

University Graduates Awareness Towards Cybercrime And Familiarity Of Its Terms: A Comparison

Dr. R.D.Padmavathy

Assistant Professor

Department of Education, Tezpur University (A Central University), Assam

padmajothi@yahoo.in

Abstract

The aim of this paper is to explore the cyber crime awareness and its familiarity of various cyber-crimes terms among graduates with respect to their gender, locality, educational level, stream of study, computer facility, number of year's familiarity with internet and number of year's participation in cyber forums are discussed. In the present study researcher adopted descriptive survey method to collect the data for the cybercrime awareness among young graduates. The sample comprised 180 samples selected using stratified proportionate sampling ages range from 19-24 years. The finding of the study shows that there is no significant difference towards cybercrime awareness among graduates with respect to their gender, locality, computer facility and stream of study but significant difference exists with respect to their educational level, number of years familiar with Internet and number of year's participation in cyber forums. Under graduates shows more familiarity on many cybercrime terms compared to post graduate students. Graduates are high risk of becoming cyber victim so proper awareness and training provision should be imparted among graduates about cybercrime.

Key words: Cybercrime, Young graduates, Internet Users, Categories, Familiarity

Introduction

Cybercrime is a new wave of crimes using internet facilities, which needs to be addressed urgently and earnestly by policy planners to protect the young generation as there is a high risk of becoming a victim of this crime (Mensch and Wilkie,2011). Also Narahari & Shah (2016) opined that internet users still lack knowledge and awareness on cybercrimes, in India and also proves that internet users are not thoroughly aware of cybercrimes and cyber

security that are prevailing. A growing net addiction is visible every corner of the world. The convergence of smart phones and internet are on stride and quite popular. This means, there is more scope for cybercrimes. Though many internet users claim to be aware of such crimes, still majority consider the cybercrime as hi-fi politically motivated attacks on big organizations. They fail to understand that it can affect any internet user. Other than hacking, a quiet majority of users are not aware of crimes like cyber stalking, mobile hacking, TOR and Deep web crimes, copyright violation, cyber bullying, phishing, child soliciting and abuse, sharing disturbing content of pornography, identify theft etc. A significant amount of internet users are not even aware whom to contact or report for any grievances regarding cybercrimes.

Thomas and Loader define cybercrime as any computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Based on this definition we can classify cyber-crimes into different categories. They are computer-assisted crimes such as fraud, theft, money laundering, sexual harassment, hate speech and pornography. Another classification is computer focused crimes. These types of crimes came into existing after the introduction of the internet. They are hacking, viral attacks, website defacement etc. (cyber-crime and society, 2006). This type of crime needs a fraction of seconds to damage the target and increasing all around the world. More adolescence, girls and women access to usage of internet through computer or smart phones for their up to date development and feel social networking sites provide a space to express their ideas with freedom and provide an online privacy without knowing the consequences.

The technological devices have completely changes the people's life styles psychologically as well as behaviourally. Living without technological gadgets and internet is impossible for many people in the growing e-world. Its influence is very high among young and adolescents who are the digital natives of the world and they are the consumers of cyberspace. A rapid change witnessed in the life styles of adolescence made them as technical consciousness and internet usage both for leisure activity and for work. As the consumers of cyberspace grows as equally cyber crimes increases. Without knowing the consequence many

graduates particularly girls, adults and children become the victims of cybercrime. Considering the safeguarding citizens from cybercrime victimization depends on the enhance among graduates creating the knowledge, awareness about issues, laws, acts and preventive measures to be adopted while using internet is need of the hour. It makes the country to prevent the graduates from cybercrime by framing “Cyber crime Act 2000”.

Categories of Cybercrimes

The cybercrimes are not fixed to, or limited to few types that are quite being heard by the graduates, but they are ever evolving with new strategies, thus throwing new challenges to crack down. Given below is the compiled list, updated from various studies (Aggarwal, 2015; Pahuja, 2011).

