

CHAPTER - 1

INTRODUCTION

The internet, as we know, has grown rapidly over the last decade. It has given rise to many new avenues in every field like education, entertainment, business, or sports. However with every boon there is a curse too. This curse is cyber crime- illegal activities committed over the internet. The internet, along with its advantages, has also exposed us to security risks. Computers today are being misused for unlawful activities like e-mail espionage, credit card fraud, spam, software piracy, spreading of viruses, and so on, which invade our privacy and offend our senses. Criminal activities over internet are on the rise. Cyber crime is a term used broadly to describe criminal activity in which computer or network are a tool, a target or a place of criminal activity. These categories are not exclusive and many activities can be characterised as falling in one or more categories. Although the term cyber crime is usually restricted to describing criminal activity in which the computers or networks are used to enable the illicit activity. Also in teaching and learning, the use of computer is inevitable and of course one should face the risk factors also attached to it. Hence, the awareness on cybercrime is very much needed for learners and also for teachers. Therefore, an attempt has been made to study the awareness on cyber crime of teacher trainees.

1.1 MEANING OF CRIME

Crime is a public wrong. It is an act of offense which violates the law of the state and is strongly disapproved by the society. Crime is defined as acts or omissions forbidden by law that can be punished by imprisonment or fine. Murder, robbery, burglary, rape, drunken driving, child neglect and failure to pay taxes are examples of crimes. The term crime is derived from the Latin word “crimen” meaning offence and also a wrong-doer. Crime is considered as an anti-social behaviour.

Each society may define crime in a different perspective. A crime may be legal or illegal. Illegal and punishable crime is the violation of any rule of

administration or law of the state or practice of any wrongdoing and harmful to self or against third parties, provided in criminal law. Legal and not punish-able crime is all acts of self defence.

1.2 CYBER CRIME

The word Cyber Crime consists of two words: “Cyber” which donates virtual space and “Crime” which donates as an act which is an offence against the society. It is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act. Cyber crime is the most prevalent crime playing a devastating role in Modern India. Not only the criminals are causing enormous losses to the society and the government but are also able to conceal their identity to a great extent. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation it can be said that, Cyber crime includes any illegal activity where computer or internet is either a tool or target or both.

The Indian Legislature doesn't provide the exact definition of Cyber crime in any statute, even the Information Technology Act, 2000; which deals with cyber crime doesn't defined the term of cyber crime. However in general the term cybercrime means any illegal activity which is carried over or with the help of internet or computers.

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes 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, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)”.

We do not have any precise definition of cyber crime; however following is the general definitions of term cyber crime:

The Oxford Dictionary defined the term cyber crime as “Criminal activities carried out by means of computers or the Internet.”

“Cyber crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them”

Professor **S.T. Viswanathan** has given three definitions in his book The Indian Cyber Laws with Cyber Glossary is as follows –

1. Any illegal action in which a computer is the tool or object of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,
2. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,
3. Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data.

1.3 CHARACTERISTICS OF CYBERCRIME

- **Specialized Knowledge:** To commit a cybercrime a person needs to be having a good knowledge about the computers and internet. Many a times cybercrime is committed by the very educated people as they have the accurate knowledge about the same. And at times it becomes very hard to trace them.
- **Geographical Challenges:** Since the crime can be done globally without being physically present at the place. The distance does not matter in cybercrimes. A person sitting in India can target a person sitting in Australia.
- **Virtual World:** The act of cyber crime takes place in the cyber space and the criminal who is committing this act is physically outside the cyber space. Every activity of the criminal while committing that crime is done over the virtual world.
- **Collection of Evidence:** It is very difficult to collect evidence of cyber crime and prove them in court of law due to the nature of cyber crime. The criminal in cyber crime invoke jurisdiction of several countries while

committing the cyber crime and at the same time he is sitting some place safe where he is not traceable.

- **Magnitude of crime unimaginable:** The cyber crime has the potential of causing injury and loss of life to an extent which cannot be imagined. The offences like cyber terrorism, cyber pornography etc has wide reach and it can destroy the websites, steal data of the companies in no time.

1.4 CLASSIFICATION OF CYBERCRIME

Given below is the list of cyber crimes, some of them are widely spread and some are not prevalent on larger scale.

1.4.a Cyber Pornography

The word 'Pornography' derived from Greek words 'Porne' and 'Graphein' means writing about prostitutes, or referred to any work of art or literature dealing with sex and sexual themes. Defining the term pornography is very difficult and it does not have any specific definition in the eyes of law as every country has their own customs and tradition. The act of pornography in some countries is legal but in some it is illegal and punishable. Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. The advent of internet in the world has started the new chapter in the porn industry. The porn industry find perfect place in internet to spread pornographic material all over the world

1.4.b Cyber Stalking

Stalking in general means behaviour of harassing or threatening the other person. Cyber Stalking is an extension of physical form of stalking, which is committed over the online medium with the use of information Technology. In cyber stalking the internet, e-mail, chat rooms etc. are used to stalk another person. It include the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass.

The internet has wide reach, the way we communicate online, the personal data of individual and other information is easily accessed by the offenders through the internet medium, and this makes the individual vulnerable to the offence such as cyber stalking. The victim is normally a person who is less thorough regarding internet services and its applications. The stalker is generally a person who is a paranoid with no self-esteem. But the traits differ from one stalker to another. Some harass to seek revenge or some do so for their own pleasure. While some just to do it for playing a mischief.

1.4.c Cyber Terrorism

The terrorism phenomenon is very complex issue in the current generation. The attacks of terrorist on the mankind have increased rapidly in last decade. Cyber-terrorism involves highly targeted efforts made with the intention of terrorism. It is an emerging threat that has the potential to cause serious damage.

According to **NATO (2008)**, cyber terrorism is “a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal.”

In Present scenario the aim of the terrorist organization is to destroy the communication, infrastructure, transportation and financial network of the country through the use of computers and networks to create fear in the minds of the people, as every country in the world is heavily depend on the technology. Recent attacks in India as well as in world have proved that the terrorist are also utilizing the computers and networking to carryout terrorist attacks.

1.4.d Hacking

Hacking is labelled as amongst the most serious of all cyber crimes. It is said that hacking erodes the faith of people in information technology and the Internet. Hacking a computer simply implies getting into another’s computer without permission. Gaining unlawful access to another’s computer is hacking. It is equivalent to phone-tapping. Hackers see the weakness in the target computer programme and then find ways to enter and access therein. Anti hacking tools such as the ‘Firewall’ technology and intrusion detection systems are preventive measures that can be taken to protect a computer from being hacked.

Hacking is done to spy into others computer systems and for stealing information/data residing therein. Hacking is done at the country level too. Frequently, Pakistani hackers are accused of hacking Indian web-sites. For instance, the web-site of SEBI (Stock Exchange Board of India) was hacked whereby a link to a pornographic web-site was inserted.

1.4.e Cyber Crimes related to Finance

The Price Waterhouse Coopers organization, which deals with the economic crime survey, has defined economic crime in cyber world as “an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It’s only a cyber crime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one.” In the background of the recent incidents of cyber crime on multinational companies and financial institutions, a greater number of organizations are becoming victims of cyber crime. One potential reason that may explain this sudden rise in cyber crime is the rise in the volume of e-business, greater penetration of internet and e-commerce.

