Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, July 2021: 5179-5185

Knowledge of Cyber Crime by Electronic Media

Naresh Kumar Maharjan

Ph. D, Faculty Member, Faculty of Management and Law
Nepal Open University, NEPAL

Abstract:
Crime is a social and economic phenomenon and is as old as the human society. As, life is about a mix of good and evil, so is the internet. For all the good it does to us, cyberspace has its dark sides too. The internet is undeniably open to exploitation. Known as cyber-crimes, these activities use of computers, the internet, cyberspace and the World Wide Web. Everybody is using computer. From while collar criminals to terrorist organizations and from teenagers to adults. All crimes performed or resorted to by abuse of electronic media or otherwise, with the purpose of influencing the functioning of computer or computer system. Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. Cyber-crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computes, cyber-crime has assumed rather sinister implications.
While the world-wide scenario on cyber-crime looks bleak, the situation in Nepal is not any better. Cyber-crimes in Nepal are slowly evolving from a simple e-mail crime to more serious crimes like hacking and source code theft. Cases of spam, hacking, cyber stalking and email fraud are rampant despite the enactment of the Electronic Transactions Act, 2063 B.S. (2008 A.D.) ETA and Banking Offence and Punishment Act, 2064 B.S. (2008 A.D.) the Nepal's Cyber Law and setting up of cyber-crimes cells in major cities. The Problem is that most cases remain unreported due to a lack of awareness.
So, in the present report an attempt has been made to describe the various types of cyber-crimes and the present scenario on the cyber-crime and the preventive measures that should be taken up to protect ourselves.
Keywords: Cyber-crime, Cyber media and law.

Introduction:

Long gone are the days when a computer took up an entire room. Now we have computers at home, laptops that travel just about anywhere, and the data networks that allow us to transmit information from virtually any location in a timely and efficient manner.

Computers and the internet can offer great benefits to society. However, they can also present opportunities for crime, much of it just traditional crime using new technology tools. Modern computer technology and the internet without question had and continue to have, a significant impact on our society and the way we nowadays conduct business. Advancements in these areas have revolutionized our access to information and the way we exchange different kinds of data. It changed the way we entertain ourselves during our leisure time and opened new ways for the consumers and the industry to conduct business on a global scale.

These advancements, however, come with the important responsibilities and expect us to significant risks. Criminals too, have recognized that computer technology, computer networks and in particular the Internet, provide new means for them to commit crime. This can be rather traditional forms of crime using none traditional means or entirely new, previously not possible forms.

Despite the growing level of interest in this field, there is still little known about the actual issues involved in securing networks and electronic assets. Many people consider anti-virus software used to defend against e-mail viruses to be the cure all for all varieties of information security threats. Viruses are a big problem, no doubt, potentially leading to huge losses in terms of lost productivity and corrupted intellectual assets. However, cyber-

crime can be much more than the release of an e-mail attachment that proclaims to all friends and business associates of unsuspecting victims.

The true damage of cyber-crime is of far greater consequence. Individuals with technical knowledge of networking and networking devices can steal sensitive information or money or conduct a host of juvenile pranks. Today the internet is connected to nearly 200 countries. The very nature of globally connected networks has made it painfully clear that cyber-criminal activity cannot be effectively addressed by individual nations or even a group of industrialized countries, whether it requires a concerted effort between industry, government officials, law enforcement and citizens of all countries.

Things can go wrong in cyberspace. There's fraud, stalking, viruses, outright theft, and more. And while he online world is still not nearly as dangerous as the physical realm, it pays to take precautions against victimization.

The Oxford Reference Online defines cyber-crime as committed over the internet. The Encyclopedia Britannica defines Cyber-crimes that is committed by means of special knowledge or expert use of computer technology. So, what exactly the Cyber Crime? Cyber-crime could reasonably include a wide variety of criminal offences and activities.

The Internet or cyber space as its sometimes called is a borderless environment unlike a brick-and-mortar world. Even through it is indispensable as a knowledge bank it is an ideal tool for someone with criminal bent of mind, who can use this environment to maximum advantage.