- ***Crimes against Individuals*** are done to harm particular individuals. These crimes care like – harassment via emails, cyber-stalking, cyber bullying, dissemination of obscene material, defamation, hacking, cracking, email spoofing, SMS spoofing, carding, cheating and fraud, child pornography, assault by threat, denial of service attack, forgery, and phishing.
- ***Cybercrimes done to harm the property of an Individual or Organizations.*** They can be classified as – Intellectual property crimes, cyber squatting, cyber vandalism, hacking computer system, computer forgery, transmitting viruses & malicious software to damage information, Trojan horses, cyber trespass, Internet time thefts, robbery or stealing money while money transfers etc.
- ***Cybercrimes against government*** are like – cyber terrorism, cyber warfare, distribution of pirated software, possession of unauthorized information etc.
- ***Cybercrimes that are highly threatening issues at societal level*** are child pornography, cyber trafficking, online gambling and financial crimes.

Review of Related Literature

This section reports a brief literature review about the issues related to cybercrime awareness, laws and security. Malhotra & Malhotra(2017) found that there is significant independent effect of variables viz. gender and locality on the level of cyber crime awareness among teacher trainees. Sukanya & Raju (2017) conducted to know the Cyber Law Awareness among Youth of Malappuram District have a basic level of understanding on information Technology Act, 2000 in India and found vast minority (41%) undergraduates from rural area are totally unfamiliar with IT Act, 2000. Gender, education and area of living do not show any significant relationship in understanding the cyber law awareness of IT Act, 2000 in India. Mokha (2017) found there is a relationship exists between the age groups and educational qualification of the respondents. So, it is the duty of one and all internet users to be aware of the cyber-crime and security and also help others by creating awareness among them.

Parmar and Patel (2016) concluded from their survey that most of the graduates, irrespective of being related to IT field were not able to actively keep themselves updated with the latest information related to cyber law and computer security. They felt that the situation could be ever worse among the graduates who are not associated with IT field. They recommended inculcating basis ethics among graduates, while creating awareness on cyber laws in India. Prabu(2015) found subjects belong to rural locality pursuing arts courses in private colleges perform better than their counterpart. In similar to this study Goel (2014) found awareness towards cybercrime is not significantly affected by gender but it is affected by area of residence and stream of study. Singaravelu & Pillai(2014) found B.Ed. students has low level of cybercrime, Moreover male B.Ed. graduates found better than female in cyber crime awareness but there is no significant difference between B.Ed. students residing areas, computer facility, participated in cyber forums in awareness on cyber crime. Mehta and Singh (2013) found there is a significant difference in male and female graduate's awareness about cyber laws in India. Aparna and Chauhan (2012) pointed out the seriousness of this security issue and need of limits its impact worldwide. Slusky and Navid (2011) found information security awareness is lower than that of its understanding among the college students at California state university.

In contrary to the above result, a study by Hasan *et al.*, (2015) found cybercrime awareness found female graduates more aware about cybercrime and compared to male students. Prabu(2015) The awareness about cyber crime of female, rural, arts subject, private college students is better and having high level of awareness than their counter part. Rajasekar (2010) found that the B.Ed. female from urban belong to science subjects show high awareness on cyber crime than their counterparts. Peng and Ramaiah (2007) found most of the users were not able to keep updated with latest information regarding computer security and observation is consistent across different fields in Singapore.

Need for the study

The general assumptions among many young graduates and adults are hacking means hijacking the accounts of email and social networking sites. Challenges that cybercriminals throw are becoming tougher day by day and the government has to keep a vigilant eye on the happenings. Unfortunately, there is a huge dearth of cyber experts to handle the issues when compared to number of cases that are being filed in India” prevailing among the common people is that the cyber criminals target only organizations and big shots and why would they bother me. But that is not the ground reality. A common man who uses internet, mobile or have any scope to share their personal transactional details by any means (either by email or by orally) can easily become prey” Both the experts felt that the security measures taken by banking and companies are not much impactful. “Honestly nothing on internet is safe. Banking verifications and sessions inquiry has been processing but when it is linked with other online website, it can be hacked very easily” (Narahari & Shah, 2016). After the extensive review of related literature it is found many researchers were carried out to know the cyber crime awareness level, awareness about cyber laws and acts, internet usage and security in general but there were no studies found to know about the cybercrime awareness of graduates of university with respect to their gender, locality, level of education, stream of study, computer facility, number of years familiarity with internet and number of years participation in cyber forums and familiarity of cybercrime terms among young graduates. Many researchers found adolescents aware of cybercrimes but no researches try to find in about the familiarity of its terms against individuals, property, threat to government

and society. Hence the study is conducted in this nature to cyber crime awareness level and familiarity of various cyber-crime terms of graduates of Assam.