1.4.f Phishing and Vishing

In computing, phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message. The term phishing arises from the use of increasingly sophisticated lures to “fish” for ‘users’ financial information and passwords. The act of sending an e-mail to a user falsely claiming to be established legitimate enterprises in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Website where they are asked to update personal information, such as passwords, credit card, social security, and bank account numbers, that the legitimate organization already has. The Website, however, is bogus and set up only to steal the user’s information. The motive behind phishing is that people will share their credit

card information, passwords, bank account numbers and other information thinking that they are sharing their information to the legitimate organization but in real they are sharing their information with bogus website or organization which is going to steal their money.

Vishing is also alike phishing; it is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial information from the public for the purpose of financial reward. The term is a combination of “voice” and phishing. Vishing exploits the public’s trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the bill payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

1.4.g Data Theft

Data and information are valuable assets in this digital age. Business secrets, technical knowhow, designs, music, films, books, personal data including usernames, credit card numbers and passwords, are some forms of property that drive the information economy. Money, time, effort and creativity go into the creation and compilation of data and information. Stealing of data and information through hacking and other means, is the most prevalent cyber crime. Applying the law of theft to information and data is a comedy of sorts. When information and data are encapsulated in a tangible form, for instance, stored in a floppy, CD, or pen-drive, they are part of moveable property and hence can be said to be stolen if the medium (floppy, CD, or pen-drive) is moved without the consent of the person in possession. Also, if the computer itself is stolen, since data and information are a part thereof, they too can be said to be stolen. However, in the online environment, where data and information are intangible i.e. mere combinations of binary numbers, the legal definition of ‘theft’ falls short. Stealing of data and information online is no ‘theft’ in the eyes of section 378 I.P.C. In this sense, the expression ‘data theft’ is a misnomer from the legal perspective. It is an expression of common parlance. For instance, if an

employee dishonestly and without the consent of his employer sends/transmits critical data through e-mail to an e-mail account belonging to him or another, it would not amount to theft under the I.P.C. However, if he were to store the data in a CD and take it away, it would amount to theft. The I.T. (Amendment) Act, 2008 however brings into existence the offence of 'data theft' (even though not encapsulated in a medium such as CD, computer pen-drive or floppy).

1.4.h Data Diddling

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating; recording, encoding, examining, checking, converting, or transmitting data. This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Electricity companies are the one who mostly suffer due to this kind of crime in India. The NDMC EC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

1.4.i Salami Attacks

A salami attack is a series of minor data security attack that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can be considered a salami attack. Crimes involving salami attacks typically difficult to detect and trace. These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. A bank employee inserts a program, into the bank's servers, that

deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

1.4.j E-mail Bombing

In internet usage, an e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelms the server. E-mail bombing refers to sending a large number of e-mails to the victim resulting in the victim's e-mail account (In case of Individual) or mail servers (in case of a company or an e-mail service provider) crashing. In one case, a foreigner who had been residing in Shimla, India for almost thirty years wanted to avail of a scheme introduced by the Shimla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Shimla Housing Board and repeatedly kept sending e-mails till their servers crashed. E-mail bombing is characterized by abusers repeatedly sending an e-mail message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources.

1.4.k E-mail spamming

It is a variant of bombing; it refers to sending e-mail to hundreds or thousands of users. E-mail spamming can be made worse if recipients reply to the e-mail, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users.

1.4.l Software Piracy

Copyright subsists throughout India in the following classes of works:-

- Original literary, dramatic and musical;
- Artistic works;

- Computer Programme;
- Cinematograph films; and
- Sound recording.

In India, the Copyright Act, 1957 governs computer software. The definition of 'literary works' specifically includes computer programmes, tables and compilations including computer databases. Some common methods of copyright infringement in relation to computer software as stated are:—

- Reproducing the original owner's software and packaging of that software, so that purchasers are deliberately misled into believing that the product they are buying is genuine software.
- Reproducing or 'burning' the original owner's software onto a blank CD, where no attempt is made to represent that the copy is genuine.
- Reproducing a number of the owner's programme on a single CDROM, known as a 'compilation' CD.

Another form of piracy that is assuming alarming shape in the information technology age is that of internet piracy when software is downloaded from the Internet or distributed via internet without the permission of the copyright owner.

1.4.m E-mail Spoofing

E-mail spoofing is a term used to describe fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. By changing certain properties of the e-mail, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. It is often associated with website spoofing which mimic an actual, well-known website but are run by another party either with fraudulent intentions or as a means of criticism of the organisation's activities.

1.4.n.SMS spoofing

SMS spoofing is like e-mail spoofing, which looks to originate from your acquainted number but in reality it is spoofed, and send from some evil minded individual. We can take this by an example. Suppose if a woman receive a Short Messaging Service (SMS) in her cellphone in the middle of a night from the mobile of her spouse asking her to bring cash as he has met with an accident. The chances are that she would check the mobile number and if she confirms that the cell is her husband's then she would rush out with cash. If this could be the response then the chances are that she is not aware of "Mobile Spoofing". Using web-based software, a cyber criminal could send anyone a message from any person's cell without even touching his mobile and no cellular service provider can say that it was a spoofed or faked one.

1.4.o Online illegal selling(Dark web)

Here criminal performs illegal activities such as selling illegal weapons, smuggled goods, drugs, or person's information to the person who is present on an illegal shopping portal. It promotes black marketing.

1.5 CAUSES OF CYBERCRIME

Cybercrime targets rich people or rich organizations like casinos, banks, and financial firms where a tremendous amount of money comes daily and hackers can easily hack sensitive information. It is an easy way to make big money. Catching these criminals is difficult. The number of cybercrimes across the globe is increasing on a daily basis. Various laws are required to safeguard the use of computers against various vulnerabilities. Following are the various reasons listed for the vulnerability of computers:

- **Capacity to store data in comparatively small space-** One unique characteristic of a computer is that it can store your data in a considerable small space. This makes it easy for the criminal to steal our data from the system and they use it for their own profit.

- **Negligence-** This is a characteristic of human conduct. While protecting the computer system we can make any negligence which makes it easy for the criminal to have access and control over your computer system.
- **Easy to access-** Due to the complex technology used, it is difficult to protect a computer system from unauthorized access. Hackers can steal information that can fool biometric systems easily and bypass firewalls need to be used to get past many security systems.
- **Loss of evidence-** The data with the crime can be destroyed easily. So while investigating a cybercrime, loss of evidence is a very common issue.

1.6 MEANING OF AWARENESS

Awareness in general means, knowledgeable being conscious; cognizant, informed alert. Awareness is the state or ability to perceive, to feel, or to be conscious of events, objects, or sensory patterns. The possessor of any knowledge must contain awareness but mere awareness does not contain any type of knowledge. More broadly, it is the state or quality of being aware of something.

1. One frequent meaning of awareness in education is Knowledge from milieu without direct teaching. For example, Public awareness of cancer, HIV/ AIDS Awareness or Nutritional awareness. This can be referred to as awareness about. Awareness may also refer to public or common knowledge or understanding about a social, scientific, or political issue.