Cyber-crime manifest itself as pornography on the web, online harassment and stalking, e-mail security violation, data security violation, virus implantations, fraud, unauthorized credit card access, and more.

The world cyber and its relative dot.com are probably the most commonly used terminologies if the modern era. In the information age the rapid development of computers, telecommunications and other technologies had led to the evolution of new forms of trans-national crimes known as cybercrimes. Cyber-crimes have a virtually no boundaries and may affect every country in the world. They may be defined as any crime with the help of computer and telecommunication technology, with the purpose if the influencing the functioning of compute or the computer systems. The extent of loss involved worldwide of cyber-crimes is tremendous as it is estimate that about 500 million people who use internet can affected by the emergence of cyber-crimes. Cyber-crimes are a very serious threat for the times to come pose one of the most difficult challenges before the law enforcement machinery. Most cyber-crimes do not involve violence but rather greed, pride, or pay on some character weakness of the victims. It is difficult to identify the culprit, as the net can be a vicious web of deceit and can be accessed from any part of the globe. For these reasons, cyber-crimes are considered as White Color Crimes.

In really, computer crime victimizes us all, wrote Buck Bloom Becker in his book, spectacular Computer crimes. Everyone has a risk to some degree. If it isn't gangster with guns making us afraid to set off the door. Its criminals with key boards making us worry of flipping the power switch on our PCs.

Classification and Types of Cyber Crimes:

Against Individuals

1. Harassment via e-mails.
2. Cyber – stalking
3. Dissemination of obscene material.
4. Defamation.
5. Unauthorized control over computer systems.
6. Indecent exposure
7. Emil spoofing
8. Cheating and fraud.

Against Individual Property

1. Computer vandalism.
2. Transmitting viruses.

3. Unauthorized control over computer system
4. Intellectual Property crimes.
5. Internet time thefts.

Against Organization

1. Unauthorized control over computer system
2. Distribution of pirated software.
3. Possession of unauthorized information.
4. Cyber terrorism against the government organization

Against Society at large

1. Pornography
2. Polluting the youth through indecent exposure
3. Trafficking
4. Financial crimes
5. Sale of illegal articles
6. Online gambling
7. Forgery

Objectives of Study

1. To study the awareness level of respondents through a demographic profile
2. To study the factor that motivate person for crime and their effect on society.
3. To study how respondent react towards the cyber-crime.
4. To review the extent of coverage of cyber-crime awareness on mass media.
5. To study effective mass media tool to disseminate cyber-crime awareness
6. Opinion of respondent regarding the cyber-crime awareness message

Research Methodology

This study has been designed, keeping in mind the methodology being followed the world over in researches. This procedure as known as Triangulation method. Triangulation has been defined as the use of two or more methods of data collection in the study of some aspect human behaviour, in the recent years it has been felt that anyone method of data collection is insufficient. As Carley 1981 has pointed out, neither type of research, when used alone can give us an accurate window to the world. They are best developed when used in conjunction. While quantitative research hel[s to understand the specifies.

Fielding and fielding 1986 suggested there are possible points of convergence in different approaches. It has now become more acceptable in recent years to combine quantitative and qualitative research and the process is triangulation of data to substantiate the hypothesis.
It is an attempt to determine why media analysis is an important area of research and highlights two key elements, namely.

1. Qualitative and quantitative analysis should be conducted of media content to identify and understand the likely impact and effects of the content on audiences the goal of content on audiences the goal of content analysis which quantitative analysis alone cannot reveal.

2. International Best Practice methodology and techniques in research should be followed for analysis to be valid, reliable and replicable key factor in research. In modern democratic societies, the media reflect views, opinions and perceptions and influence views, opinions and perceptions.

3. Both primary and secondary data were collected. Secondary date was collected. Secondary data was collected from different magazines, newspapers, and internet. The primary data was collected through questionnaire survey method which was conducted in Kathmandu valley.
   The primary data is collected through questionnaire survey method. For this purpose, 100 respondents were randomly selected, an attempt was made to check their attitude towards uses pattern of credit card and their

level of satisfaction. Certain attributed were rated on five scales and the final score has been calculated by using weighted tanking method. The data thus received was tabulated; analyzed and appropriate result was drawn. Univariate and bivariate data analysis techniques were used to analyze the data.

