Indian Journal of Science and Technology, *Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/100189, August 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Influence of Educational Qualification on Different Types of Cyber Crime: A Statistical Interpretation

Yerra Shankar Rao[1*], Aswin Kumar Rauta[2], Hemraj Saini[3] and Tarini Charana Panda[4]

[1]Department of Mathematics, GIET Ghangapatana, Bhubaneswar - 752054, Odisha, India; sankar.math1@gmail.com
[2]Department of Mathematics, S.K.C.G. College, Paralakhemundi, Gagapati - 761200, Odisha, India; aswani.kumar@gmail.com
[3]Department of CSE, Jaypee University of Information Technology, Waknaghat, Solan - 173234, Himachal Pradesh, India; hemraj1977@yahoo.co.in
[4]Department of Mathematics, Revenshaw University, Cuttack - 753003, Odisha, India; tc_panda@yahoo.co.in

Abstract

Objectives: In this paper, the impact of educational qualification (general education) on different types of cyber crime activities has investigated. **Methods/Statistical Analysis**: A cross sectional survey using Questionnaires method was conducted among 2000 different types of persons working in different fields having different qualification having age more than 18 years. But a sample of 180 students is considered for the better interpretation of data. The collected data is interpreted statistically using one-way ANOVA.**Findings:** The influence of general education on four types of cyber crimes viz. financial misappropriation, extramarital affairs, misleading for job and crime in academic/research have been investigated. Results suggest no significant influence of different qualification on cyber crime. The finding shows that the involvements in cyber crime of qualified persons have negative effect on the value of education which leads to a bad impact in the development of the society.**Application/Improvements:** The proposed analysis is helpful to build the society with proper understanding about the cyber-attacks in various domains.

Keywords:ANOVA, Cyber Crime, Impact of Cyber Crimes, Statistical Analysis, Types of Cyber Crime

Nomenclature

- $\alpha \rightarrow$ Crime due to financial misappropriation
- $\beta \rightarrow$ Crime due to extramarital affairs
- $\gamma \rightarrow$ Crime due to misleading for job
- $\delta \rightarrow$ Crime in academic/research
- $A \rightarrow$ Matriculation
- $B \rightarrow$ Intermediate.
- $C \rightarrow$ Graduate.
- $D \rightarrow$ Post Graduate.
- $A_\alpha \rightarrow$ Matriculation qualified committing the crime due to financial misappropriation.
- $A_\beta \rightarrow$ Matriculation qualified committing the crime due to extramarital affairs.
- $A_\gamma \rightarrow$ Matriculation qualified committing the crime due to misleading for job.
- $A_\delta \rightarrow$ Matriculation qualified committing crime in academic/research.
- $B_\alpha \rightarrow$ Intermediate qualified committing the crime due to financial misappropriation.
- $B_\beta \rightarrow$ Intermediate qualified committing the crime due to extramarital affairs.
- $B_\gamma \rightarrow$ Intermediate qualified committing the crime due to misleading for job.
- $B_\delta \rightarrow$ Intermediate qualified committing the crime in academic/research.
- $C_\alpha \rightarrow$ Graduate qualified committing the crime due to financial misappropriation.
- $C_\beta \rightarrow$ Graduate qualified committing the crime due to extramarital affairs.
- $C_\gamma \rightarrow$ Graduate qualified committing the crime due to misleading for job.
- $C_\delta \rightarrow$ Graduate qualified committing the crime in academic and research.

**Author for correspondence*

$D_\alpha \rightarrow$ Post Graduate qualified committing the crime due to financial misappropriation.

$D_\beta \rightarrow$ Post Graduate qualified committing the crime due to extramarital affairs.

$D_\gamma \rightarrow$ Post Graduate qualified committing the crime due to misleading for job.

$D_\delta \rightarrow$ Post Graduate qualified committing the crime in academic/research.

V_r : Variation between treatments.

V_e : Variation within treatments.

V_t : Total variation.

