# A SURVEY OF B.Ed. STUDENTS' PERCEPTION AND AWARENESS TOWARDS CYBERCRIME

NEETU SPRING
RESEARCH SCHOLAR, FACULTY OF EDUCATION, INTEGRAL UNIVERSITY, LUCKNOW, INDIA

***ABSTRACT*:** Cybercrime is a term used broadly to describe criminal activity in which computers or networks are a tool, a target or a place of criminal activity, this term is also used to include traditional crimes in teaching and learning, in which computers or internet is used to enable illicit activity. The use of internet is inevitable and of course one should face the risk factors attached to it. Hence, the perception and the awareness on cybercrime is very much needed for the learners as well as for teachers. Therefore, an attempt has been made to know the perception and awareness of B.Ed. students and to suggest its prevention. The purpose of this study is to protect them by providing empirical evidence from the policy makers in combating the attacks of the cybercrime and to suggest few precautions for its prevention. The study examines the relationship between perception and awareness of the students' in respect to their gender and age. A field survey is conducted among 200 B.Ed. students from college of education in Lucknow District of Uttar Pradesh.

A self structured questionnaire is used to perception that covers demographic information and seven most known cybercrime and a scale developed and validated by Dr. S. Raj Shekhar (2011), is used to find out the awareness towards the cybercrime. Percentile analysis , correlational analysis are done to test the hypotheses. In addition knowledge of prevention from cybercrime is given and the findings are 1) Male students are more aware and have affirmative insights than female,2) Students in the age group 18-23 years have lower perception and awareness than those aged 24 years and above . The study also provides the ways to prevent the B.Ed. students from cybercrime which will protect them reducing the high risk of becoming a victim.

**Key Words:** Awareness, Cybercrime, Cyber security, Perception, Prevention

## INTRODUCTION

Cybercrime or computer crime refers to criminal activity involving a computer. The computer may be used in the commission of a crime or it may be the target. Cyber -crimes are essentially a combination of these two elements and can be best defined as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as the Internet (chat rooms ,emails, noticeboards and groups)and mobile phones(SMS/MMS)". According to U.S. Department of justice ,The term "cyber –crime" can refer to offences including criminal activity against data ,infringement of content and copyright, fraud ,unauthorized access, child pornography and cyber – stalking.

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 high risk of becoming a victim of this crime (Ashokhia, 2010, Menseh and wilkie, 2011) There are two main categories that define the make up of cybercrimes. Firstly those that target computer networks or devices such as viruses, malware or denial of service attacks. The second category relate to crimes that are facilitated by computer networks or devices like cyber-stalking fraud, identity theft extortion, phishing (Spam) and theft of classified information.

In order to highlight the scale of Cybercrime globally the Norton Cybercrime Report 2011 revealed 430 million adults in 24 countries had been victims of Cybercrime in that year. Centre for strategic and international studies (CSIS) reported that every year there is a financial loss of 445 million dollar in world economy due to Cybercrime.

"With cybercrime forecast to become a USD 2.1 trillion business by 2019, frustration is growing among security experts" (Apac/junipers net/the shield)

Cybercrime statistics along with an increasing number of research studies indicate that young people do not always behave ethically in online activities and hence, there is a chance of every internet user becoming a victim (Mc quade, 2009), (Chen et al. (2008) state that human factors are involved in security awareness process. Human beings are usually the first line of defence to secure information assets, no matter how advanced and rigid the security technology solutions may be. All the security breaches such a virus infections, identity theft and hacking are the direct cause of carelessness and lack of knowledge and action on the part of users. (Chen et al, 2008). A high level information about the cybercrime and its prevention to young people should be given especially in educational institutions that would decrease the occurrence of cybercrime (Sembok, 2008),

Therefore, human factors such as gender, age, knowledge and experience may assist in knowing about the cybercrime. Students perception will help them to decide their actions while working on computers and using internet .All the persons who use internet today must be aware of the criminal activities taking place on the cyber space. Online transactions have made a large impact on the internet as it has totally changed the old and conventional methods of doing business. The identity of the customer with which you are dealing must br verified to prevent identity theft .Data and information must be protected on your website to protect it from illegal and unauthorised access.