Objectives of the Study

- To study the cyber crime awareness level of graduate students of Assam.
- To find out the familiarity of various cyber-crimes terms in cyber space among graduates of university.
- To study the cybercrime awareness of graduates of university with respect to their gender, locality, level of education, stream of study, computer facility, number of years familiarity with internet and number of years participation in cyber forums.

Hypotheses of the Study

- Cyber crime awareness level of graduates is positive.
- There exists no significant difference in cybercrime awareness of graduates of university with respect to their gender, locality, stream of study, level of education, computer facility, number of year's familiarity with internet and number of year's participation in cyber forums.
- The graduates possess positive awareness and familiarity towards various cyber-crimes terms.

Research Design of the study**(a) Methodology of the Study:**

In the present study researcher adopted Descriptive survey method to collect the data for the cybercrime awareness among graduates of university from a population who uses computer and internet facilities in daily life.

(b) Population and Sample of the Study:

The population for the study includes the entire graduates of Sonitpur district. The investigator has selected 180 samples using simple random sampling technique. The samples were drawn from the graduates studying in undergraduate and postgraduate course in Tezpur University. This includes both the male and female young graduates. The sample consists of

ninety undergraduate and ninety post graduate young graduates studying in university. The questionnaire was sent through email to 200 graduate students. The responses received from 180 samples were considered as a sample for this study. The graduate's ages range from 19-24 years.

(c) Research Tools Used for the study:

To meet the objectives of the study cybercrime awareness level scale constructed by Dr. Rajasekar S (2011) and personal information schedule developed by investigator to get the information and names of the various cybercrimes in cyberspaces. It consists of 36 statements in that 21 are positive and 15 negative statements with 5 options. Each statement was against five point scale from strongly agree, agree, undecided, disagree to strongly disagree and weightage of 5, 4, 3, 2, 1 were given in the order for positive statements and scoring is reversed for the negative statements. The positive statements having the scoring as 5,4,3,2 and 1 and for the negative statements it has been reversed. The score ranges from 36 to 180. The construct validity of the scale was found to be 0.87 and reliability was determined by using the Spearman-Brown prophecy formula, was found to be 0.76.

(d) Statistical Technique:

The study conducted to observe how a graduate understands the concept of cybercrime, awareness and familiarity with its terms. The data were analysed using mean, standard deviation and t-test to measure cyber crime awareness of university graduates.

Data Analysis and Interpretation

The data analysis for the present study is done with the help Statistical Package for the Social Sciences (SPSS) programme and the results are presented below.

Table 1: Showing descriptive and differential analysis for cybercrime awareness on the stream of study.

Variables	Sub Variables	N	Mean	SD	t-value	Sig. Level
Gender	Male	50	142.27	10.60	0.861 (178)	0.390
	Female	130	140.77	10.26		
Locality	Urban	100	141.63	10.58	0.703 (178)	0.483
	Rural	80	140.52	10.03		
Level of Education	Undergraduate	90	142.15	10.44	1.149 (178)	0.025
	Postgraduate	90	140.37	10.25		
Stream of study	Arts	105	140.36	10.21	1.253 (178)	0.212
	Science	75	142.32	10.49		
Computer Facility	Having own computer	100	141.58	10.56	0.668 (178)	0.505
	Not having own computer	80	140.51	10.02		
No. of years familiar with Internet	Less than 2 years	95	140.03	10.65	0.200 (178)	0.042
	More than 2years	85	146.34	10.06		
No. of years participation in cyber forums	Less than 2 years	134	148.37	10.24	0.415 (178)	0.035
	More than 2years	46	140.63	10.75		

Interpretation

- It is inferred from the above table, the calculated t- value is found to be 0.861with df 178 and level of significance is 0.390 which is greater than the 0.05 level of significance. It indicates male and female graduates do not differ significantly. Thus, the null hypothesis there is no significant difference towards cybercrime awareness among graduates of university with respect to their gender is accepted. Further the obtained difference between male and female are likely due to chance. The mean score of male graduates is 142.27 which is higher than the female graduates mean score of 140.77. It can be interpreted that male graduates has more awareness towards cybercrime than female young graduates.