2. In psychology, the most popular meaning of awareness is awareness as self-perceptions. For example- when we say awareness of Body, Emotional Awareness, awareness of self or strength awareness. This can be described as awareness of. This can be seen as sensitivity to oneself. In all these awareness, it is a kind of self-awareness (awareness of own individuality). Here awareness denotes “unique perception”. Unique perception is completely subjective. It does not require great knowledge. Unique perception of all is considered a “higher” form of awareness.

3. The third meaning of awareness is Awareness of ability to deal with. Some awareness tests are conducted to find out the ability to deal with specific situation, and tasks. For example-Computer Awareness Test. Again, the assumption is that the populations under consideration possess the ability or skill.

1.7 SIGNIFICANCE OF THE STUDY

Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Today e-mail and websites have become the preferred means of communication. This includes not only educational and informative material but also information that might be undesirable or anti-social. Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. In teaching-learning process, the use of internet is inevitable. It also helps a teacher and student to update their knowledge by getting the new information about new researches, new techniques etc. A teacher and a student can also get connected outside the classroom through the internet. And when they get the benefits of internet then of course they should face the risk factors also attached to it. Hence, the awareness on cyber crime is very much needed for the learners and also for teachers, so that they can prevent to face the unexpected problems or cyber crimes such as hacking, phishing, spam, computer viruses, sabotage, wire fraud, ATM fraud, internet fraud, identity theft etc. and they can take the appropriate measures to sort out these problems. Today's B.Ed. students are the future teachers. They have the responsibility to educate the student's community against Cyber crimes. If they are sound in the knowledge over cyber crimes then they will teach their students too.

Now-a-days cybercrime has increased; the Central government has taken steps to spread awareness about cybercrimes, issue of alerts / advisories, capacity building / training of law enforcement personnel / prosecutors / judicial officers, improving cyber forensic facilities etc. Students are the future of our nation. There is a need of raising awareness about cybercrime among teachers and students. Teachers are the nation builders; if they are aware about these crimes

automatically their knowledge will get transferred to their students. This is the best way of raising awareness about cybercrimes among students. Cybercrime shows no sign of slowing down so, there is a huge need of raising awareness among new generation. It increases day by day, if the youth of our society already know about these cybercrimes, they will never get trapped in it. Hence, the awareness on cybercrime is very much needed for the learners and also for teachers, so that they can prevent to face the unexpected problems or cybercrimes such as hacking, phishing, spam, computer viruses, sabotage, wire fraud, ATM fraud, internet fraud, identity theft etc. The present study will be conducted to find out the cybercrime awareness among teacher trainees, so that it could be known that whether they are aware about the cybercrimes or not.

1.8 STATEMENT OF THE PROBLEM

The problem undertaken for the present research is stated as:

“A STUDY OF CYBER CRIME AWARENESS AMONG TEACHER TRAINEES IN RELATION TO THEIR GENDER AND LOCALITY IN JAMMU DISTRICT”.

1.9 OPERATIONAL DEFINITIONS OF KEY TERM

- **CRIME:**-Crime is the violation of any rule of administration or law of the state or practice of any wrong doing and harmful to self or against third parties.
- **CYBERCRIME:**-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, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)”.
▪ **AWARENESS:**-In the present study, awareness is the state or condition of being aware i.e. having knowledge and consciousness of cyber crime.
- **TEACHER TRAINEES:**- Teacher trainees are one’s who are doing B.Ed to become trained teachers.

1.10 OBJECTIVES OF THE PRESENT STUDY

The objectives of the present study were:

- To find the difference in the awareness of cybercrime among B.Ed. teacher trainees with respect to their gender (male and female).
- To find the difference in the awareness of cybercrime among B.Ed. teacher trainees with respect to their locality (urban and rural).
- To find the difference in the awareness of cybercrime among B.Ed. teacher trainees on the basis of interactional effect of gender (male and female) and locality (urban and rural).

1.11 HYPOTHESES OF THE STUDY

- There is no significant difference in the awareness of cybercrime among B.Ed. teacher trainees with respect to their gender (male and female).
- There is no significant difference in the awareness of cybercrime among B.Ed. teacher trainees with respect to their locality (urban and rural).
- There is no significant difference in the awareness of cybercrime among B.Ed. teacher trainees on the basis of interactional effect of gender (male and female) and locality (urban and rural).

1.12 DELIMITATIONS OF THE STUDY

Due to lack of time and other resources, the study was carried out with certain delimitations:

- The study was confined to Jammu District only.
- The sample was confined to 200 B.Ed. teacher trainees only.
- Only 5 colleges were covered in the present study.

CHAPTER - 2

REVIEW OF RELATED LITERATURE

Review of related literature in any field of investigation has become an inevitable part of research work. It surveys books, scholarly articles, and any other sources relevant to a particular issue, area of research, of theory and by doing so, provides a description, summary and critical evaluation of these works in relation to the research problem being investigated. Literature review is designed to provide an overview of sources we have explored while researching a particular topic and to demonstrate to the readers how our research fits within a larger field of study. Best (1977) is of the strong opinion that ‘familiarity with the literature in any problem area helps the students to discover what is already known, what others have attempted to find out, what method of approach have been promising or disappointing and what problems remain to be solved.’

Literature review is done with the purpose of helping the research worker to develop a thorough understanding and insight into the work already done and the areas left untouched or unexplored. It also helps to avoid unnecessary duplication and may help to progress towards the solution of new problem. The present study is not the first work in this field but it is an attempt to add little more in the vast field of educational research, it is presumed that the survey of related literature will make the present investigation more direct and to the point. The investigator has made an earnest effort to find out and study the researches related to topic under investigation concluded by the various researchers and scholars. Available studies which are directly or indirectly related have been reported as follows:

Jamil and Khan (2011) while comparing the data protection act in India with that of European countries have concluded that the Indian cyberlaws are very poor and it is very necessary to actually bring in the appropriate cyber law and awareness about them. There is not much of awareness regarding protecting the data. There is a continuous rise in cybercrime as there is huge population but lesser resources to manage the population and the cybercrimes that take place.

Arpana., and Chouhan,M. (2012) conducted a study regarding awareness of cyber crime in tricity to find out awareness among different respondents on the issue of Cyber Crime. In conducting the research, the author used SPSS 13.0 software program and took the hypothesis that there is no association between Respondents Occupation and the level of Cyber Crime Awareness. The results revealed that 33% Student, 13% IT Professional, 33% Businessman and 13% Advocate respondents think that major drawback, which prevent Cyber Crime from being solved in India is Lack of awareness among people. 58% student, 42% IT Professionals,37% businessman and 61% advocates respondents are of view that Law enforcement agencies are not fully equipped due to which cybercrimes occur. Rest 9% students, 45% IT Professional, 30% Businessman and 26% advocate respondents feels that all the factors are responsible which prevent cyber crime to be solved in India.

Mehta,S., and Singh,V. (2013) conducted a study of awareness about cyberlaws in the Indian society and found that there is a significant difference between the awareness level of male and female users of internet services. It was also established that the male netizens are more aware for Indian cyberlaws in comparison to their female counterparts. On the similar lines, there exits a significant difference between the awareness level of employee-users and non-employee-users of internet services and it was found that the employed users are more aware for Indian cyberlaws in comparison to non-employees.