Past studies have examined students attitude towards computer skills and ethics among educators (Shariff and Deni, 2005, Aris et al, 2004, Sembok, 2003). However, only few studies are, conducted to examine student's awareness and their perception towards cybercrime. So the students of B.Ed. have been taken to do study for the purpose. The following objectives are set for the study.

To study the level of perception towards 'Cybercrime' in terms of Gender and age
To study the level of awareness towards 'Cybercrime' in terms of Gender and age
To study the relationship between level of perception and level of awareness towards cybercrime

**Prevention of Cyber-crimes:**

Computer users can adopt various techniques to prevent cybercrime.

Most security software comes with a firewall. Turn on the firewall that comes with their router as well.

Don't Accept Offers of "Free PC Scans" That Pop up When You Use the Internet.

Some "scans" don't just give misleading results; they actually try to install unwanted software on your PC.

Make sure to apply relevant patches to your computer as soon as possible so that your system is protected. Similar to the way fabric patches are used to repair holes in clothing, software patches repair holes in software programs. Patches are updates that fix a particular problem or vulnerability within a program. If patches are not applied to the software, hackers exploit the vulnerabilities and compromise your system for malicious activities.

Protect Yourself from Identity theft .

The best way to prevent identity theft is to protect your identification, personal information and financial information from prying eyes. Do not reveal key personal information on social web sites like Facebook, Twitter, My Space etc. Don't keep all of your identification and financial information in one place and never write down your PIN (personal identification numbers) anywhere.

Don't fall prey for phishing scheme .

**Phishing** is the process by which someone obtains private information through deceptive or illicit means in order to falsely assume another persons'identity.

Do not open suspicious mails. Never click any link in the mail. Always copy the URL from mail and paste in the browser's address bar.

Don't tell ANYONE your password

Passwords are a common form of authentication and are often the only barrier between a user and your personal information. This should never be necessary. Good systems are set up so that nobody but you will ever know your password and authorized IT workers have their own accounts giving them access to what they need.

There are several programs attackers can use to help guess or "crack" password, but by choosing good passwords and keeping them confidential, you can make it more difficult for an unauthorized person to access your information.

Make your password complex

A good password should contain a mix of all the four types of characters: uppercase and lowercase letters, numbers, and symbols. Any character on your Windows or Mac keyboard is legal in a password you make for your own computer. Remember to include at least 8 characters and avoid common words and proper names. Do not repeat old passwords. Use separate password for each of the applications that you use. The more complex the password the more difficult to guess by others. Also passwords need to be changed at regular intervals.

Use variations on a strong "base" password

It's tough to remember a series of strong passwords and use a different one for each online system or site you access. The temptation is to use the same password for several or all systems and sites. That's a bad idea -- if a Bad Guy gets a hold of your password, he'll have the key that fits all of your doors. Instead, create a strong "base" password and then unique variations on it for each online system or site system you use. Here's a strong password: 6RQlk%3Z. Remember to change your "base" password and its variations on a regular base.

Always lock your computer (by pressing CTRL + ALT + DELETE and hitting "Enter") before walking away from it.

Don't click the "unsubscribe" link at the bottom of unsolicited emails.

You are responsible for all the activities carried out on your system using the login names assigned to you. Protect your system in all respects.

Use a password in only one place

Reusing passwords or using the same password all over the place is like carrying one key that unlocks your house, your car, your office, your briefcase, and your safe deposit locker. One lost key could let a thief unlock all the doors. Remember: Change your passwords on a schedule to keep them fresh.

Maintenance or rectification of faults in the system shall be carried out under close supervision.

DO NOT install Microsoft patches or updates sent by email (They are fake)

Microsoft never sends out patches or updates by email. There are no exceptions. Keep that in mind and you won't be a victim of a Microsoft patch hoax. Always install patches from your local patch server or from Microsoft update server. Never install patches from mail attachments or any other unauthorized sources.