- It is inferred from the above table, the calculated t- value is found to be 0.703 with df 178 and level of significance is 0.483 which is greater than the 0.05 level of significance. It indicates urban and rural graduates do not differ significantly. Thus, the null hypothesis there is no significant difference towards cybercrime awareness among graduates of university with respect to their locality is accepted. Further the obtained difference between urban and rural are likely due to chance. The mean score of urban graduates is 141.63 which are higher than the rural graduates mean score of 140.52. It can be interpreted that urban graduates have more awareness towards cybercrime than rural young graduates.

- It is inferred from the above table, the calculated t- value is found to be 1.149 with df 178 and level of significance is 0.025 which is less than the 0.05 level of significance. It indicates under graduate and post graduate graduates not differ significantly. Thus, the null hypothesis there is a significant difference towards cybercrime awareness among graduates of university with respect to their level of education is not accepted. Further the obtained difference between under graduate and post graduate are likely not due to chance. The mean score of under graduate graduates is 142.15 which are higher than the post graduate graduates mean score of 140.37. It can be interpreted that under graduate graduates have more awareness towards cybercrime than post graduate young graduates.

- It is inferred from the above table, the calculated t- value is found to be 1.253 with df 178 and level of significance is 0.212 which is greater than the 0.05 level of significance. It indicates arts and science graduates do not differ significantly. Thus, the null hypothesis there is no significant difference towards cybercrime awareness among graduates of university with respect to their stream of study is accepted. Further the obtained difference between arts and science are likely due to chance. The mean score of arts stream graduates is 140.36 which are higher than the science stream graduates mean score of 142.32. It can be interpreted that science stream graduates have more awareness towards cybercrime than arts stream young graduates.

- It is inferred from the above table, the calculated t- value is found to be 0.668 with df 178 and level of significance is 0.505 which is greater than the 0.05 level of significance. It indicates having own computer and not having own computer graduates do not differ significantly. Thus, the null hypothesis there is no significant difference towards cybercrime awareness among graduates of university with respect to their computer facility is accepted. Further the obtained difference between graduates having own computer and not having own computer are likely due to chance. The mean score of having own computer graduates is 141.58 which is higher than the not having own computer graduates mean score of 140.51. It can be interpreted that graduates having own computer has more awareness towards cybercrime than graduates not having own computer.

- It is inferred from the above table, the calculated t- value is found to be 0.200 with df 178 and level of significance is 0.042 which is less than the 0.05 level of significance. It indicates student's familiarity in internet less than 2 years and more than 2 years graduates differ significantly. Thus, the null hypothesis there is no significant difference towards cybercrime awareness among graduates of university with respect to their number of years familiar with internet less than 2 years and more than 2 years graduates is not accepted. Further the obtained difference between less than 2 years and more than 2 years are not likely due to chance. The mean score of less than 2 years graduates is 140.63 which is higher than the more than 2 years graduates mean score of 146.34. It can be interpreted that graduates having more than 2 years familiar with internet has more awareness towards cybercrime than graduates having less than 2 years of familiarity with computer.

- It is inferred from the above table, the calculated t- value is found to be 0.415 with df 178 and level of significance is 0.415 which is greater than the 0.05 level of significance. It indicates student's participation in cyber forums less than 2 years and more than 2 years graduates differ significantly. Thus, the null hypothesis there is no significant difference towards cybercrime awareness among graduates of university with respect to their number of years participation in cyber forums is not accepted. Further the obtained difference in student's participation in cyber forums between less than 2 years and more than 2 years are likely not due to chance. The mean score of less than 2 years graduates is 148.37 which is

higher than the student's participation in cyber forums more than 2 years graduates 140.63. It can be interpreted that graduates participation in cyber forums less than 2 years has more awareness towards cybercrime than more than 2 years.

Familiarity with Cyber Crimes Terms

Cyber crimes were divided into crime against individuals, crime against property, crime against threat to government and cyber crime against society. Samples were asked to recognise the term of cyber crime.