Goel,U. (2014) conducted a study on ‘Awareness among B.Ed training teachers towards cybercrime’. For this purpose a sample of 120 B.Ed students was selected from Sonipat district. The data was collected by Cyber Crime Awareness Scale (CCAS-RS) developed by Dr. S. Rajasekar. The study reveals that there is no significant difference towards cyber-crime awareness among

boys and girls. There is no significant difference towards cyber-crime awareness among rural boys and girls. There is significant difference towards cyber-crime awareness among urban boys and girls, science and art boys and science and art girls. The result shows that awareness towards cyber-crime is not significantly affected by Gender, whether it is male or female but it is significantly affected by area, whether it is rural or urban and stream, whether it is science or art.

Yu,S.(2014) conducted an exploratory study on ‘Fear of cyber crime among college students in the United States’. Precisely, four cyber crimes were chosen, including online scam, cyber bullying, digital piracy, and computer virus. This study was the first study that takes into account all four types of cyber crime concurrently. The results of the study revealed that the Computer virus is the most feared cyber crime, followed by online scam and cyber bullying. It also has the highest perceived risk, followed by online scam and cyber bullying. Computer virus also entails the most victimization experience, followed by cyber bullying and online scam. Cyber bullying is perceived as the most serious cyber crime, followed by online scam and computer virus. Digital piracy has the lowest score on all four variables. It also seems these four cyber crimes do not generate much fear, perceived risk, or victimization experience. Only perceived crime seriousness is relatively higher.

Manasrah et al. (2015) conducted a case study of Jordan ‘Towards improving university students awareness of spam email and cybercrime’ .They tried to inspect the awareness and the attitude of college students in three main Universities in Jordan. As total, 600 students from educational, science and IT colleges were surveyed. They investigated the main factors as they thought it could attract the students to open and read the spam emails that could lead them to be a victim of cybercrimes. These factors are technological, social, economical and religious. The results showed that some of the educational major participants seldom use their email accounts, while others have some knowledge on spam emails and cybercrimes, yet they may get stimulated to follow certain emails. Those participants are more vulnerable to cybercrimes.

Hasan et al.,(2015) conducted a survey to analyze the cybercrime awareness in Malaysia and found that female students are more aware of cybercrime as compared to male students.

Ismailova,R. and Muhametjanova,G. (2016) in their study on ‘Cyber crime risk awareness in Kyrgyz Republic’ found that despite the huge number of reports about computer crimes in the web, the knowledge about cybercrime is quite low and students are mostly not aware of many aspects of computer crime. Analysis was done to determine dependence of information security awareness rate on computer literacy rate and the education field of students and it was concluded that although information technology is of wide usage, the information security topics need to be taught to prevent them from becoming victims of cyber crime.

Mocha,A.(2017) in her study on ‘Awareness of Cyber Crime and Security’ attempts to analyze the awareness of cyber crime among internet users with different age groups and educational qualifications and finds that there is a relationship exists between the age groups and educational qualification of the respondents. She further concluded that 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.

Punjabi,R. (2019) conducted a study on ‘Cyber crime awareness among B.Ed. students’ to check the awareness level and to find out the preventive measures the students use to prevent cybercrimes. Survey method was used to collect the data. The results revealed that almost all B.Ed. students have internet on their mobile handset, have social networking account (Face book, LinkedIn, yahoo, Google plus) and install different android applications. Majority of respondents have stopped shopping online, as they experienced hanging up of their device due to Virus and used antivirus software to protect it. Majority of B.Ed. students use mobile frequently for the online transaction, but they avoid disclosing their personal details and have stopped shopping online as they agreed that it leads to hacking of one’s account which showed that they are aware of cybercrimes. They also agreed that women and children are more prone

to Cybercrime and some have come across illegal activities like Stalking, hacking, bullying and hanging up of their device.

Zwilling et al.,(2020) conducted a comparative study on cyber security awareness, knowledge and behaviour among individuals in general and across four countries: Israel, Slovenia, Poland and Turkey in particular and found that internet users possess adequate cyber threat awareness but apply only minimal protective measures usually relatively common and simple ones. The study findings also show that higher cyber knowledge is connected to the level of cyber awareness, beyond the differences in respondent country or gender.

Alharbi,T. and Tassaddiq,A.(2021) investigated and evaluated the level of cyber-security awareness and user compliance among undergraduate students at Majmaah University using a scientific questionnaire based on several safety factors for the use of the Internet and found that most of the participants were unaware of the fundamental concept of cyber-security and did not know how to manage their data, even though 92% of them had attended a formal security awareness program.

Chaudhari et al., (2021) in their study ‘To assess the awareness regarding cyber crime and cyber security among undergraduate students from selected nursing institute of Nashik city’ revealed that undergraduate nursing students have significant score (15.68) of cybercrime and having poor knowledge of cyber safety. Also, there was a significance association found between cybercrime and cyber safety with their selected socio-demographic characteristics like age, gender, father occupation, mother occupation, monthly family income, Time spends on Internet, Internet use as, Awareness about cybercrime, feel safe while using Internet, knowledge about Hacking, known victims of cybercrime, cybercrime investigation cell.

Garba et al., (2022) conducted a study to identify the level of cyber-security awareness of students in Northeastern Nigeria. A quantitative approach was used for data collection and cyberbully, personal information, internet banking, internet addiction, and Self-protection were the items ask for cyber-security awareness level identification. Descriptive analysis was performed for initial result findings using SPSS and OriginPro for graphical design. The result shows

that the students have some basic knowledge of cybersecurity in an item like internet banking, while other items like cyberbully, self-protection and, internet addiction result show moderate awareness, the students' participation based on gender, males constitute 77.1% i.e. (N=340) and females constitute 22.9% i.e. (N=101).

CHAPTER – 3

METHODS AND PROCEDURE

For the study and solution of every problem in education, one has to undertake many steps in a well regulated order. After selecting a problem, research procedure has to be adopted for arriving at valid conclusions. The investigation is required to discuss and the selected sample and procedure employed.

The order of discussion of these aspects is given below:-

1. Population
2. Variables studied
3. Sampling
4. Selection of tool
5. Description of tool
6. Administration of tool
7. Scoring procedure
8. Statistical technique applied.

3.1 POPULATION

The population of the study consisted of B.Ed. teachers trainees of Jammu district and a representative sample from the population was selected by the investigator.

3.2 VARIABLES STUDIED

In the present study there are two independent variables and one dependent variable which are to be studied:-

a) Independent variable:

- i) Gender: Male and Female
- ii) Locality: Rural and Urban

b) Dependent Variable: Cyber crime Awareness Scale Scores

3.3 SAMPLING

Sampling is the basis of all statistical methodology of research. The investigator can never collect data from the whole population in any investigation. The investigator has to take selected groups of individuals who would represent the whole population and form the basis for making reference of certain population of facts. This is known as sampling. The size of sample varies from study to study, method and nature of population. It is easier, less time consuming than the whole population.

The sample is used in collecting the research data. So sampling is fundamental to all statistical methodology of research. A good sample will produce a result very much approaching the population and generalization would be effective. It is a tool, which enable us to draw conclusions about the characteristics of the population, after studying only those subjects that are included in a sample. Sampling is both advantageous and essential. It saves the investigator's time, money and energy.

In the present study, the sample of 200 teacher trainees was selected from 5 different B.Ed. colleges of Jammu by using simple random sampling technique. The researcher distributed the cyber crime awareness scale to the teacher trainees of B.Ed. colleges as listed in the table below:

Table 3.1 Showing the details of B.Ed. college selected.