4. The secondary data was collected from various books, research articles, journals, of various universities. Cyber-crime cell of Kathmandu, the ICFAI university journal cyber law and by the different magazines.

5. In the first method, a time series content analysis was conducted on the Cyber-crime awareness related messages that appear in the print and electronic media in Nepal, taking a sample of Nepal Telecom, N-cell, Smart-cell and 5 newspapers the cybercrime awareness related messages appearing in them were studies during the time period of one year.

Limitations of the Study

1. In spite of making all my efforts to make the dissertation a perfect one there are certain limitations in the study, which are felt while writing the report. As the study is an exploratory one designed to find new hypothesis, readers are not suggested to conclude the result. The study suffers from the basic, limitations of the possibilities of difference between what is recorded and what is true.
2. The sample size is less and therefore the test that could be done on large population cannot be done.
3. There has lack of time and financial resources prevented the investigator from carrying out an in-depth study.
4. The findings of the survey are based on the subjective opinion of the respondent and there is no way of assessing the truth of the statements.
5. It was difficult to collect information due to the resistance of some of respondents.
6. Language barrier amongst the enumerations and the target group.

Tools for Analysis

For analyzing the data, we used three for different types of tests for the conclusion of the study.
1. Shi square test.
2. Percentage method
3. Mean test
4. Kolmogorov-Smirnov test.

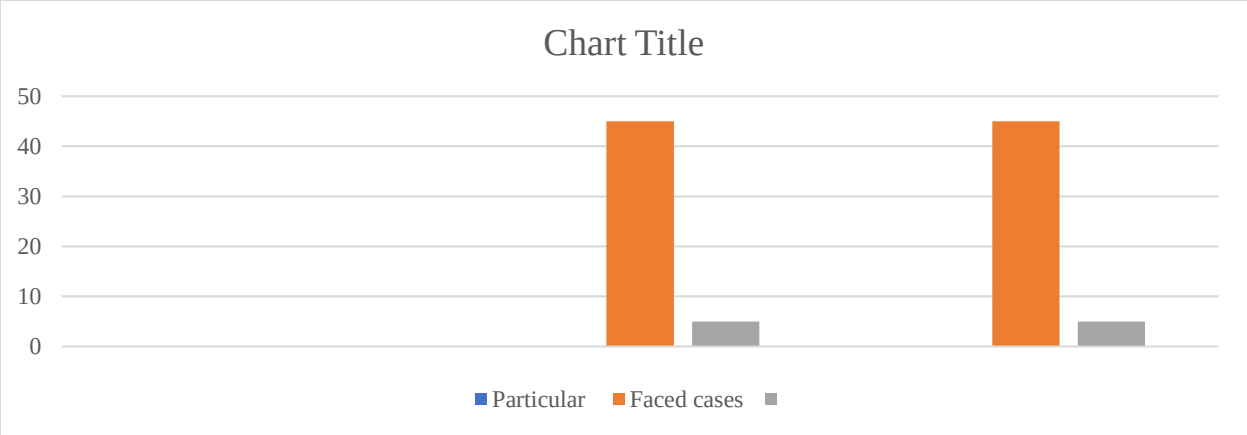
Analysis and Interpretation

Relationship between demographic feature and awareness level.

Table No. 1

Factor	Chi Square test	Chi Square table value	Significant and no significant
Profession	5.6	11.07	Not significant
Nature of work	0.32	5.991	Not significant
Qualification	4.32	7.815	Not significant

By applying chi square test, it has concluded that all the factors are not significant that means all the factors reject the null hypothesis that means Demographic feature affect the awareness level of respondent.