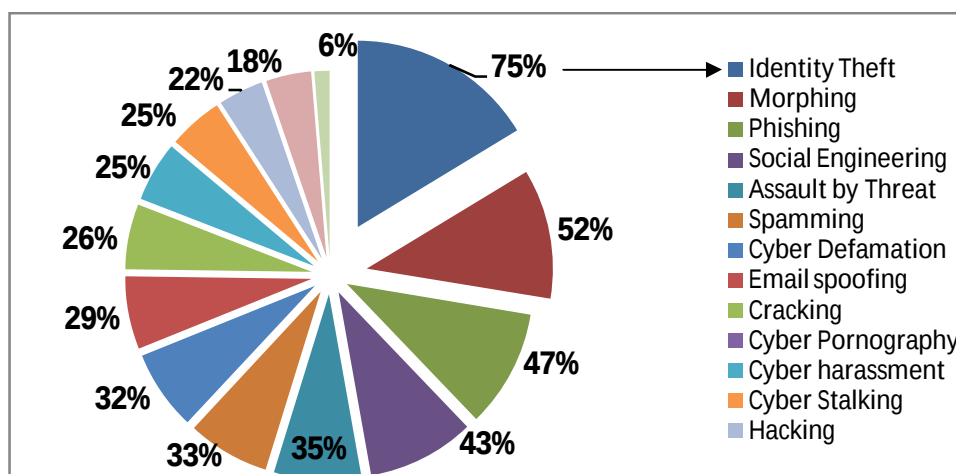
More than 93% of graduates are not aware with the term SMS spoofing, 81% of graduates are not aware with the term hacking, Being the most often crime a large majority 74% of graduates are strange to cyber harassment and cyber pornography, 73% of graduates are unfamiliar to cheating and fraud and cracking, Majority of graduates more than 65% are unfamiliar with cyber stalking, spamming, cyber defamation, assault by threat. 57% graduates are unfamiliar with the cyber crime social engineering, 54% are unfamiliar with the term Phishing and 48% are unfamiliar with the term Morphing. But vast majority (75%) of the graduates are familiar with identity theft, next to that 52% are familiar with morphing, 47% of graduates are familiar about phishing and considering the rest more than 20% and less than 30% graduates are aware about the terms assault by threat, spamming, cyber defamation, email spoofing, cracking, cyber pornography, cyber harassment and cyber stalking. a vast minority of graduates are unfamiliar with the term SMS spoofing(6%), cheating fraud and Hacking.

Table 2: Familiarity with Cyber Crimes against Individual

Education Level of Preservice Teachers →	Post graduate		Undergraduate	
Cyber Crimes Terms ↓	Familiarity	Non Familiarity	Familiarity	Non Familiarity
Assault by Threat	39 (22%)	74 (41%)	24 (13%)	43 (24%)
Cheating & Fraud	14 (7.7%)	65 (36%)	33 (18%)	68(37%)
Cracking	17 (9.4%)	67 (37%)	31 (17%)	65 (36%)
Cyber Defamation	16 (8.8%)	54 (30%)	44 (24%)	66 (36%)

Cyber harassment	16 (8.8%)	69(38%)	29 (16%)	66 (36%)
Cyber Pornography	24 (13%)	76 (42%)	22 (12%)	58 (32%)
Cyber Stalking	22 (12%)	80(36%)	18(10%)	60(33%)
Email spoofing	24(13%)	69(38%)	29(16%)	58(32%)
Hacking	14(7.7%)	79(43%)	19(11%)	68(38%)
Identity Theft	70(39%)	34(19%)	64(36%)	12(6.6%)
Morphing	57(32%)	62(34%)	36(20%)	25(14%)
Phishing	64(36%)	79(44%)	19(11%)	18(10%)
SMS Spoofing	6(3%)	93(52%)	5(3%))	76(42%)
Social Engineering	11(6%)	32(18%)	66(37%)	71(39%)
Spamming	22(12%)	61(34%)	37(21%)	60(33%)

Figure 1: Pie chart showing the percentage wise distribution of familiarity of cybercrime term against individuals



Considering the graduates educational level, awareness about cyber crime terms among undergraduate graduates showed more familiar with social engineering, cyber defamation, spamming, cheating and frauds, cracking, email spoofing and cyber harassment compared to post graduate. In other words, post graduates percentage wise non familiarity of cyber crime against individuals is high compared to under graduate. Among the Post graduates awareness should be increased considering the terms SMS spoofing, phishing,