S.No	Name of the College	Male	Female	Total
1	Govt. College of Education	20	20	40
2	Sher-e-Kashmir College of Education	20	20	40
3	B.N. College of Education	20	20	40
4	Sacred Heart College of Education	20	20	40
5	M.C. Khalsa College of Education	20	20	40
	Total	100	100	200

3.4 SELECTION OF TOOL

A tool is a device to collect information from the sample. The selection of a suitable instrument or tool is of vital importance for any successful research which depends upon the nature of the problem. It is the selection of the appropriate tool which enables the researcher to arrive at certain generalization about the problem.

For the present study, the investigator used the Cyber Crime Awareness Scale developed by Dr. S. Rajasekar based on Likert scale.

3.5 RELIABILITY AND VALIDITY

Reliability

The reliability of the Cyber Crime awareness scale was established by the split half method (odd-even numbered) using Pearson Product Moment correlation. This only gives the reliability of half scale and hence the coefficient of the reliability of the full scale was determined by using the Spearman- Brown prophecy formula and was found to be 0.76, which is high and therefore the scale is reliable.

Validity

The Cyber Crime awareness scale has construct validity as items were selected having the 't' values equal to or greater than 1.75 (Edwards,1975). Its intrinsic validity was found to be 0.87 and hence the scale is valid.

3.6 ADMINISTRATION OF TOOL

Before administering the scale, the investigator made everything clear to the B.Ed teacher trainees about the scale by explaining them how they should tick (√) mark about the statements related to Cyber Crime. No time was set. All precautions were taken to prevent discussions between students. Precaution was also taken to prevent coping. The sheets were collected, scoring was done on the basis prescribed procedure and raw scores were obtained.

3.7 SCORING PROCEDURE

After collection of data the first thing done was scoring. The following scheme was used for scoring the responses.

Nature of Statements	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
Positive	5	4	3	2	1
Negative	1	2	3	4	5

3.8 STATISTICAL TECHNIQUES USED

In present study, the investigator was concerned with following techniques:

In the present study, the statistical technique Two-way Analysis of variance with 2x2 factorial design was applied in order to study the study of Cyber Crime Awareness among Teacher Trainees belonging to different gender and locality.

CHAPTER – 4

ANALYSIS AND INTERPRETATION OF DATA

One of the most important step in any research project is the organization of analysis and interpretation of data. The tabulated data has no meaning unless it is analysed and interpreted by some suitable statistical technique so as to arrive at significant conclusion.

Analysis of data means studying the tabulated data in order to determine inherent facts or meanings. It involves the breaking up of the complex factors into simpler parts and putting them together for the purpose of the interpretation. The interpretation of data helps the investigator to analyse the same problem or the related problem with appropriate statistical techniques without wasting their labour. After the collection of data, it must be carefully edited, systematically analyzed, intelligently interpreted and rationally concluded.

The purpose of interpretation is essentially to know – what do the results show? What do they mean? What is their significance etc. So the interpretation is considered to be the most important step in the total procedure of research.

4.1 ASSUMPTIONS OF ANALYSIS OF VARIANCE

ANOVA is a powerful statistical technique or tool used to test the homogeneity of several means. It was developed by R.A. Fisher, an English Statistician in 1920's who was also considered to be the father of modern statistics. It is an economical method of testing significant differences between the means of two groups.

In its simplest form, the analysis of variances is used to test the significance of the differences between two or more groups. According to Fisher, "Analysis of variance (ANOVA) is the separation of variance ascribable to our group of causes from variance ascribable to other groups."

Following are the important assumptions of Analysis of variance :-

- 1) **Independence of Groups:-** It is assumed that the groups selected should be made up of randomly selected subjects and are independent.
- 2) **Homogeneity of variance :-** It is assumed that the population from which groups have been selected have equal variances. In symbols, it is presented as ,

$$\sigma^2_1 = \sigma^2_2 \dots\dots\dots \sigma^2_k$$

- 3) **Normality of Distribution :-** The sample selected from the population should have normal distribution.
- 4) **Additivity :-** It has been stated that the total variance is obtained due to sum of two or other sources of variances i.e. variations.

4.2 ADVANTAGES OF ANALYSIS OF VARIANCE

Following are the advantages of ANOVA :-

- 1) Analysis of variance helps to compare all the groups or any number of comparison in a single test.
- 2) It is time saving and also involves less risk of errors i.e. when we reject the null hypothesis at small variance to be significant at .05 level.
- 3) The results obtained through analysis of variance are understandable and interpretable.

- 4) It is a powerful statistical technique for testing significance of mean difference.
- 5) The analysis of variance is useful when there are more than two groups to be compared for testing significance of mean difference.

4.3 SELECTION OF THE STATISTICAL TECHNIQUE OF ANALYSIS

In the present investigation the investigator was interested to find out the difference among B.Ed. teachers trainees towards cyber crime.

In view of these consideration, the technique of two way ANOVA was used to realize the objectives of the study. The use of ANOVA was considered most appropriate technique.

4.4 ANALYSIS OF VARIANCE

In the present study, the two – way analysis of variance technique is applied to the data of awareness scores with the factorial design as 2x2 factorial matrices with cyber crime as criteria, which was studied in relation to different Gender (male and female) and locality (rural and urban).

4.5 GENERAL COMPUTATIONAL STEPS FOR COMPUTATION OF TWO WAY ANOVA

Following are the general computational steps employed in two way ANOVA

Step I. Correction or C = $\frac{(\sum X_T)^2}{N_T}$

Step II. Sum of squares for total (SS_T)

$$SS_T = \sum X_T^2 - C$$

Step III. Sum of squares for A (SS_A)

$$SS_A = \frac{(\sum A_1)^2}{NA_1} + \frac{(\sum A_2)^2}{NA_2} - C$$

Step IV. Sum of squares for B (SS_B)

$$SS_B = \frac{(\sum B_1)^2}{NB_1} + \frac{(\sum B_2)^2}{NB_2} - C$$

Step V. Sum of squares for Between cells ($SS_{\text{Bet. cells}}$)

$$SS_{\text{Bet. cells}} = \frac{(\sum A_1 B_1)^2}{N_1} + \frac{(\sum A_1 B_2)^2}{N_2} + \frac{(\sum A_2 B_1)^2}{N_3} + \frac{(\sum A_2 B_2)^2}{N_4} - C$$

Step VI. Sum of squares for Interaction ($SS_{A \times B}$)

$$SS_{A \times B} = SS_{\text{Bet. cells}} - (SS_A + SS_B)$$

Step VII. Sum of squares for within (SS_W)

$$SS_W = SS_T - SS_{\text{Bet. cells}}$$

Summary of two – way ANOVA

Sources of variance	SS	DF	MS	F	Level of Significance
A (Columns)					
B (Rows)					
AxB (Columns & Rows)					
Within					

Table 4.1 Showing scores of awareness of B.Ed. teachers trainee towards cyber crime.