**Social Networking Safety**

Social networking sites like Facebook are great tools for connecting with friends and keeping up-to-date with the good and bad things that are going on in your social circles.

Unfortunately, the kind and amount of personal information that makes for great social networking can be used by people with bad intentions to cause real, physical harm.

Use caution accepting friend requests in social media venues such as Facebook. Just because someone sends a friend request, it is not necessary to accept it. Be certain the person is someone known to you.

The following sections present review of literatures and hypotheses development, Research method, test of hypotheses, findings and conclusions.

## REVIEW OF LITERATURE AND HYPOTHESIS DEVELOPMENT-

Colfer (2007; Li, 2006) state that there are dissimilar perceptions and awareness between men and women. According to Titi (2003) women are more aware of cyber regulations and have superior ethical values compared to men. Women are less likely to become victims as compared to men.

Neiss et al. (2009) state that perception and awareness of young people are dissimilar between age groups. It is because young people and older people have different perspectives. Young people give more negative emotional perception than older adults.

Reyns,2010;Ngo et.al.,2011;wolak et al., 2006;Choi, 2008. It has been persistently reported that younger people are more likelyto be victimised than older people .The Australian Youth Affairs Commission (AYAC, 2010) submitted a report on cyber safety to the office of privacy commissioner in which they state that students in the age group of 18-24 are in high risk envioronments when expose to online activities.

Knowledge is very important for young people to prevent cybercrime (Curtis and colwell, 2000; Wang et al., 2008) Chwki (2005) states that educating young people would help decrease the risk of students in cyberspace.

Ashokhia (2010), finds that the level of education contributes significant differences to the students' perceptions of cybercrime.

Knowledge helps people to be more aware on cybercrime (Levin et al.., 2008). The number of cybercrime victims could be reduced by introducing proper awareness activities such as training programs, sufficient resource for compliance, develop policies & regulations and sufficient protection of personal information. (Choi, 2008; Leving et al. 2008; Chawki, 2005; Bougaardt and Kyobe, 2011).

Choi (2008) emphasises on the effectiveness of university programs in promoting knowledge and values about cybercrime as these programs could improve future behaviours of students towards cybercrime in terms of safety and security.

Based on the review of above literatures it is anticipated that gender, age and knowledge have significant influences on cybercrime. The following four null hypotheses are developed based on the above assumption and in line with the objectives of this study.

$H_0$= There is no association between perception of cybercrime and gender

$H_0$= There is no association between awareness of cybercrime and gender

$H_0$= There is no association between perception of cybercrime and age group.

$H_0$= There is no association between awareness of cybercrime and age group

## RESEARCH METHODOLOGY

Primary data is used to examine the influence of age and gender on both awareness and perception . A sample of 200 students of B.Ed. were selected using cluster sampling method and the study was conducted in different training colleges of Education in Lucknow District of Uttar Pradesh, India. For this a structured questionnaire developed by researcher is used to know the perception and a standardized scale developed and validated by Dr. S. Raj Shekhar (2011), is used to find out the awareness of the B.Ed. students of cybercrime.

Questionnaire were distributed and were completed and returned back to us in time. In the Questionnaire of perception seven most known cybercrimes were noted such as 1) Hacking 2) Theft 3) Cyber stalling 4) Identity theft 5) Malicious software 6) Computer vandalism 7) Child soliciting and abuse, besides this demographic information is also collected .

Frequency and percentile are done to examine the levels very low, moderate, high and very high) of perceptions about the above mentioned most known crimes and correlation analysis is done to examine the association strength between age and gender of perception and awareness .Finally, we check the correlation between level of perception and level of awareness of cybercrime.

## Results and Discussions

If we look at the percentile analysis of demographic data we find that 60% of the respondents are male and 40% are female. 30.4%( majority) of the respondents are in the age group of 20-24 years,31.3% (majority)of respondents use internet for 2-4 hrs.; 46.8%(majority) of the respondents have internet access through broadband . 41.8%(majority) have knowledge of cybercrime.

