all whereas 12 per cent of the respondents occasionally use them, this no should be rose as fast as possible in case of definite usage of preventive measures and even there updating should take place on a defined basis.

Sending of fake mails to the strangers I mean the people never acquainted before revealed that 64 per cent of the respondents does not do so, followed by 24 per cent may send those mails but not intentionally rather by mistake, 12 per cent of the users purposely send them which is a crime in itself 55 per cent of the respondents say that they send friend requests to their friends only on any social networking site.... The numbers of respondents who intentionally send these friend requests to strangers reveal that 30 per cent of the respondents, 15 per cent of respondents do not send these kinds of request to strangers.

This study reveals that 50 per cent of the respondents are never brought any product online and only 34 per cent of the respondents are making the purchases online, a large

 ISSN: 2454-4248
323 – 337

percentage 60 people are planning to make a purchase. The respondents reply regarding the purchase made by them , the mode of purchase is mostly 10 of respondents i.e. 29.41% make the payment through master or debit users i.e. 44.12% make the payment by credit card a whereas only 26.47 per cent i.e. 9 uses' payment mode is direct account number of the banks.

The Respondents reply regarding satisfaction of delivery of goods processed through online purchase depicts that 70.59 per cent of the respondents i.e. 24 people are satisfied and 10 persons i.e. 29.41% are not satisfied through their purchase.

The results of this study further infer that 64 per cent of the respondents having the knowledge that internets adverse usage may lead to several crimes , followed by 24 per cent of the respondents have little bit hint of it and 12 per cent of the respondents have no knowledge regarding it , which should be essentially acquired.

The analysis of that e-crime creates mental illness depicts that show that 54 per cent of the respondents are aware of it and 31 per cent are having no opinion which is a shameful % whereas only 15% respondents are not having any knowledge and views regarding that.

The number of respondents, who have unauthorized log in, is done by 15 per cent of the respondents intentionally, 30 per cent do it by mistake, and 55 per cent of respondents never did so.

The readymade material prepared by someone else, means ever stolen data shows that 50 per cent of the respondents do so, whereas 30 per cent of the respondents do not use it ever, 20 per cent of the respondents are of the opinion that they never stole readymade material prepared by someone else.

Among the internet users, only 45 per cent of the respondents agree that e-crime any effect upon e-commerce whereas 31per cent are not agreeing with these views and a huge percentage of 24% do not put any opinion regarding that e-commerce and e-crime are interrelated.

The respondent's opinion regarding that are they the victim of cyber crime during online shopping reveals that 26.47 per cent of the respondents i.e. 9 customers amongst the total of 34 are the victim of cyber crime and 25 customers i.e. 73.53% are of good opinion about that they were never the victim of cyber crime during their online purchase.

Respondent's opinion about that whether the hackers ever succeed in breaking their id or profile's password reveals that 58 per cent of the respondents never came across with these kind of difficulties , 13 per cent of the respondents are unsatisfied and their profile got hacked twice according to them and 13 per cent of the respondents are of the opinion that their profile or id got hacked many times , which made them face a lots of difficulties... and still 16% respondent's are of the opinion that their id or profile got hacked once till now.

The respondent's opinion regarding that are they the victim of cyber crime during online shopping reveals that 26.47 per cent of the respondents i.e. 9 customers amongst the total of 34 are the victim of cyber crime and 25 customers i.e. 73.53% are of good opinion about that they were never the victim of cyber crime during their online purchase...

Respondent's opinion about that whether the hackers ever succeed in breaking their id or profile's password reveals that 58 per cent of the respondents never came across with these kind of difficulties , 13 per cent of the respondents are unsatisfied and their profile got hacked twice according to them and 13 per cent of the respondents are of the opinion that their profile or id got hacked many times , which made them face a lots of difficulties... and still 16% respondent's are of the opinion that their id or profile got hacked once till now Regarding the updating of their password's refer to that 29% of the internet users do change it monthly and 27% of the users never did it , which is an alarming % rather password should be renewed frequently to avoid various further difficulties and 22% of the users change it annually which should also be improved and 22% of the users update it weekly which is a very nice practice and should definitely be carried on further.

Further the study reveals that whether the internet user ever misused any strangers credit card then 8% of the respondents agree that yes they did so and 92% per cent of the respondents are do not agree that means they never did so... then the enquiry was that have the user ever contributed for foiling or stopping cyber attacks then , 48 per cent of the respondents are disagree that they never contributed and 28 per cent of the respondents are neither agree nor disagree means they don't provide any opinion about the statement and further 24% of the user say that yes they have contributed for stopping cyber attacks..