		GENDER		
		Female (A₁)	Male(A₂)	
LOCALITY	Rural (B₁)	112	129	
		104	111	
		108	105	
		99	120	
		106	110	
		135	113	
		112	106	
		128	122	
		99	124	
		100	123	
		$\Sigma A_1 B_1 = 1103$	$\Sigma A_2 B_1 = 1163$	$\Sigma B_1 = 2266$
	$N_1 = 10$	$N_3 = 10$	$NB_1 = 20$	

	Urban (B₂)	123	98	
		108	106	
		100	104	
		114	96	
		115	94	
		102	109	
		122	100	
		127	123	
		115	99	
		105	94	
		$\Sigma A_1 B_2 = 1131$	$\Sigma A_2 B_2 = 1023$	$\Sigma B_2 = 2154$
		$N_2 = 10$	$N_4 = 10$	$N B_2 = 20$
		$\Sigma A_1 = 2234$	$\Sigma A_2 = 2186$	$\Sigma X_T = 4420$
		$N A_1 = 20$	$N A_3 = 20$	$N_T = 40$

Table 4.2 : Showing Scores of Two Way ANOVA

		GENDER	
		(A₁) Female	(A₁) Male
LOCALITY (B)	B₁ Rural	12544	16641
		10816	12321
		11664	11025
		9801	14400
		11236	12100
		18225	12769
		12544	11236
		16384	14884
		9801	15376
		10000	15129
		$\Sigma A_1^2 B_1 = 123015$	$\Sigma A_2^2 B_1 = 135881$
		15129	9604

		11664	11236	
		10000	10816	
		12996	9216	
	B₂	13225	8836	
	Urban	10404	11881	
		14884	10000	
		16129	15129	
		13225	9801	
		11025	8836	
		$\Sigma A_1 B_2^2 = 128681$	$\Sigma A_1 B_2^2 = 105355$	
		$\Sigma A_1^2 = 251696$	$\Sigma A_2^2 = 241236$	$\Sigma X_T^2 = 492932$

Step I. Correction or C
$$C = \frac{(\Sigma X_T)^2}{N_T}$$

$$= \frac{(4420)^2}{40}$$

$$= \frac{19536400}{40} = 488410$$

Step II. Sum of squares for Total (SS_T)

$$SS_T = \Sigma X_T^2 - C$$

$$SS_T = 492932 - 488410$$

$$SS_T = 4522$$

Step III. Sum of squares for A (SS_A)

$$SS_A = \frac{(\Sigma A_1)^2}{NA_1} + \frac{(\Sigma A_2)^2}{NA_2} - C$$

$$= \frac{(2234)^2}{20} + \frac{(2186)^2}{20} - 488410$$

$$= \frac{4990756}{20} + \frac{4778596}{20} - 488410$$

$$= 249537.8 + 238929.8 - 488410$$

$$= 488467.6 - 488410$$

$$SS_A = 57.6$$

Step IV. Sum of squares for B(SS_B)

$$\begin{aligned} SS_B &= \frac{(\sum B_1)^2}{NB_1} + \frac{(\sum B_2)^2}{NB_2} + \frac{(\sum B_3)^2}{NB_3} - C \\ &= \frac{(2266)^2}{20} + \frac{(2154)^2}{20} - 488410 \\ &= \frac{5134756}{20} + \frac{4639716}{20} - 488410 \\ &= 256737.8 + 231985.8 - 488410 \\ &= 488723.6 - 488410 \end{aligned}$$

$$SS_B = 313.6$$

Step V. Sum of squares for Between cells (SS_{Bet.cells})

$$\begin{aligned} SS_{\text{Bet cells}} &= \frac{(\sum A_1 B_1)^2}{n_1} + \frac{(\sum A_1 B_2)^2}{n_2} + \frac{(\sum A_2 B_1)^2}{n_3} + \frac{(\sum A_2 B_2)^2}{n_4} - C \\ &= \frac{(1103)^2}{10} + \frac{(1131)^2}{10} + \frac{(1163)^2}{10} + \frac{(1023)^2}{10} - 488410 \\ &= \frac{1216609}{10} + \frac{1279161}{10} + \frac{1352569}{10} + \frac{1046529}{10} - 488410 \\ &= 121660.9 + 127916.1 + 135256.9 + 104652.9 - 488410 \\ &= 489486.8 - 488410 \end{aligned}$$

$$SS_{\text{Bet cells}} = 1076.8$$

Step VI. Sum of squares for interaction (SS_{AxB})

$$\begin{aligned} SS_{AxB} &= SS_{\text{Bet.cells}} - (SS_A + SS_B) \\ &= 1076.8 - (57.6 + 313.6) \\ &= 1076.8 - 371.2 \end{aligned}$$

$$SS_{AxB} = 705.6$$

Step VII. Sum of square for within (SS_w)

$$\begin{aligned} SS_w &= SS_T - SS_{\text{Bet.cells}} \\ &= 4522 - 1076.8 \\ &= 3445.2 \end{aligned}$$

Table 4.3 : Showing the summary of ANOVA for 2x2 Factorial Design

Source of variance	SS	Df	MS	F-ratio	Level of Significance
A (Gender)	57.6	1	57.6	0.60	Not significant
B (Locality)	313.6	1	313.6	3.27	Not significant
AxB	705.6	1	705.6	7.37	Significant
Within	3445.2	36	95.7		

Interpretation

The F- ratio for the factor ‘A’ Gender i.e. (Male and Female) came out to be 0.60 and the table values for significance are 4.11 and 7.39 at .05 and .01 level of significance against df 1 and 36 respectively. It means that there is no significant difference in the awareness of B.Ed. teachers trainee i.e. male and female teachers trainee towards cyber crime. Hence, hypothesis no. 1 stating that there is no significant difference in the awareness of B.Ed. teachers trainee i.e. male and female towards cyber crime stands accepted.

The F- ratio for the factor ‘B’ Locality i.e. (Rural and Urban) came out to be 3.27 and the table values for significance are 4.11 and 7.39 at 0.05 and 0.01 level of significance against df 1 and 36 respectively. It means that there is no significant difference in the awareness of B.Ed. teachers trainee belonging to different Locality i.e. (Rural and Urban) towards cyber crime. Hence, hypothesis no. 2 stating that there is significant difference in the awareness of B.Ed. teachers belonging to different Locality i.e. (rural and urban) towards cyber crime stands accepted.

The F-ratio for interaction AxB (Gender x Locality) has been found to be 7.37 which is more than the table value 4.11 at 0.05 level of significance. It indicates that under joint influence of gender (male and female) and locality (rural and urban) there is significant difference is seen in the awareness of B.Ed. teachers towards cyber crime. Hence, Hypothesis no. 3 i.e. stands rejected.

CHAPTER - 5

CONCLUSIONS, EDUCATIONAL IMPLICATIONS AND SUGGESTIONS FOR FURTHER RESEARCH

5.1 CONCLUSIONS

The following findings are drawn on the basis of study:

- 1) There is no significant difference in the awareness of B.Ed. teacher trainees belonging to different gender (Male and Female) towards cyber crime.
- 2) There is no significant difference in the awareness of B.Ed. teacher trainees belonging to different locality (Rural and Urban) towards cyber crime.

- 3) Significant difference is seen in the awareness of B.Ed. teacher trainees towards cyber crime under joint influence of gender (Male and Female) and locality (Rural and Urban).

5.2 EDUCATIONAL IMPLICATIONS

One basic objective of educational research is to improve the educational sector by implementing findings of the research studies in it. Therefore, if a research work does not have point of implication mentioned separately, it is not considered as research work of education.