If we look at the percentile analysis of respondents' perception of seven most common crimes, Table -1 shows that respondents have different level of knowledge of

Hacking that is 31% moderate,26.5% high, 22%low, 10.5% very low and 10%very high knowledge respectively .Thus it could be deduced that the majority of the respondents have moderate knowledge. In case of Theft, the results shows that the majority of the respondents have moderate knowledge at 35.5%.while 31% high,15% low,13.5% very low and 5% very high knowledge respectively. Thus it is concluded that majority of them have moderate knowledge. In case of cyber stalking high knowledge at 35%, while 18.5% moderate ,12.5% low,12% very high and 9.5%very low. From this case we deduced majority have high level of knowledge. In case of Identity theft high knowledge at 33%,while 27% moderate, 19% low ,12% very low and 9% at very high level of knowledge. In this case majority is at high level of knowledge. In case of malicious software majority is at moderate level that is 30% , 23%at high level,22% at low level, 17% at very low level and 7.5% at very high knowledge. In this category majority have high level of knowledge. In case of computer vandalism high knowledge at 30.5%, 22.5% at moderate,22.5% at low ,15% at very high and 9.5% at very low level of knowledge. High level of knowledge is found among majority of cases in this type of cybercrime .In case of child soliciting and abuse majority is at moderate level which is 31.5%, 27% at low level, 20% at high level, 18%at very low level and 3.5% at very high level of knowledge and in the last category of type of cybercrime the majority falls at moderate level. If we analyse the overall result of knowledge of cybercrime types, which shows their perception towards cybercrime is 28.5% and 28.05 at high and moderate level respectively, 21.7% at low,12.8% at very low and only 8.86 %at very high level.It can be concluded that majority of respondents have either high or moderate level of perception towards cybercrime and moderate level of perception is found as far as low and very low level is considered . If we look at the high level then it is very low.

**Table-1. Perception of respondents**

| TYPES OF CYBERCRIME | f &% | VERY LOW | LOW | MODERATE | HIGH | VERY HIGH | TOTAL |
|---|---|---|---|---|---|---|---|
| 1.HACKING | f | 21.0 | 44.0 | 62.0 | 53.0 | 20.0 | 200 |
| | % | 10.5 | 22.0 | 31.0 | 26.5 | 10.0 | 100 |
| 2.THEFT | f | 27.0 | 30.0 | 71.0 | 62.0 | 10.0 | 200 |
| | % | 13.5 | 15.0 | 35.5 | 31.0 | 05.0 | 100 |
| 3.CYBER STACKING | f | 19.0 | 50.0 | 37.0 | 70.0 | 24.0 | 200 |
| | % | 09.5 | 12.5 | 18.5 | 35.0 | 12.0 | 100 |
| 4.IDENTITY THEFT | f | 24.0 | 38.0 | 54.0 | 66.0 | 18.0 | 200 |
| | % | 12.0 | 19.0 | 27.0 | 33.0 | 09.0 | 100 |
| 5.MALICIOUS SOFTWARE | f | 34.0 | 44.0 | 60.0 | 47.0 | 15.0 | 200 |
| | % | 17.0 | 22.0 | 30.0 | 23.5 | 07.5 | 100 |
| 6.COMPUTER VANDALISM | f | 19.0 | 45.0 | 45.0 | 61.0 | 30.0 | 200 |
| | % | 09.5 | 22.5 | 22.5 | 30.5 | 15.0 | 100 |
| 7.CHILD SOLICITING AND ABUSE | f | 36.0 | 54.0 | 63.0 | 40.0 | 07.0 | 200 |
| | % | 18.0 | 27.0 | 31.5 | 20.0 | 03.5 | 100 |
| TOTAL | f | 180.0 | 305.0 | 392.0 | 399.0 | 124.0 | 1400 |
| | % | 012.8 | 021.7 | 028.0 | 028.5 | 008.8 | 700 |

We use Pearson's pair wise product moment correlation coefficient (r) to examine the correlation between variables such as age and gender. For statistical analysis we use IBM-20.0 SPSS. It is analysed that positive correlation existed between the age and gender which is 0.134.we use z-test for gender and f-test for age. we analyse the results from both aspects such as level of perception and level of awareness for gender and age .