1. Introduction

The rapid globalization of the world is due to the internet networking. The technological advancement of a country depends on its online system. Online services provide extensive individual, social, and economic benefits for modern society. In the today's digital world, the use of computer and internet in every sector such as business, office, education, social networking, employment and financial transaction etc. is inevitable. The internet has made PC an essential segment in national improvement. But the growing online system also provides ground for malicious behavior. Utilizing the characteristics of the Internet, such as scalability, anonymity and global reach, cybercrime emerged as a new form of crime. Cybercrimes as offenses that are executed against individuals or social events of individuals with a criminal reason to purposely hurt the reputation of the loss or cause physical or mental naughtiness to the setback clearly or roundaboutly, using bleeding edge telecom frameworks, for instance, Internet (Chat rooms, messages, notice sheets and get-togethers etc.) and cell phones (SMS/MMS etc.). However, cybercrime is an undeniable danger, just a minority of customers are specifically deceived. Significantly more are made mindful of the danger, and numerous individuals stay reluctant to take part online because of the apparent danger of cybercrime. Purchaser situated cybercrime, which incorporates data fraud, Visa extortion, and phishing, expands the danger of utilizing online administrations for all Internet clients[1,2]. The budgetary effect of cybercrime on e-business and business when all is said in done has heightened drastically as of late, obviously the quickest developing kind of wrongdoing. Organizations everywhere throughout the world are upset, lose touchy data, and experience profitability decreases as a consequence of cybercrime[3]. Recently the crime in research / academic areas have appeared due to plagiarism and unauthorized downloading of important documents/ books etc. Though the laws like intellectual property right, copy right act have made by the government but still it persists. As each institution possesses a unique culture, has different systems of administration, policies and is of dissimilar types, so it is significant to be acquainted with if the type of educational qualification determines people concern in cybercrime activities. Again the recent problem throughout the globe is providing job to all. The unemployment problem is an opportunity for the cyber criminals to deceive the people by giving false advertisement to provide job. Another major problem is the use of social sites like Facebook, Whatsapp, Twitter, Matrimonial sites etc. to make unreal relationship and then establishing the extramarital affairs and finally harassing the people. Almost all the cyber crimes are done by the educated persons. Hence the numerous techniques used by cyber criminals have been recognized as, stalking, spamming, embezzlement, spoofing, hacking, cyber pornography and sniffing etc. The computer related harassment is defined as the state where a personage uses a computer or computer network to converse indecent language, or make any submission of that nature, or threaten any illegal or wicked act. Administrators are frequently used to tempt unsuspecting public. Phishing is typically carried out by email spoofing, or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one[4–6]. Another form of cybercrime is stalking. Stalking occurs when one person repetitively intrudes on another to such a degree that the recipient fears for his or her security. This involves any shape of annoyance or threatening of a human being, whether bodily or through the use of electronics (unwanted phone calls, SMS/MMS). For all intents and purposes, any undesirable contact between two people that specifically or in a roundabout way impart a danger or spot the sufferer in apprehension can be considered stalking. A few stalkers build up an interest for someone else with whom they have no individual affiliation. At the point when the casualty does not react as the stalker trusts, the stalker may attempt to constrain the casualty to obey by utilization of dangers and terrorizing. Whenever dangers and terrorizing fall flat, a few stalkers go round to savagery. Stalking happens if PC wrongdoing and those people who participate in this freak conduct have turned into a piece of our computerized society[7,8]. While the accurate harm brought about

by PC culprits is open for civil argument, their presence and expansion in numbers is unchallenged. The criminal component in our general public has a tendency to be the early adopters of innovation as it regularly helps them to wind up better at their criminal tradecraft.

Hence we have considered the effect of different qualification on different types of cyber crimes. In this paper, we focus on the relationship between general qualification and cybercrime in India. This allows us to quantify the impact of cybercrime in a statistically robust manner. Questionnaires were used for data gathering. A sample of 180 persons was careworn from a population of 2000 people working in different field in the state of Odisha, India. The instrument contains 16 items with 4-point scale of Most-times, now and again, rarely and never. We then create explanatory variables in four groups. The first group has qualification as matriculation, the second group has qualification as intermediate, the third group has qualification as graduation and finally, the fourth group has qualification as post-graduation. But all groups are considered as to commit the four types of cyber crimes viz. crime due to financial misappropriation, crime due to extramarital affairs, crime due to misleading for job and crime in academic/research areas.