Cyber crime awareness is required since computer is prevalent and versatile device. It acts as a nervous system for every advancement in the society. Teacher trainees should be aware of while using their e-mail accounts, while using their Credit or Debit cards in public places and they should sign out from their account without forgetting. Cyber security is what helps to prevent issues like data breaches, cyber attacks and identity theft. It is used to protect yourself and your data from unauthorized access, modification and deletion. Thus cyber awareness enables us to be a victim of cyber crimes. The level of Cyber crime awareness of teacher trainees should be developed through various awareness programs. If the teacher trainees are aware about cyber crimes then in future they will educate their students too. A unit regarding cyber crimes should be included in the B.Ed. curriculum. Symposiums and seminars regarding cyber crimes may be organised in colleges to create awareness. In schools and colleges, a separate subject on cyber crimes may be included to create awareness among students.

5.3 SUGGESTIONS FOR FURTHER RESEARCH

The present study has answered few questions but also led to some other questions. In the present study the investigator came across a number of issues on which work could be carried out in future.

Further research can be conducted on the line given below:-

- 1) The study was confined only to the sample of 200 B.Ed teacher trainees of Jammu district. Same type of work can be done on a large sample with more variables.

- 2) The present study cannot be final and comprehensive; more work can be done on different samples of different age groups.
- 3) The present study deals with teacher trainees, same type of work can be done on higher secondary school students, college students, university students and thus comparisons can be drawn.
- 4) The study can be carried out in other districts also like Kathua, Samba, etc.
- 5) Similar study may be conducted on some weaker sections of the society.

SUMMARY

SUPERVISOR

Dr. Rajinder Kour

Associate Professor

INVESTIGATOR

Sahira Choudhary

M.Ed. Student

**TOPIC: A STUDY OF CYBER CRIME AWARENESS
AMONG TEACHER TRAINEES IN RELATION TO
THEIR GENDER AND LOCALITY IN JAMMU
DISTRICT**

A) INTRODUCTION

The internet, as we know, has grown rapidly over the last decade. It has given rise to many new avenues in every field like education, entertainment, business, or sports. However with every boon there is a curse too. This curse is cyber crime- illegal activities committed over the internet. The internet, along with its advantages, has also exposed us to security risks. Computers today are being misused for unlawful activities like e-mail espionage, credit card fraud, spam, software piracy, spreading of viruses, and so on, which invade our privacy and offend our senses. Criminal activities over internet are on the rise. Cyber crime is a term used broadly to describe criminal activity in which computer or network are a tool, a target or a place of criminal activity. These categories are not exclusive and many activities can be characterised as falling in one or more categories. Although the term cyber crime is usually restricted to describing criminal activity in which the computers or networks are used to enable the illicit activity.

B) MEANING OF CRIME

Crime is a public wrong. It is an act of offense which violates the law of the state and is strongly disapproved by the society. Crime is defined as act or omission forbidden by law that can be punished by imprisonment or fine. Murder, robbery, burglary, rape, drunken driving, child neglect and failure to pay taxes are examples of crimes. The term crime is derived from the Latin word “crimen” meaning offence and also a wrong-doer. Crime is considered as an anti-social behaviour.

C) MEANING OF CYBERCRIME

The word Cyber Crime consists of two words: “Cyber” which donates virtual space and “Crime” which donates as an act which is an offence against the society. It is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act.

The Indian Legislature doesn't provide the exact definition of Cyber crime in any statute, even the Information Technology Act, 2000; which deals with cyber crime doesn't defined the term of cyber crime. However in general the term cybercrime means any illegal activity which is carried over or with the help of internet or computers.

Dr. Debarati Halder and **Dr. K. Jaishankar** define cybercrimes 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, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".

D) CHARACTERISTICS OF CYBERCRIME

- **Specialized Knowledge:** To commit a cybercrime a person needs to be having a good knowledge about the computers and internet. Many a times cybercrime is committed by the very educated people as they have the accurate knowledge about the same. And at times it becomes very hard to trace them.
- **Geographical Challenges:** Since the crime can be done globally without being physically present at the place. The distance does not matter in cybercrimes. A person sitting in India can target a person sitting in Australia.
- **Virtual World:** The act of cyber crime takes place in the cyber space and the criminal who is committing this act is physically outside the cyber space. Every activity of the criminal while committing that crime is done over the virtual world.
- **Collection of Evidence:** It is very difficult to collect evidence of cyber crime and prove them in court of law due to the nature of cyber crime. The criminal in cyber crime invoke jurisdiction of several countries while committing the cyber crime and at the same time he is sitting some place safe where he is not traceable.

- **Magnitude of crime unimaginable:** The cyber crime has the potential of causing injury and loss of life to an extent which cannot be imagined. The offences like cyber terrorism, cyber pornography etc has wide reach and it can destroy the websites, steal data of the companies in no time.

E) CLASSIFICATION OF CYBERCRIME

Given below is the list of cyber crimes, some of them are widely spread and some are not prevalent on larger scale.

- **Cyber Pornography**

The word ‘Pornography’ derived from Greek words ‘Porne’ and ‘Graphein’ means writing about prostitutes, or referred to any work of art or literature dealing with sex and sexual themes. Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials.

- **Cyber Stalking**

Stalking in general means behaviour of harassing or threatening the other person. Cyber Stalking is an extension of physical form of stalking, which is committed over the online medium with the use of information Technology. In cyber stalking the internet, e-mail, chat rooms etc. are used to stalk another person. It include the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass.

- **Cyber Terrorism**

The terrorism phenomenon is very complex issue in the current generation. The attacks of terrorist on the mankind have increased rapidly in last decade. Cyber-terrorism involves highly targeted efforts made with the intention of terrorism. It is an emerging threat that has the potential to cause serious damage.

According to **NATO (2008)**, cyber terrorism is “a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal.”

- **Hacking**

Hacking is labelled as amongst the most serious of all cyber crimes. It is said that hacking erodes the faith of people in information technology and the Internet. Hacking a computer simply implies getting into another’s computer without permission. Gaining unlawful access to another’s computer is hacking. It is equivalent to phone-tapping. Hackers see the weakness in the target computer programme and then find ways to enter and access therein.

- **Cyber Crimes related to Finance**

The Price Waterhouse Coopers organization, which deals with the economic crime survey, has defined economic crime in cyber world as “an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details.

- **Phishing and Vishing**

In computing, phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message.

Vishing is also alike phishing; it is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial information from the public for the purpose of financial reward. The term is a combination of “voice” and phishing. Vishing exploits the public’s trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer.

- **Data Theft**

Data and information are valuable assets in this digital age. Business secrets, technical knowhow, designs, music, films, books, personal data including usernames, credit card numbers and passwords, are some forms of property that drive the information economy. Money, time, effort and creativity go into the creation and compilation of data and information. Stealing of data and information through hacking and other means, is the most prevalent cyber crime.

- **Data Diddling**

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating; recording, encoding, examining, checking, converting, or transmitting data.

- **Salami Attacks**

A salami attack is a series of minor data security attack that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can be considered a salami attack.