If we look at Table 2, we find p-value of both level of perception and level of awareness shows that there are significant difference between male and female regarding the level of perception and the level of awareness of cybercrime at 5% level of significance. It indicates that the male and female of B.Ed. students have different level of perception and awareness of cybercrime .These findings do not support null hypothesis 1 and null hypothesis 2.Therefore, we do reject the null hypotheses.

**Table-2 .Level of perception and awareness –gender**

| LEVEL | GENDER | N | MEAN | SD | MEAN DIFFERENCE | Z-VALUE | P-VALUE | REMARK |
|---|---|---|---|---|---|---|---|---|
| Level of Perception | Male | 120 | 3.98 | 0.452 | | | | |
| | Female | 80 | 3.87 | 0.436 | -0.118 | -2.362 | 0.019 | significant |
| Level of Awareness | Male | 120 | 3.40 | 0.597 | | | | |
| | Female | 80 | 3.22 | 0.723 | -0.187 | -2.583 | 0.010 | significant |

Table 3, reveals that the p-value of both level i.e., level of perception and level of awareness are significant differences among students in different age groups relating to their perception and awareness of cybercrime at 1% level of significance .It indicates that there are significant difference between young people's perception and their age as well as between awareness of cybercrime and their age .Therefore ,we do reject the null hypothesis 3 and null hypothesis4

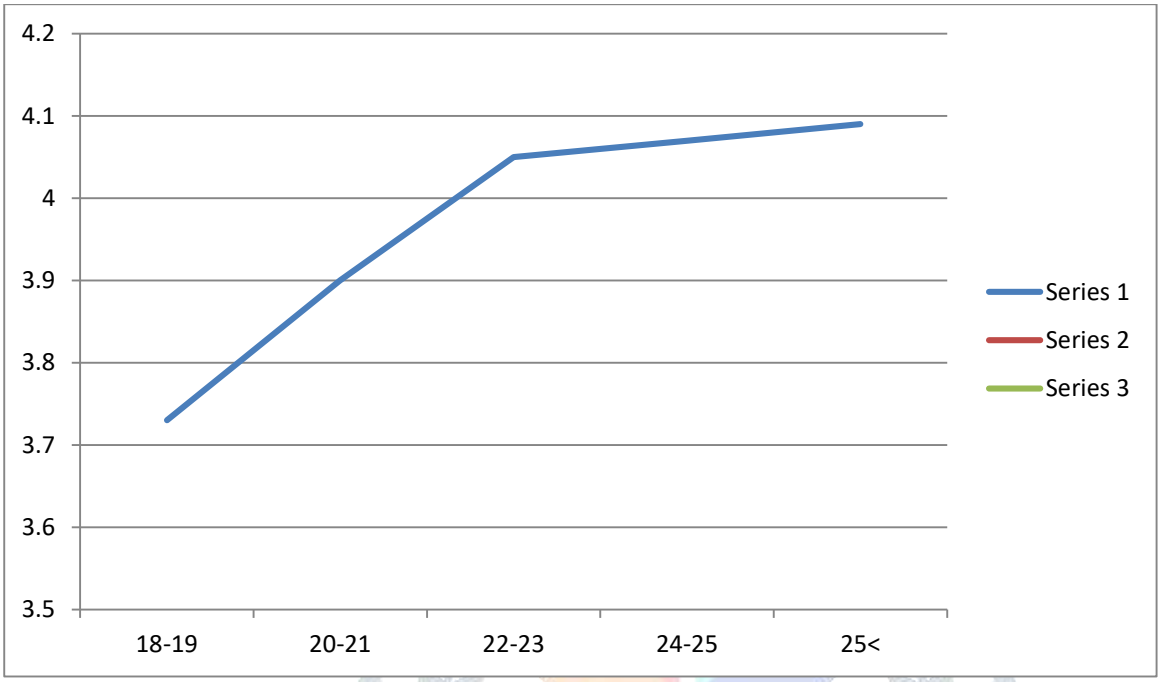
**Table-3.Level of perception and awareness-Age**

| LEVEL | VARIABLE | F | P-VALUE | REMARK |
|---|---|---|---|---|
| Level of perception | Age | 6.880 | 0.000 | Significant |
| Level of Awareness | Age | 4.508 | 0.001 | Significant |

All the four null hypotheses are rejected .Therefore we could say that there are significant relationship between awareness age and gender. similarly ,there are significant relationship between perception age and gender.