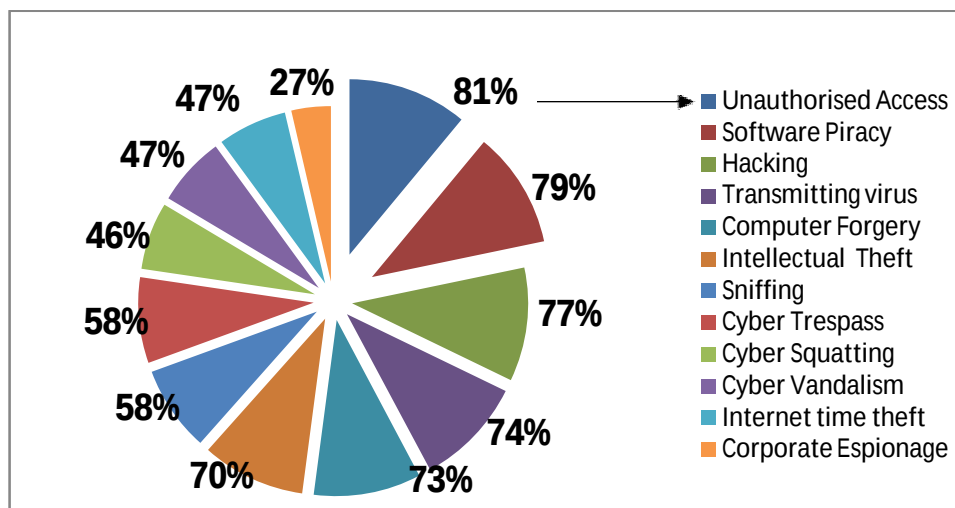
hacking, cyber pornography, cyber harassment, email spoofing, cracking, cyber stalking, spamming and morphing and assault by threat.

Majority of post graduate and undergraduate were familiar with Social engineering, cheating and fraud and Cracking. Considering the SMS spoofing both undergraduate and post graduates are non familiar with the cybercrime term.

Table 3: Familiarity with Cyber Crimes against Property

Education Level of Preservice Teachers →	Post graduate		Undergraduate	
Cyber Crimes Terms ↓	Familiarity	Non Familiarity	Familiarity	Non familiarity
Corporate Espionage	10(10%)	49(28%)	32 (17%)	81(45%)
Computer Forgery	65(36%)	17(9%)	66(37%)	32(17%)
Cyber Squatting	52(29%)	66(37%)	30(17%)	32(17%)
Cyber Trespass	34(19%)	48(27%)	70(39%)	28(15%)
Cyber Vandalism	32(17%)	50(28%)	54(30%)	44(24%)
Unauthorised access or control over computer system	76(42%)	6(3%)	70(39%)	28(15%)
Hacking computer	58(32%)	24(13%)	81(45%)	17(9%)
Intellectual Property theft	52(29%)	30(17%)	74(41%)	24(13%)
Internet time theft	44(24%)	38(21%)	41(23%)	57(32%)
Transmitting Virus	74(41%)	8(4%)	59(33%)	39(22%)
Sniffing	34(19%)	48(27%)	70(39%)	28(15%)
Software Piracy	73(40%)	9(5%)	70(39%)	28(15%)

Figure 2: Pie chart showing the percentage wise distribution of familiarity of cybercrime term against property