We have interviewed the officers, executive assistants, clerk cadre, cashiers, typist cadre, typists, technicians and stenographers, messenger, drivers, cleaners, stewards and security guards, temporary staff or general public etc. working in different sectors(Health Sector, Education Sector, Banking Sector,Business etc.) having different educational qualifications involving in different types of cyber crime activities .We have described the key research questions and how we selected relevant questions from the survey for use in our model.

2. Literature Review

Cyber crime has become a major problem in recent years across the globe. Many investigations have been done by number of researchers in this regard, but the list of all such is not possible to present here.So some of them which is relevant to our topic are presented here. In[8] has analyzed the effect of debit card usage by newspaper articles on card fraud.In[2] have demonstrated the consumer's reaction on cybercrime. In[1] have studied the involvement of students on cybercrime activities in tertiary institutions in Enugu state of Nigeria. Deloitte[5] has presented the Indian banking fraud survey. In[8] has illustrated the influence of age on the cyber crime. In[9] have investigated the cyber crime activities due to sex and lies. In[10] have studied the fear of crime in online in Zaria-Kaduna state of Nigeria. In[11] have examined the impact of social media characteristics on customer. In[12] have explained the factors affecting social network service use. [13] has investigated the pornography on the internet and an evaluation of moral panic. In[14,15] have investigated the self-reported computer criminal behavior. In[16] have studied the case of social learning theory and digital piracy. In [21] has studied the influence of the cyber-social environment on fear of victimization. In[13] have analyzed the impact of consumer and product characteristics on e-commerce adoption in India. In[22] has explained the effect of internet crime on development. In[23] has demonstrated the fear of cyber crime among college students in the United States. In[24] has shown the impact of fraud and fraudulent practices on the performance of banks in Nigeria. In[25] has investigated the hacking and harassment for online victimization. In[26] has presented a comparative study on digital piracy justification: Asian students versus American students.

The literature survey indicates that several researchers have investigated the cyber crime activities by considering several factors, but so far author's knowledge, the influence of general educational qualification on cyber crime has not been studied. Therefore, an attempt has been made to assess the educational qualification of people's involvement in cyber criminal activities. The education system in India comprises of matriculation (10th standard), intermediate (+2), undergraduate, and post graduate. Generally, an individual required to be admitted into a college or university to pursue higher education after passing the 10th standard education. It is the most particular form of education where an individual takes a specific course of study. On completion of the course; the individual obtained an academic degree, diploma or certificate that will assist such an individual to get a job. The noticeable gap between what is learnt in school/college/university and the reality of the work place has been largely accredited to poor learning condition. The breakdown in the superiority of education, has led peoples to strange behaviors and the reason why students fit into place themselves in cybercrimes. Cybercrime refers to any form of crime committed by any individual during the use of a computer and network. The field of mental wrongdoing scene examination has been utilized with customary criminal examinations as a part of request to help agents in narrowing down the quantity of potential suspects, leading

legitimate suspect meetings, and managing suspects in a trial/court setting. Several specialists have endeavored to develop mental wrongdoing scene investigation into the computerized/electronic space with blended results. The constrained studies on specific subsets of PC crooks, for example, infection authors, has given some bearing in regards to the identity qualities to incorporate into prescient and danger models gives a structure to utilizing striking case focuses and a simple criminal scientific classification in light of the essential segments of aptitude and inspiration, keeping in mind the end goal to help agents managing computerized wrongdoing scenes.

2.1 Significance of the Study

This study consists of the job holder as well as general public having at least matriculation qualification and having age more than 18 years. These people have formal academic education but not having ethical education, law and security qualification. So this study will help policy makers of the Govt. to formulate the programs of value education in the curriculum. This also will helpful to the institutions and students to understand the consequence of engaging in cyber crime.So institutions would also design the academic activities to impart good moral to the students.

