Perception About Cyber Crimes Among Students in Arts and Science Colleges in Chennai

S. Subbulakshmi, V. Jayanthi, T. Devi Kamatchi

Abstract— The internet helps us in providing information as well as storing all our data, with the rapid increase in our modern technology; it has become very difficult to keep our private information safe. The Internet has also bred a new kind of crime CYBER-CRIME. The other name for Cyber crimes are "Internet Games" and "yahoo yahoo". Common internet users are unaware of Cyber crimes like hacking, identity theft, Credit/debit card frauds, cyber terrorism and many more crimes. This paper attempts to draw out the awareness level of students about cyber crime.

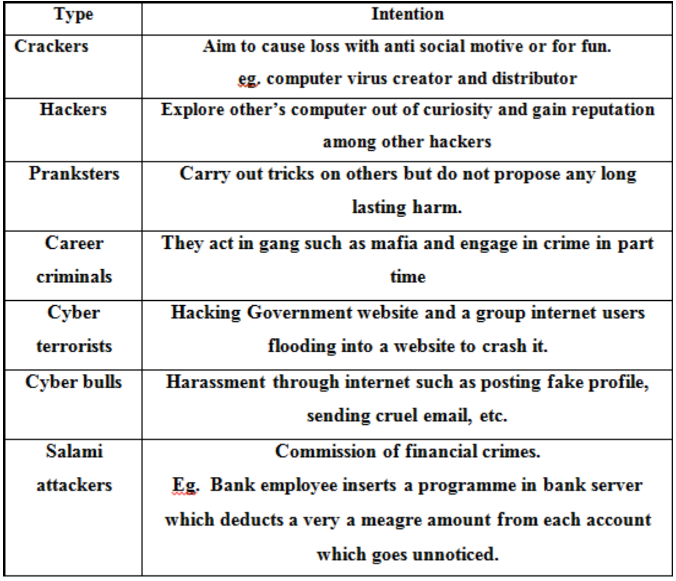
Keywords: Cyber Crime – types of cyber crimes – problems faced by the victim - awareness

I. INTRODUCTION

Cyber crime is a crime in which a computer is the object or a tool to commit crime or an offense. Cyber criminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes.. Cyber criminals like **Crackers, Hackers**, **and Pranksters, Career criminals, Cyber terrorists & Salami attackers** use platforms such as social networking sites, emails, chat rooms, pirated software, websites, etc., to attack victims. Common types of cyber crime include **online bank information theft, identity theft, online predatory crimes cyber terrorism and unauthorized computer access.**

At present, Out of the top 10 most targeted countries by cyber attackers, **India ranks fourth**. Cyber-attacks are an illegal activity and are continuously increasing in India for financial loot.The majority of cyber-crimes are centred on forgery, fraud and phishing. **India is the third most targeted country for phishing attack after the US and the UK.**

Table No.1
Types of Cyber Criminals



Type	Intention
Crackers	Aim to cause loss with anti social motive or for fun. eg. computer virus creator and distributor
Hackers	Explore other's computer out of curiosity and gain reputation among other hackers
Pranksters	Carry out tricks on others but do not propose any long lasting harm.
Career criminals	They act in gang such as mafia and engage in crime in part time
Cyber terrorists	Hacking Government website and a group internet users flooding into a website to crash it.
Cyber bulls	Harassment through internet such as posting fake profile, sending cruel email, etc.
Salami attackers	Commission of financial crimes. Eg. Bank employee inserts a programme in bank server which deducts a very a meagre amount from each account which goes unnoticed.

Table No.2
Types of Cyber Crimes

Type	Intention
Data crime	**Data collection, data modification and data theft.**
Network crime	**Network Interference and network sabotage**
Access crime	**Unauthorised access and virus dissemination**
Relative Crime	**Abetting cyber crime, computer related crime and content related crime.**

II. SCOPE OF THE STUDY

- ❖ To discover the awareness level as regards to cybercrime among students in Colleges in Chennai.
- ❖ To find the relationship between the misuse of internet and cybercrime.

Revised Manuscript Received on September 10, 2019.