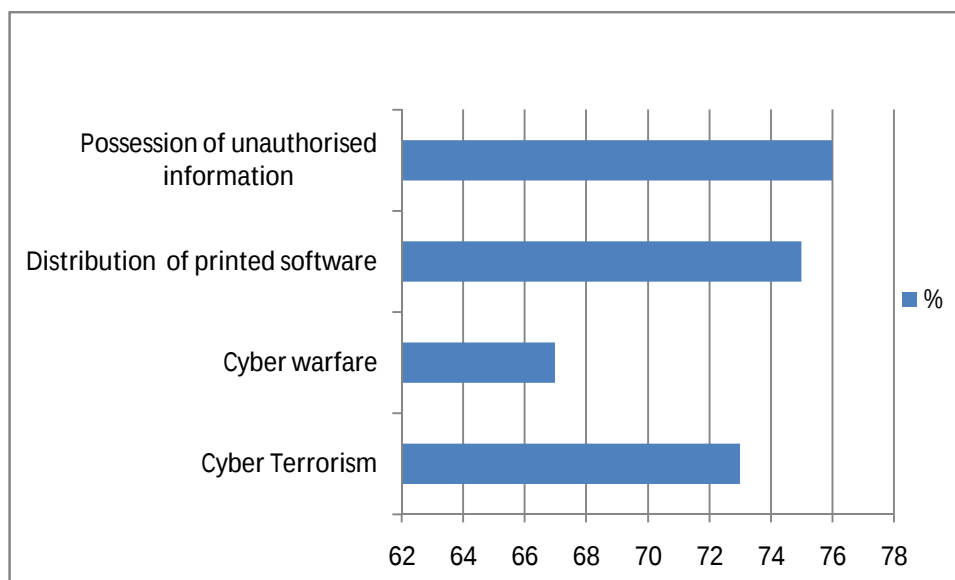


It is inferred from the above Table 3, vast majority of the graduates are aware and familiarity about the term Unauthorised access or control over computer system (81%) and software piracy (79%). More than 70% of graduates have awareness about computer Hacking, transmitting Virus, Computer forgery and Intellectual Property theft. But only 58% were aware about the cyber trespass and sniffing. Less than 50% of graduates are aware about cyber squatting, cyber vandalism and internet time theft. But the very sad is only 27% graduates are aware about that Corporate Espionage.

Table 4: Familiarity with Cybercrimes Threat to Government

Education Level of Preservice Teachers Cyber Crimes Terms	Post graduate		Undergraduate	
	Familiarity	Non familiarity	Familiarity	Non familiarity
Cyber Terrorism	17(10%)	65(36%)	31(17%)	67(37%)
Cyber warfare	16(9%)	66(37%)	44(24%)	54(30%)
Distribution of printed software	16(9%)	66(37%)	29(16%)	69(38%)
Possession of unauthorised information	22(12%)	58(32%)	20(12%)	80(44%)

Figure 3: Bar chart showing the Familiarity with Cybercrimes Threat to Government



It is inferred from the above Table 3; more than 65 % of the graduates are unaware and not familiarity about the term cyber terrorism, cyber warfare, distribution of printed software and possession of unauthorised information. Comparing the awareness about familiarity with cybercrimes threat to government, high number of undergraduate graduates shows a non familiarity with the terms.

Table 5: Familiarity with Cyber crimes against Society

Education Level of Preservice Teachers →	Post graduate		Undergraduate	
Cyber Crimes Terms ↓	Familiarity	Non familiarity	Familiarity	Non familiarity
Child pornography	22(13%)	60(33%)	18(10%)	80(44%)
Cyber extortion	24(14%)	58(32%)	29(16%)	69(38%)
Financial crime	25(14%)	57(32%)	36(20%)	62(34%)
Web Jacking	18(10%)	64(35%)	19(11%)	79(44%)
Online Gambling	14(8%)	68(38%)	19(11%)	79(43%)

It is inferred from the above Table 4, considering the familiarity with cyber crimes against society high graduates (81%) show that they were not familiar with the online gambling. More than 65 % of the graduates are aware and familiarity about the term cyber

extortion, child pornography, web jacking and financial crime. Comparing the awareness about familiarity with cybercrimes against society, high numbers of post graduates are non familiarity with the terms.

Findings of the Study

On the base of findings of present investigation the main findings of the study are

- There is no significant difference towards cybercrime awareness among graduates of university with respect to their gender, locality, computer facility and stream of study.
- But there is a significant difference towards cybercrime awareness among graduates of university with respect to their educational level, Number of years familiar with Internet and number of year's participation in cyber forums.
- Majority of graduates are unfamiliar with the cyber crime terms against individuals, crime against property, crime against threat to government and cyber crime against society.

Conclusion

This study proves that graduates are not having more awareness about cyber crimes terms and addicted to internet. This shows there is a scope for cybercrimes. They have more misconceptions about cybercrimes. Though they claim that they were aware about the cybercrimes, still majority of the graduates are not aware about less than 30% graduates are aware about the terms assault by threat, spamming, cyber defamation, email spoofing, cracking, cyber pornography, cyber harassment and cyber stalking. A vast minority of graduates are unfamiliar with the term SMS spoofing (6%), cheating fraud, Social engineering, cyber trespass, sniffing, cyber squatting, cyber vandalism and internet time theft. But the very sad is only 27% graduates are aware about that Corporate Espionage. While considering the cyber crime against the property and threat to government more than 65 % of the graduates are unaware about the term cyber terrorism, cyber warfare, distribution of

printed software and possession of unauthorised information, cyber extortion, child pornography, web jacking and financial crime.