3. Methodology

The study was conducted with a population size of 2000 persons of different categories like students, teachers, officers, executive assistants, clerk cadre, cashiers, typist cadre, technicians, stenographers, messenger, drivers, cleaners, stewards, security guards, temporary staff and general public having the educational qualifications at least Matriculation working in different sectors including health sector, educational sector, banking sector, business or private firm etc. across state of Odisha, India to investigate the impact of general qualification on the cyber crime activities. The instrument for data collection was a 16–item questionnaire with 4-opinion response of Mostly (M), Sometimes(S), Rarely (R) and Never (N). A sample of 180 persons was considered for the data analysis.Mean and Variance of the data have calculated to analyze the ANOVA table. The one-way ANOVA is employed to verify the null hypothesis at 0.05 level of significance. The following Questionnaires were imposed to the people.

Questionnaires**:**

1. Spread computer virus through internet
2. Hacking people's personal and sensitive information in internet.
3. Obtain license or digital signature certificate by misrepresentation of the facts.
4. Publishing false digital certificate.
5. Personal ID theft.
6. Upload female picture without their consent.
7. Use social network sites to track people.
8. Constantly placing unwanted calls to people.
9. Sending unwanted text messages and e-mails to people.
10. Use internet to do illegal business.
11. Unauthorized use of Account numbers and ATM cards.
12. Guessing passwords.
13. Unauthorized downloading the books/research papers.
14. Illegally posting the advertisements for Job/ admission.
15. Counseling through online for placement.
16. Spam e-mails

After getting the 4 types of responses such as Mostly (M), Sometimes(S), Rarely (R) and Never (N), we concluded those persons involving in cyber crime activities and their numbers are given in Table 1.

3.1 Research Hypotheses

H_0**:** The different educational qualified persons have no significance difference on their involvement in different cyber crime activities.

Table 1. Number of persons involving in cyber crime activities having different types of qualifications

A_α (11)	B_α (12)	C_α (12)	D_α (10)
A_β (15)	B_β (17)	C_β (13)	D_β (11)
A_γ (8)	B_γ (10)	C_γ (15)	D_γ (14)
A_δ (2)	B_δ (3)	C_δ (10)	D_δ (17)

4. Statistical Interpretation (Analysis of Variance)

Table 1 contains the number of persons involving in cyber crime activities having different types of qualifications engaged in different sectors. These people have the age above 18 years. They spread computer virus via internet, upload the female pictures without their permission, uploading false advertisement to provide job, hacking others websites and downloading unauthorized research material/books etc.

In Table 2, the mean of different crimes and total mean of the crime has calculated. We conclude that the crime due to extramarital affair is more than the rest of crimes. Also the crime in academic and research area is less than the other crimes. Column-4 of above table shows that the post graduate qualified persons are more involved in the crime of academic and research areas.

V_r : Variation of row means from grand mean

$$= 4[(11.25 - 11.25)^2 + (11.25 - 14)^2 + (11.25 - 11.75)^2 + (11.25 - 8)^2] = 73.5$$

V_t : Total Variation

$$= (11.25 - 11)^2 + (11.25 - 12)^2 + (11.25 - 12)^2 + (11.25 - 10)^2 + (11.25 - 15)^2 + (11.25 - 17)^2 + (11.25 - 13)^2 + (11.25 - 11)^2 + + (11.25 - 8)^2 + (11.25 - 10)^2 + (11.25 - 15)^2 + (11.25 - 14)^2 +$$

V_e : Random Variation

$$= V_t - V_r = 201.5$$

Table 3 shows the analysis of variation, which is used to verify the hypothesis to be rejected or accepted.