Dr. S. Subbulakshmi, Associate Professor & Head, PG Dept of Commerce, SDNB Vaishnav College, Chennai, Tamil Nadu, India
(Email:subbupetchi72@gmail.com)

Dr. V. Jayanthi, Assistant Professor, Department of Business Administration, Vels Institute of Science, technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India.
(Email :jayanthiii.murali@gmail.com)

Dr. T. Devi Kamatchi, Assistant Professor, Department of Commerce, A.M. Jain College, Meenambakkam, Chennai, Tamil Nadu, India.
(Email: iyaneshkamatchi@gmail.com)

III. OBJECTIVES OF THE STUDY

❖ To study and understand about the psychological problems faced by college students with regard to cybercrimes in Chennai.

❖ To identify the factors which create awareness about cyber crime on the performance of students in colleges in Chennai

❖ To provide suitable suggestions based on the findings of the study.

IV. RESEARCH METHODOLOGY

Research design:

Descriptive analysis.

Sample area & sample size colleges in chennai & 150

Sample design:

"convenient sample".

V. SOURCES OF DATA

Primary data:

Well structured questionnaire was used to collect data from the college students.

Secondary data:

Secondary data was collected from internet, journals, magazines, government bulletins etc.

Reliability Analysis :

This study satisfies Cronbach's Alpha acceptable range 0.7 and above. The reliability co-efficient for the items are 0.893**.** Hence the researcher proceeded with the structured questionnaire.

VI. LIMITATIONS OF THE STUDY

1. The study is confined to a specific period and hence the sample size is 150
2. The data collection is primary and the hence there may be personal bias
3. The survey is conducted only in Chennai hence, the results from the study may or may not be applied to other areas
4. Interpretation of the study is based on the assumption that the respondents have given correct information.

VII. REVIEW OF LITERATURE

- **Monalisa Hati** - analysed the awareness level and suggested some preventive measures to overcome the cyber crime. This paper observed and tinted the computer related crimes which affects a nation at large and also suggested that the importance of creating wakefulness to overcome such threat. **International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 5, Issue 7, July 2016 & Monalisa Hati (2016).**
- **HemrajSaini, Yerra Shankar Rao, T.C.Panda (2012)-** The researchers' tried to figure out the impact of cyber crimes on the society. They found out that the serious impact over the society is in the form of economical disrupt, psychological disorder, threat to National defense etc., **International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209 HemrajSaini, Yerra Shankar Rao, T.C.Panda (2012)**
- **Md Shamimul Hasan et al.-** The aim of this study is to protect the students by creating awareness and to provide some empirical evidences to the policy makers in combating cybercrime. This paper also helps to protect the young generation by reducing the high risk of becoming a victim on their activities. ***Journal of Social Science*** **Volume 11, Issue 4 Pages 395-404 Md Shamimul Hasan et al. (2015).**

VIII. ANALYSIS AND INTERPRETATION & RESULTS

Data analysis and interpretation is the process of assigning meaning to the collected information and determining the conclusions, significance and implications of the findings. The collected data have been analyzed with the help of statistical techniques to understand the outcomes with reference to objectives and hypothesis. Data processing was carried out with the help of MS Excel and SPSS 18. The analytical tools applied for the study are,

✓ Percentage analysis

✓ Regression Analysis

✓ Path Analysis

GENERAL FINDINGS

PERCENTAGE ANALYSIS

❖ Majority of respondents, ie.,6 3% were female.

❖ 65% are at the age group of 18-25 years.

❖ 53% are graduates.

❖ 96% have accessed the internet.

❖ 74% have accessed the computer at home.

❖ 58% ready to spend 1-2 hours on browsing.

❖ Nearly, 58% use the computer for downloading.