Most of the graduates though aware about IT act 2000, in country like India vast majority are unaware about the legal system. So government should take necessary measure to create awareness not only in general about the laws but also the basic preventive measures to follow in day today life activities. Most of graduates revealed that they heard about the term cybercrime, cyberspace and laws but they were not aware about the terms and its meaning. Without knowing about the issues protecting them from cyber criminals is not possible. So government and authorities should take serious concern on this modern crime issues and create proper awareness to remove the ignorance about cybercrime.

Reference

- Aggarwal, Gifty. (2015).General Awareness on Cyber Crime. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5 (8), 204-206.
- Aparna and Chauhan, M. (2012), Preventing Cyber Crime: A Study Regarding Awareness of Cyber Crime in Tricity. *International Journal of Enterprise Computing and Business Systems*, January, Vol 2, Issue 1.
- Cyber-Crime and Society (2006).As cited in Sukanya, K. P.& Raju, C. V(2017). Cyber Law Awareness among Youth of Malappuram District. *IOSR Journal of Humanities and Social Science*, 22(4), Ver. 5, 23-30.
- Glossary of Cybercrime Terms.
Retrieved from <https://dealers-insurance.com/glossaryofcybercrieterms.php>
- Goel, U. (2014). Awareness among B.Ed Teacher Training towards Cybercrime - A Study. *Learning Community*: 5(2 & 3).107-117.
- Hasan, et al., (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. *Journal of Social Sciences*, Vol. 11 (4): 395.404
- Malhotra,T. & Malhotra,M.(2017). Cyber Crime Awareness among Teacher Trainees. *Scholarly Research Journal for interdisciplinary Studies*. 4 (31). 5249- 5259.
- Mensch, S. and L. Wilkie, (2011). Information security activities of college young graduates: An exploratory study. *Acad. Inform. Manage. Sci. J.*, 14: 91-116.
- Mehta, S & Vikram, S.(2013).A Study of Awareness about Cyber laws in The Indian Society. Volume 4 Issue 1. Retrieved from <https://www.researchgate.net/publication/322071015>
- Mokha, A.K.(2017). A Study on Awareness of Cyber Crime and Security. *Research Journal of Humanities and Social Sciences*. 8(4), 459-464.

- Narahari, A.C. & Shah, V.(2016).Cyber Crime and Security – A Study on Awareness among Graduates of Anand. *International Journal of Advance Research and Innovative Ideas in Education*. 2(6). 1164-1172.
- Parmar, A. & Patel, K. (2016). *Critical Study and Analysis of Cyber Law Awareness among Graduates*. Conference: International Conference on ICT for Sustainable Development. Retrieved from http://link.springer.com/chapter/10.1007%2F978-981-10-0135-2_32, Volume: 409.
- Prabhu, S.(2015). Awareness on Cyber Crime among Arts and Science Students. *International journal of Teacher Educational Research*.4 (9).7-13.
- Peng, Tan Kar and. Ramaiah, C.K.(2007). Awareness of Cyber Laws in Young Singaporeans. *DESIDOC Bulletin of Information Technology*, Vol. 27, No. 6, pp. 41-53.
- Rajasekar S. (2013).Cyber Crime Awareness Scale, National Psychological Corporation, Kacheri Ghat, Bhargav Bhawan, Agra.
- Singaravelu & Pillai. (2014). B.Ed. student's awareness on cybercrime in Perambalur district. *International Journal of Teacher Educational Research*. 3(3). 37-40.
- Sukanya, K. P.& Raju, C. V.(2017). Cyber Law Awareness among Youth of Malappuram District. *IOSR Journal of Humanities and Social Science*, 22(4), Ver. 5 ,23-30.
- Slusky, L. and Partow-Navid, P. (2012)._Students Information Security Practices and Awareness, *Journal of Information Privacy and Security*, 8:4, 3-26, DOI: [10.1080/15536548.2012.10845664](https://doi.org/10.1080/15536548.2012.10845664)