Table 2. Mean of different crimes and total mean of the crime has calculated

	A	B	C	D	ROW SUM(SR)	ROW MEAN(MR)
α	11	12	12	10	45	11.25
β	15	17	13	11	56	14
γ	8	10	15	14	47	11.75
δ	2	3	10	17	32	8
					Grand Total(TG)=180 Grand Mean(MG)=11.25	

Table 3. Analysis of Variation

Variation	Degree of Freedom (df)	Mean $= \frac{variation}{df}$	F_{cal}	F_{tab} (0.05 level)
Between treatments $V_r = 73.5$	3	$\hat{S}_r^2 = 24.5$	$F = \frac{\hat{S}_r^2}{\hat{S}_e^2} = 1.4590$ **df: 3, 12**	$F_{0.95} = 3.49$
Within treatments $V_e = 201.5$	12	$\hat{S}_e^2 = 16.7916$		
$V_t = 275$	15			

5. Discussion of the Result

The summary of one-way ANOVA is presented in table-3 to analyze the null hypothesis. Since $\mathbf{F_{cal} < F_{tab}}$ at 0.05 level of significance .So the hypothesis is accepted .i.e. the educational qualification does not depend on the person's behavior on their involvement in different cyber crime activities. This may be attributed to the fact that each person has his own perception towards the crime irrespective of the educational qualification. From the Figure 1, it is well interpreted that the number of crime due to sexual harassment is more than the other crimes in the recent years. Figure 2 illustrate that the post graduate qualified persons do more crime in research/academy area than compared to others. So the only general qualification will not help a person to be a better citizen unless the moral education is acquired during their study.

6. Suggestions

It is contended by numerous creators that direction in morals ought to be a center part of the educational programs. This concentrate likewise recommends that morals instruction might be essential to accomplishing the objectives of enhanced security hones, legitimate consistence, and client trust. Additionally, coursework in the territories of law, security, and morals may serve to make a consciousness of the measurements of the cybercrime issue and counteract it. If the youths are agreed the required academic training, the knowledge established will be channeled towards the growth of the country. As recognized by the national strategy on training in various times that no country can transcend the nature of its instructive framework. The general population's contri-

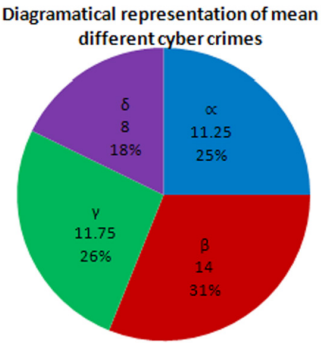

Figure 1. Diagrammatical representation of mean of different cyber crimes.

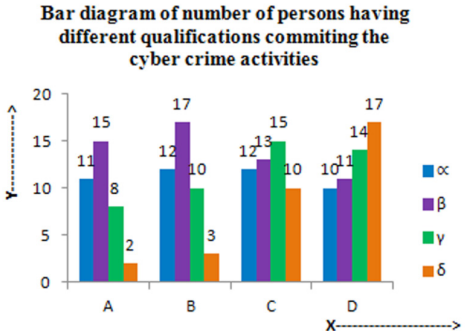

Figure 2. Bar diagram of number of persons having different qualifications committing the cyber crime activities.

bution in cybercrime is reliant on organization sort. The ramifications of the finding for information and improvement is that the present level of individuals' contribution in cybercrime negatively affects the estimation of training and by augmentation, has led to the misfortune in monetary advancement of the State. It is suggested that administration ought to enable the law requirement organizations to checkmate and manage culprits of cybercrime.

7. Conclusion

In this paper, the investigation reveals that the people's cyber crime activities are not depending on the higher qualifications. In the world of cyber crime the people possessing graduate /post graduate qualification are equally responsible to those persons having matriculation or intermediate qualification.Another finding is that the person having qualification post graduate are more involvement in the cyber crime activities in academic / research than comparison to others but overall crime is almost same. Further the cyber crime on extramarital affair is highest than other crimes and it is equally shared all four categories. Hence this investigation will give an insight to the future researchers to focus on the academic qualification while studding the cyber crime problems.