Specific Findings

REGRESSION ANALYSIS

RELATIONSHIP BETWEEN AWARENESS LEVEL AND MEANS OF CYBERCRIME

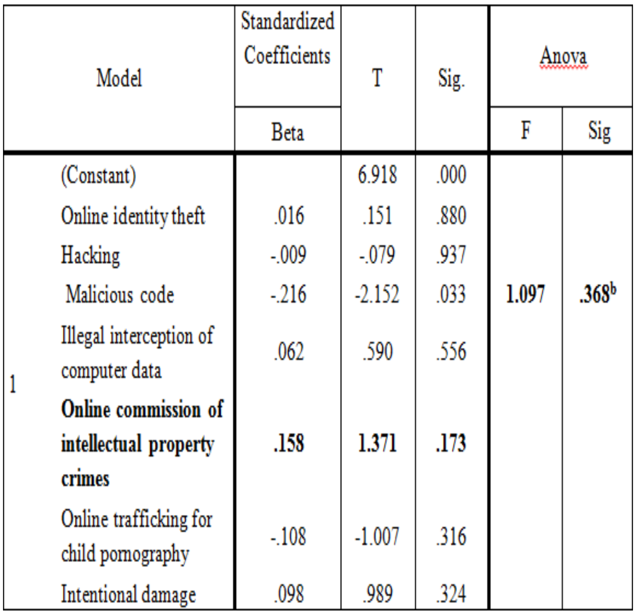
H0 –

Means of Cyber crime do not influence the Awareness level on cyber crime.

H1 –

Means of Cyber crime influences the Awareness level on cyber crime.

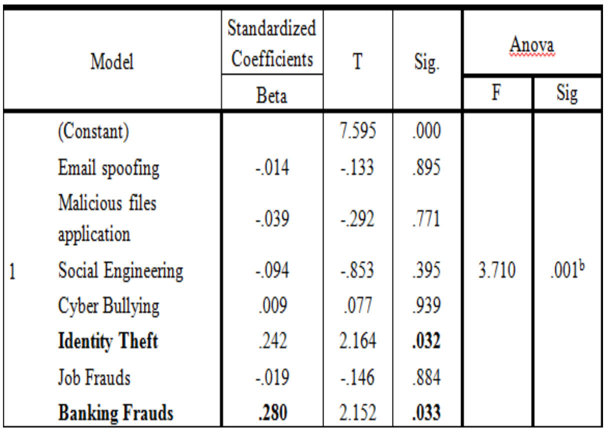
Table No.3



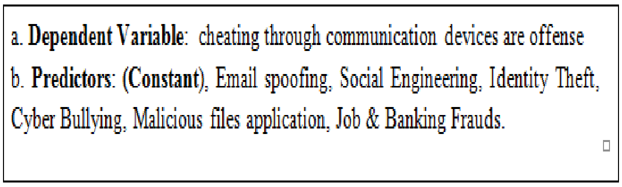
	Model	Standardized Coefficients	T	Sig.	Anova	
		Beta			F	Sig
1	(Constant)		6.918	.000	1.097	.368b
	Online identity theft	.016	.151	.880		
	Hacking	-.009	-.079	.937		
	Malicious code	-.216	-2.152	.033		
	Illegal interception of computer data	.062	.590	.556		
	Online commission of intellectual property crimes	**.158**	**1.371**	**.173**		
	Online trafficking for child pornography	-.108	-1.007	.316		
	Intentional damage	.098	.989	.324		

RELATIONSHIP BETWEEN CHEATING THROUGH COMMON DEVICES

Table No.4



	Model	Standardized Coefficients	T	Sig.	Anova	
		Beta			F	Sig
1	(Constant)		7.595	.000	3.710	.001b
	Email spoofing	-.014	-.133	.895		
	Malicious files application	-.039	-.292	.771		
	Social Engineering	-.094	-.853	.395		
	Cyber Bullying	.009	.077	.939		
	Identity Theft	.242	2.164	**.032**		
	Job Frauds	-.019	-.146	.884		
	Banking Frauds	**.280**	2.152	**.033**		



a. **Dependent Variable**: cheating through communication devices are offense

b. **Predictors**: **(Constant)**, Email spoofing, Social Engineering, Identity Theft, Cyber Bullying, Malicious files application, Job & Banking Frauds.

INFERENCE:

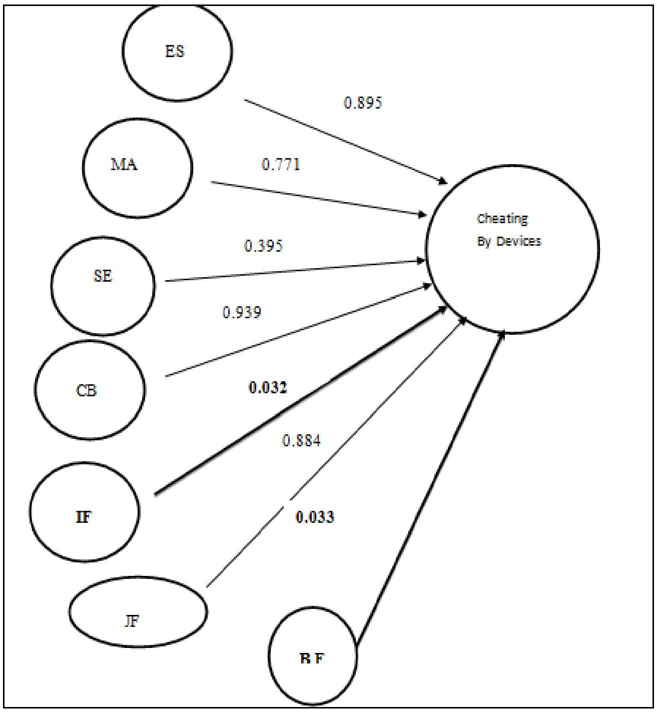
All the above crimes are punishable and have its significance on identity theft and banking frauds. The result highlighted that the **banking frauds** is an important variable which influence the person to commit crimes. The result also highlighted that the banking frauds has the largest beta value **(i.e.,) .280**

PATH ANALYSIS

Path analysis involves the analysis and comparison of two models – a full model with all the possible paths included and reduced model which has some of the parts deleted because they are hypothesized not to contribute to the model.

1) Full path analysis
2) Reduced (or) hypothesized path analysis

FULL PATH ANALYSIS



ABBREVATIONS:

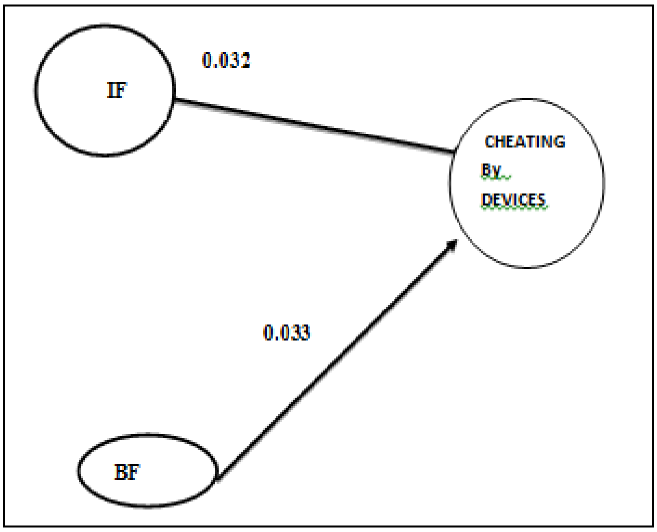
ES – Email Spoofing: MA – Malicious files application: SE – Social Engineering

CB – Cyber Bullying: IF – Identity Frauds: JF – Job frauds & BF – Banking frauds

The path co-efficient have derived from the series of multiple regression analysis. **Lined arrows** are showing the **direct contribution** to have impact on student's awareness about cyber-crime. Path co-efficient are significant values from the multiple regression analysis. The result of the model is explained below:

REDUCED (OR) HYPOTHESIZED PATH ANALYSIS

The reduced (or) hypothesized model after concealing insight lines is depicted in the underneath diagram.



INTERPRETATION:

All the independent variables do not have any impact except the banking frauds and identity frauds.

IX. SUGGESTIONS

- The reviewed social studies curriculum can reflect internet crimes as an emerging social problem and issue.
- The government may begin a radical sensitization of college students as to the ills and dangers inherent in involvement in internet crime.
- The government may build computer –training centers in colleges to increase the student's computer literacy standard.

X. CONCLUSION

This paper highlighted and concluded that with the National harmonizing efforts, co-ordination and co-operation among various Government and Non Government Organizations NGO'S) are required to put their efforts and to take action towards the cyber-crimes. The Government has to take steps to educate people especially youth to create awareness about cyber crimes. This paper also suggested that the cyber laws has to be modified which suits to the changing needs and to make tighter judicial system to diminish the crimes.

XI. REFERENCES

JOURNALS

1. RS, S.R. and Preethisri, T.J., 2018. AWARENESS OF CYBER CRIME AMONG COLLEGE STUDENTS-AN ANALYTICAL STUDY. *INTERNATIONAL JOURNAL OF MANAGEMENT AND SOCIAL SCIENCES (IJMSS)*, *8*(1.3), pp.91-93.
2. Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, Visited: 28/01/2012.
3. CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html, Visited: 28/01/2012.