This study lastly reveals that 82 per cent of the respondents have a strong opinion that yes e-commerce is playing an important role in economic development of the economy whereas only 18 per cent of the respondents don't agree to the above said statement.

Acknowledgements

Authors would like to thank the researchers or academicians whose works have been cited in this paper. Authors are also grateful to Punjabi University Patiala for offering sufficient library and internet facility.

References

[1] J Govil, Ramifications of cyber crime suggestive Preventive measure Electro/Information Technology, IEEE, 2007.

[2] Shabana Kabee, Maqbool Uddin Shaikh , The Relationship between Cyber Crime and Mental Illness, IEEE, 2008.

[3] Kweku K. Arthur, Martin S. Olivier, Hein S. Vente, Jan H.P. Eloff, Considerations Towards a Cyber Crime Profiling System, IEEE, 2008.

[4] Gianluigi Me, Paolo Spagnoletti, Situational Crime Prevention and Cyber-crime investigation: the Online Pedo-pornography case study, IEEE, 2005.

[5] A.B. Patki, S. Lakshminarayanan, S. Sivasubramanian, S.S. Sarma, Cyber Crime Information System for Cyberethics Awareness, Department of Information Technology, Government of India, 2003.

[6] Peter M. Bednar, Vasilios Katos Cheryl Hennell, Cyber-Crime Investigations: Complex Collaborative Decision Making, IEEE, 2005.

[7] Federico Neri, Paolo Geraci, Gianluca Sanna, Liviana Lotti, Online Police Station : a state-of-the-art Italian Semantic Technology against cybercrime, IEEE, 2005.

[8] Leonard Kwan, Pradeep Ray, Greg Stephens, Towards a Methodology for Profiling Cyber Criminals, IEEE, 2008.

[9] Deng-Yiv Chiu, Tien-Tsun Chung, Chen-Shu Wang, Attacking and defending perspective of e-Crime behavior and psychology: A systemic dynamic simulation approach, IEEE, 2009.

[10] Clay Wilson, Holding Management Accountable: A New Policy for Protection Against Computer crime, IEEE, 2000.

[11] Gregory B. White, The Community Cyber Security Maturity Model, IEEE, 2007.

[12] Neil C. Rowe, Counter planning Deceptions: To Foil Cyber-Attack Plans, IEEE, 2003.

[13] Miles A. McQueen, Wayne F. Boyer, Deception used for Cyber Defense of Control Systems, IEEE, 2009.

[14] Henry C. Lee, Cyber Crime and Challenges for Crime Investigation in the Information, IEEE, 2008.

[15] Animesh bharti, legislative measures to deal with economic crimes in India, deputy secretary (crime monitoring), ministry of home affairs, government of India, 128th international training course participants' papers, resource material series no.67. available at http://www.unafei.or.jp/ english/pdf/RS_No67/No67_22PA_Bharti.pdf

[16] Atul Kamboj, Mukhdeep Singh, Cyber Terrorism: Terrorists go hi-tech, Egyptian Computer Science Journal, 29 (30), 2007.

[17] Cyber Crime In India : Cyber Stalking – Online Harassment, Available at http://www. Indianchild .com/ cyberstalking.htm.

[18] Harpreet Kaur, Cyber Stalking: Know It, Report It, Stop It!, Available at https://lawlex.org/lex-bulletin/cyber-stalking-know-it-report-it-stop-it/9555

[19] Sakshi Shrivastava, All You Need to Know About CyberStalking, Available at https://www.fuzia.com /article_detail /2052 /all-you-need-to-know-about-cyberstalking?tp=5

[20] Brett Pladna, The Lack of Attention in the Prevention of Cyber Crime and How to improve it, Available at http://www.infosecwriters.com/Papers/BPladna_Cybercrime.pdf

[21] Shrimati Das, Cyber Crime and Cyber Ethics: Staying Safe and Enabled in the Cyber Space , Quest: Multidisciplinary Journal of Humanities and Social Sciences, Volume 1 Issue 2: Article No. 1 Available at "http://www.sncwgs.ac.in/wp-content/uploads/2015/01/1-CYBER-CRIME-AND-CYBER-ETHICS.pdf