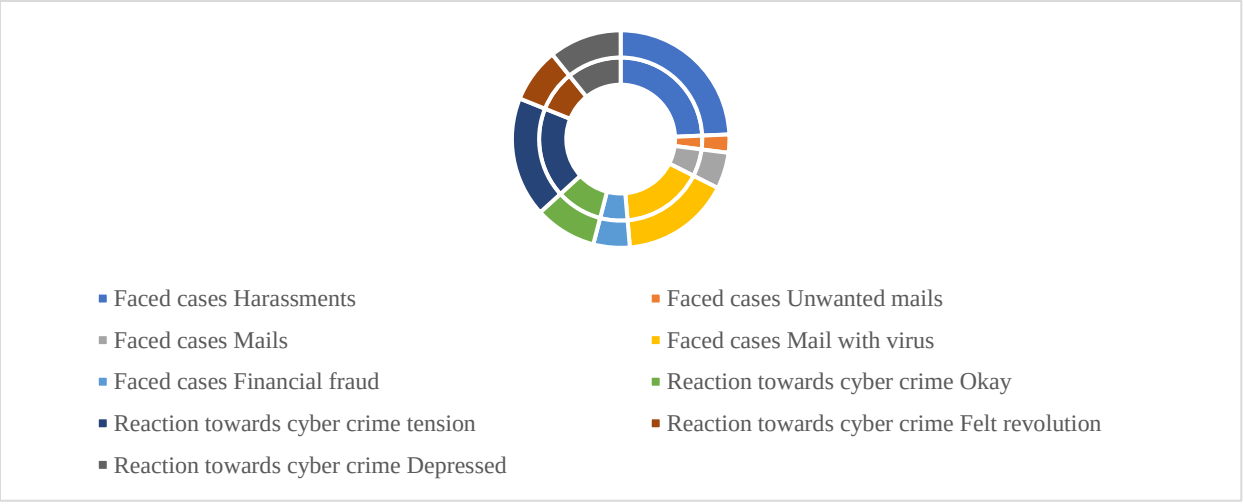


Percentage Method

Motivating the factor for crime and behavior or common people against it.

Cyber Crimes Table No. 2

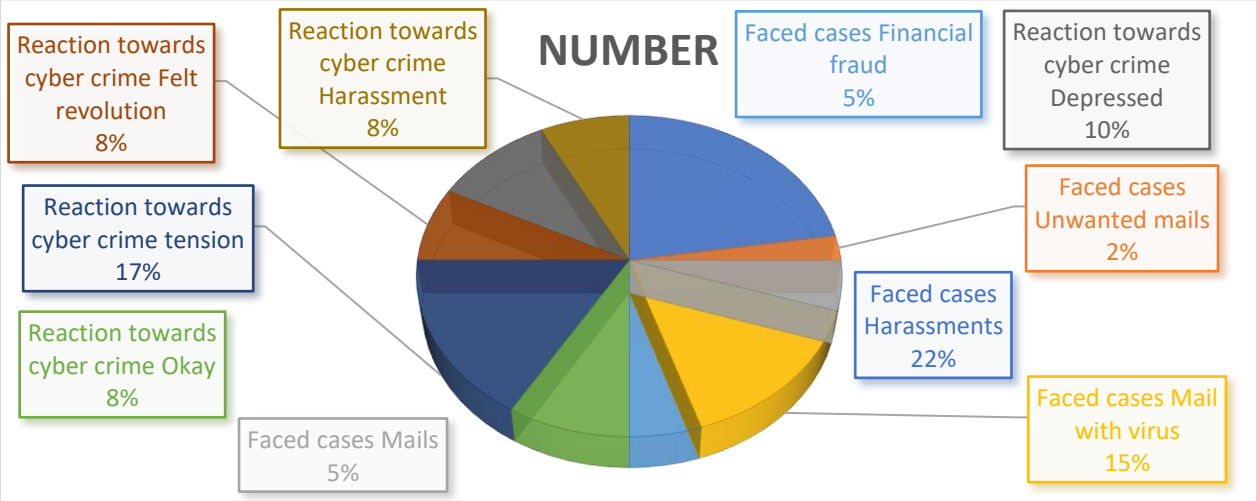
Particular	Classification	Number	Percentage
cases	Cyber stalking	40	40
	Obscene emails	5	5
	hacking passwords	15	15
	MMs	40	40
Motivating factors	Sexual harassment	38	38
	Obsession for love	5	5
	Revenge/hate	22	22
	Ego	15	15
	Just for fun	20	20