Figure 1 reveals that the perception of different age groups are statistically varied between students in the age group of 18-19 years(M=3.73) and those of 22-23 years (M=4.05) and 24-25years (M=4.07).Students in the age group of 22-23 years and 24-25 years reported significantly higher perception on cybercrime compared to students of 18-19 years. There are no significant differences between other groups.

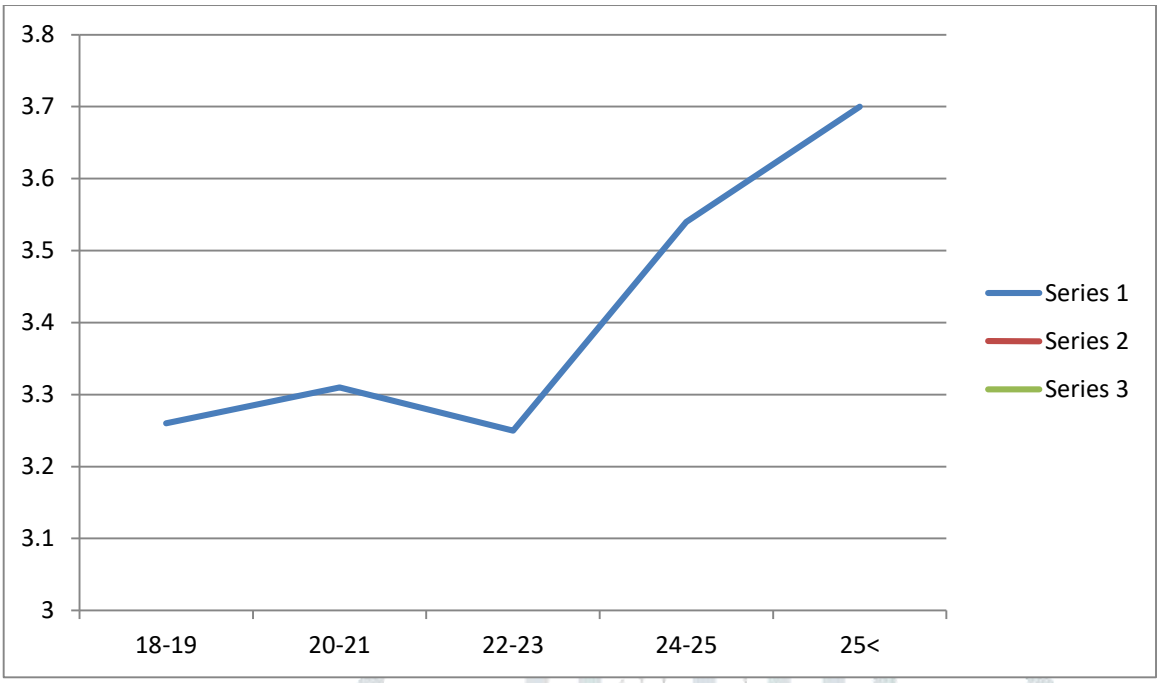
**Fig.1 Relationship between perception and age**




Age group(years)

Figure 2 reveals that the awareness of different age groups are statistically varied between students of 18-19 years(M=3.26) and those of 24-25 years (M=3.25) also reveals significant differences with those of 24-25 years and more than 25 years. The result reports that students in the age group 24-25 years and more than 25 years have significant higher awareness of cybercrime compared to those of 18-23 years .There are no significant differences between other groups.