7. References

1. Odo B, Chinasa R, Odo AI. The extent of involvement in cybercrime activities among students' in tertiary institutions in Enugu State of Nigeria. Global Journal of Computer Science and Technology: Information and Technology. 2015; 15(3):1–6.
2. Böhme R, Moore T. How do consumers react to cybercrime?Proceedings of 7th APWG eCrime Reseachers Summit, Las Croabas; 2012.p. 1–12.
3. Burns S, Roberts L. Applying the theory of planned behavior to predicting online safety behavior. Crime Prevention and Community Safety. 2013; 15(1):48–64.
4. Clough J. Princples of cybercrime. Cambridge University; 2010.
5. Deloitte. Indian banking fraud survey: Navigating the Challenging, Environment [Internet]. 2012. [Cited 2016 Apr10]. Available from: https://www.academia.edu/4363002/India_Banking_Fraud_Survey_2012.
6. Dhanalakshmi R, Prabhu C, Chellapan C. Detection of phishing websites and secure transactions. International Journal of Communication Network and Security. 2011; 1(2):15–21.
7. Dorofeev S, Grant P. Statistics for real-life sample surveys: non-simple random samples and weighted data. 6th edn, Cambridge University Press: Boston; 2006.
8. Shalini D. Demographic relationship of cyber crime in india with special reference to various age groups. Abhinav National Monthly Refereed Journal of Research in Commerce and Management. 2014; 3(4):70–3.
9. Dinei F, Herley C. Sex, lies and cyber-crime surveys. Economics of Information Security and Privacy III. Bruce Schneier (ed.), Springer-Verlag: New York; 2013.p. 35–53.
10. Hair JF. Multivariate data analysis'. 7th edn, Prentice Hall; 2010.
11. Amichai-Hamburger Y, Hayat Z. The impact of the Internet on the social lives of users: A representative sample from 13 countries. Computers in Human Behavior. 2011; 27(1):585–9.
12. Henson B, Reyns BW, Fisher BS. Fear of crime online? Examining the Institutions in Zaria-Kaduna state of Nigeria. American International Journal of Contemporary Research. 2013; 3(9):98–114.
13. Jain SK, Jain M. Exploring impact of consumer and product characteristics on e-commerce adoption: A study

of consumers in India. Journal of Technology Management for Growing Economies. 2011; 2(2):35–64.
14. Jiao Y, Yang J, Xu S. A study of the impact of social media characteristics on customer adoption intention of social media. International Academic Workshop on Social Science (IAW-SC-13); 2013.p. 1095–9.
15. Kosse A. Do newspaper articles on card fraud affect debit card usage? Netherlands Central Bank, Research Department, DNB Working Papers 339 {internet]. 2012 Mar. [Cited 2016 Apr 10]. Available from: http://www.dnb.nl/binaries/working%20Paper%20339_tcm46-269083.pdf.
16. Kwon O, Wen Y. An empirical study of the factors affecting social network service use. Computers in Human Behavior. 2010; 26(2):254–63.
17. Littlewood A. Cyberporn and moral panic: an evaluation of press reactions to pornography on the internet. Library and Information Research. 2003; 27(86):8–18.
18. Rogers MK, Seigfried K, Tidke K. Self-reported computer criminal behavior: A psychological analysis. Digital Investigation. 2006; 3:116–20.
19. Matthews B. Computer Crimes: Cybercrime Information, Facts and Resources [Internet]. 2015. [Cited 2016 Apr 10]. Available from: http://www.thefreeresource.com/computer-crimes-cybercrimeinformation-factsand-resources.
20. Morris RG, Higgins GE. Criminological theory in the digital age: The case of social learning theory and digital piracy. Journal of Criminal Justice. 2010; 38:470–80.
21. Randa R. The influence of the cyber-social environment on fear of victimization: Cyber bullying and school. Security Journal. 2013; 26:331–48.
22. Salifu A. Impact of Internet crime on development. Journal of Financial Crime. 2008; 15(4):432–44.
23. Yu S. Fear of cyber crime among college students in the United States: An exploratory study. International Journal of Cyber Criminology. 2014; 8(1):36–46.
24. Saini H, Rao YS, Panda TC. Cyber-Crimes and their Impacts: A review. International Journal of Engineering Research and Applications. 2012; 2(2):202–9.
25. Wilsem J. Hacking and harassment: Do they have something in common? Comparing risk factors for online victimization. Journal of Contemporary Criminal Justice. 2013; 29(4):437–53.
26. Yu S. Digital piracy justification: Asian students versus American students. International Criminal Justice Review. 2013; 23(2):185–96.