General People Table No. 2

Particular	Classification	Number	Percentage
Faced cases	Harassments	45	45
	Unwanted mails	5	5
	Mails	10	10
	Mail with virus	30	30

	Financial fraud	10	10
Reaction towards cyber crime	Okay	17	17
	tension	33	33
	Felt revolution	15	15
	Depressed	20	20
	Harassment	15	15

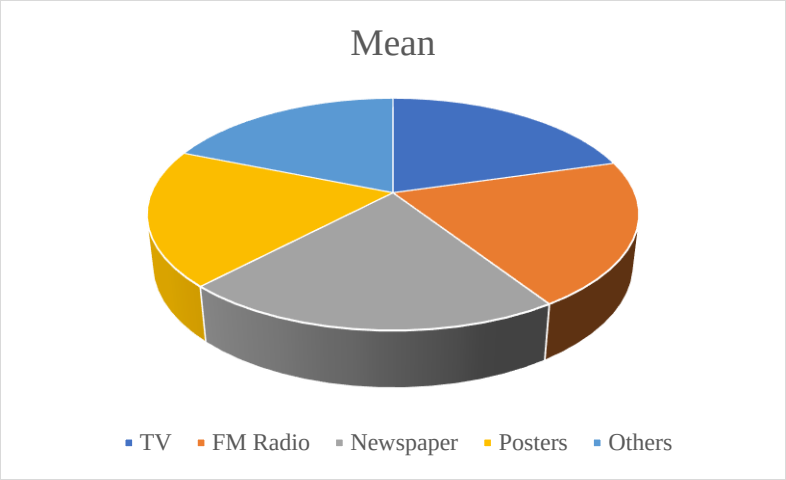


With the help of this method, it concluded that love and hate become a reason for the person for committing a cyber crime and MMS is the main offence of cybercrime and general people more affected by the attacks on mails because they are very much addicted to internet without having a knowledge about the use of internet and due to cyber crime cases affected person faces the problem of tension and sometimes it become a reason for their depression.

Mass Media Profile

Mean Test Table No. 3

Media	Mean	Ranking
TV	3.03	1
FM Radio	2.99	3
Newspaper	3.14	2
Posters	2.81	4
Others	2.78	5



It was fond that newspaper expose cyber crime awareness messages at large frequency and provide complete detail time on the cyber-crime awareness message.

Viewership Table No. 4

Media	Mean	Ranking
TV	3.38	1
FM Radio	3.2	2
Newspaper	3.02	3
Posters	2.85	4
Others	2.08	5

According to this it concludes that Television reach to more people because of their representation style, no doubt newspaper exposes very well about cybercrime awareness message but does not targets society at large because in Nepalese people are not educate and they illiterate.

Findings & Suggestions

1. As per the popular notion that electronic media are more popular amongst the modern generation. The study revealed that impact of newspapers. So, there should be more bombardment of crispy designed messages on newspapers.
2. More stress should be given to other aspects of cyber crime awareness
3. The designing of the print messages should be done in such a way that the message crisp and interesting.
4. The messages related to cyber-crime awareness should be delivered more frequently.

References

1. Cuellar M. et.al.2001 the traditional dimension of cyber crime and terrorism. Abraham D. Seymour E. Goodman Eds. PaloAlto, CA: Leland Stan-ford Junior University.
2. Hugh, S. A 2006Computer and Intellectual property crime: Federal and State law. Arlington, VA BNA Books
3. Levy, s1984 Hackers Heroes of the computer revolution.
4. Girisha, R. J 2015 Cyberlaw: National and International Perspectives. Upper Saddle River, NJ: Prentice Hall.
5. National academy of Engineering 1985 Information technologies and social transformations Washington DC National academy of Printing Press.
6. Crimes in cyber space – VD Dudeja.
7. Encyclopedia of Cyber crime
8. Raymond ES the new hacker's dictionary. Cambridge MA: MIT Press.
9. Central Investigation Bureau (CIB), Kathmandu
10. Cyber Bureau, Cyber Crime Investigation Cell, Kathmandu.