**Fig.2-Relationship between awareness and age**




Age group(years)

We believe that there is a positive relationship between awareness and perception of cybercrime. Therefore, we examine the Pearson correlation between them If we look at the Table- 4.It shows that there is a positive correlation between respondents perception level and awareness level of cybercrime at 1%level of significance. This suggests , the higher the level of awareness, the higher the level of perception.

**Table-4.Correlation between Level of perception and Level of awareness of Cybercrime**

| | | Perception of cybercrime | Awareness of cybercrime |
|---|---|---|---|
| **Perception of cybercrime** | Pearson correlation | 1 | 0.281** |
| | Sig.(2-tailed) | | 0.000 |
| | N | 200 | 200 |
| **Awareness on cybercrime** | | | |
| | Pearson correlation | 0.281 | 1 |
| | Sig.(2-tailed) | 0.000 | |
| | N | 200 | 200 |

## Conclusion

This study concludes that gender and age have significant influences on the level of perception and awareness of cybercrime. We test two hypotheses on the relationships between perception and age and gender. We also test two hypotheses on relationship between awareness and age and gender. All four null hypotheses are rejected in this study. We find male students are more aware than female students about cybercrime. For the age group, we find students in the age group of 23-25 years have significantly higher perception of cybercrime than those of 18-19 years and the age group of 24-25 and more than 25 years have significantly higher awareness of cybercrime compared to those 18-23

years ,This suggests students with greater awareness and perceptions of cybercrime are more cautious about the same . More revealing fact is that perception and awareness are positively correlated at 1% level of significance .The findings indicate that the level of awareness and level of perception of the respondents regarding cybercrime are equal. The study suggests having higher knowledge of cybercrime also have better awareness of the cybercrime. Curtis and colwell (2000; Atkinson et al., 2009) mentioned that unambiguous knowledge of cybercrime would help young people in preventing and avoiding this delinquency. By education, students can develop positive attitude towards cyberspace (Wang et al .,2008). Thus the result of this study is to some extent similar to the findings of previous studies.

This study recommends necessary policy measures to be taken by the learning institutions including B.Ed. to prevent alarming cybercrime. Educating young people with some knowledge on cybercrime (given in this paper) would help increase their level of awareness and also perception on cybercrime.

## References

Aris, A., R. Zainuddin, R. Kamarudin and Z.M. Daud, 2004. The Impact of students' background and attitudes on their computer skills: A case study on three selected secondary schools in Segamat, Johar. Proceeding of the Seminar Hasil Penyelidikan Peringkat Kebangsaan, (PPK'04), pp:249-261.

Chen, C.C., B.D. Medlin and R.S. Shaw, 2008. A cross-cultural investigation of situational information security awareness programs. Inform. Manage. Comput, Security, 16:360-376.

Choi, K., 2008. Structural equation modeling assessment of key causal factors in computer crime victimization. Ph.D dissertation, Indianan University of Pennsylvania, USA.

Colfer, E., 2007. Online privacy and people's awareness: A Study of Irish students. MSc Thesis, School of Science, Worldford Institute of Technology, Ireland.

Curtis, P.A. and L. Colwell, 2000. Cybercrime: The next challenge: An overview of the challenges faced by law enforcement while investigating computer crimes in the year 2000 and beyond. School of Law.

Hasan, M.S., N. Omar and Z.S. Hossain, 2015. Corporate attributes and market capitalization: Evidence from Bangladesh. AESTImATIO IED Int. J. Finance, 11:92-105.

Sembok, T.M., 2003. Ethics of information technology. Proceedings of the Regional meeting on Ethics of Science and Technology, RUSHAP, UNESCO, Nov. 5-7, Bangkok.

Shariff, S. And S. Deni, 2005. An exploratory study of level of awarenss and perception towards computer ethics among it educators of institutes of higher learning in Lembah Klang. Technical Report, University Teknologi MARA, Malaysia.

## Web References

http://en.wikipedia.org/wiki/Computer_crime

http://www.thewindowsclub.com/types-cybercrime

https://ncdrc.res.in/national-cyber-crime-reference-hand-book

http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india.html

http://in.norton.com/

http://ncrb.gov.in/

http://www.ncpc.org