- **E-mail Bombing**

E-mail bombing refers to sending a large number of e-mails to the victim resulting in the victim's e-mail account(In case of Individual) or mail servers (in case of a company or an e-mail service provider) crashing.

- **E-mail spamming**

It is a variant of bombing; it refers to sending e-mail to hundreds or thousands of users. E-mail spamming can be made worse if recipients reply to the e-mail, causing all the original addressees to receive the reply. It may also occur

innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users.

- **Software Piracy**

Some common methods of copyright infringement in relation to computer software as stated are:—

- Reproducing the original owner's software and packaging of that software, so that purchasers are deliberately misled into believing that the product they are buying is genuine software.
- Reproducing or 'burning' the original owner's software onto a blank CD, where no attempt is made to represent that the copy is genuine.
- Reproducing a number of the owner's programme on a single CDROM, known as a 'compilation' CD.

- **E-mail Spoofing**

E-mail spoofing is a term used to describe fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. By changing certain properties of the e-mail, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. It is often associated with website spoofing which mimic an actual, well-known website but are run by another party either with fraudulent intentions or as a means of criticism of the organisation's activities.

- **SMS spoofing**

SMS spoofing is like e-mail spoofing, which looks to originate from your acquainted number but in reality it is spoofed, and send from some evil minded individual. We can take this by an example. Suppose if a woman receive a Short Messaging Service (SMS) in her cellphone in the middle of a night from the mobile of her spouse asking her to bring cash as he has met with an accident. The chances are that she would check the mobile number and if she confirms that

the cell is her husband's then she would rush out with cash. If this could be the response then the chances are that she is not aware of "Mobile Spoofing". Using web-based software, a cyber criminal could send anyone a message from any person's cell without even touching his mobile and no cellular service provider can say that it was a spoofed or faked one.

- **Online illegal selling(Dark web)**

Here criminal performs illegal activities such as selling illegal weapons, smuggled goods, drugs, or person's information to the person who is present on an illegal shopping portal. It promotes black marketing.

F) CAUSES OF CYBERCRIME

Cybercrime targets rich people or rich organizations like casinos, banks, and financial firms where a tremendous amount of money comes daily and hackers can easily hack sensitive information. It is an easy way to make big money. Catching these criminals is difficult. The number of cybercrimes across the globe is increasing on a daily basis. Various laws are required to safeguard the use of computers against various vulnerabilities. Following are the various reasons listed for the vulnerability of computers:

- **Capacity to store data in comparatively small space-** One unique characteristic of a computer is that it can store your data in a considerable small space. This makes it easy for the criminal to steal our data from the system and they use it for their own profit.
- **Negligence-** This is a characteristic of human conduct. While protecting the computer system we can make any negligence which makes it easy for the criminal to have access and control over your computer system.
- **Easy to access-** Due to the complex technology used, it is difficult to protect a computer system from unauthorized access. Hackers can steal information that can fool biometric systems easily and bypass firewalls need to be used to get past many security systems.

- **Loss of evidence-** The data with the crime can be destroyed easily. So while investigating a cybercrime, loss of evidence is a very common issue.

G) STATEMENT OF THE PROBLEM

“A STUDY OF CYBER CRIME AWARENESS AMONG TEACHER TRAINEES IN RELATION TO THEIR GENDER AND LOCALITY IN JAMMU DISTRICT”.

H) OPERATIONAL DEFINITIONS OF KEY TERMS USED

- **CRIME:-**Crime is the violation of any rule of administration or law of the state or practice of any wrong doing and harmful to self or against third parties.
- **CYBERCRIME:-**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, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)”.
- **AWARENESS:-**In the present study, awareness is the state or condition of being aware i.e. having knowledge and consciousness of cyber crime.
- **TEACHER TRAINEES:-** Teacher trainees are one’s who are doing B.Ed to become trained teachers.

I) OBJECTIVES OF THE STUDY

The objectives of the present study were:

- To find the difference in the awareness of cybercrime among B.Ed. teacher trainees with respect to their gender (male and female).

- To find the difference in the awareness of cybercrime among B.Ed. teacher trainees with respect to their locality (urban and rural).
- To find the difference in the awareness of cybercrime among B.Ed. teacher trainees on the basis of interactional effect of gender (male and female) and locality (urban and rural).

J) HYPOTHESES OF THE STUDY

- There is no significant difference in the awareness of cybercrime among B.Ed. teacher trainees with respect to their gender (male and female).
- There is no significant difference in the awareness of cybercrime among B.Ed. teacher trainees with respect to their locality (urban and rural).
- There is no significant difference in the awareness of cybercrime among B.Ed. teacher trainees on the basis of interactional effect of gender (male and female) and locality (urban and rural).

K) DELIMITATIONS OF THE PRESENT STUDY

Due to lack of time and other resources, the study was carried out with certain delimitations:

- The study was confined to Jammu District only.
- The sample was confined to 200 B.Ed. teacher trainees only.
- Only 5 colleges were covered in the present study.

L) POPULATION

The population of the study consisted of B.Ed. teachers trainees of Jammu district and a representative sample from the population was selected by the investigator.

M) VARIABLES STUDIED

In the present study there are two independent variables and one dependent variable which are to be studied:

a) Independent variable:

- i) Gender: Male and Female
- ii) Locality: Rural and Urban

b) Dependent Variable: Cyber crime Awareness Scale Scores

N) SAMPLING

Sampling is the basis of all statistical methodology of research. The investigator can never collect data from the whole population in any investigation. The investigator has to take selected groups of individuals who would represent the whole population and form the basis for making reference of certain population of facts. This is known as sampling. The size of sample varies from study to study, method and nature of population. It is easier, less time consuming than the whole population.

In the present study, the sample of 200 teacher trainees was selected from 5 different B.Ed. colleges of Jammu by using simple random sampling technique.

O) SELECTION OF TOOL

A tool is a device to collect information from the sample. The selection of a suitable instrument or tool is of vital importance for any successful research which depends upon the nature of the problem. It is the selection of the appropriate tool which enables the researcher to arrive at certain generalization about the problem.

For the present study, the investigator used the Cyber Crime Awareness Scale developed by Dr. S. Rajasekar based on Likert scale.

P) RELIABILITY AND VALIDITY

Reliability

The reliability of the Cyber Crime awareness scale was established by the split half method (odd-even numbered) using Pearson Product Moment

correlation. This only gives the reliability of half scale and hence the coefficient of the reliability of the full scale was determined by using the Spearman- Brown prophecy formula and was found to be 0.76, which is high and therefore the scale is reliable.

Validity

The Cyber Crime awareness scale has construct validity as items were selected having the ‘t’ values equal to or greater than 1.75 (Edwards,1975). Its intrinsic validity was found to be 0.87 and hence the scale is valid.

Q) ADMINISTRATION OF TOOL

Before administering the scale, the investigator made everything clear to the teacher trainees about the scale by explaining them how they should tick (√) mark about the statements related to Cyber Crime. No time was set. All precautions were taken to prevent discussions between students. Precaution was also taken to prevent coping. The sheets were collected, scoring was done on the basis prescribed procedure and raw scores were obtained.

R) SCORING PROCEDURE

After collection of data the first thing done was scoring. The following scheme was used for scoring the responses.

Nature of Statements	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
Positive	5	4	3	2	1
Negative	1	2	3	4	5

S) STATISTICAL TECHNIQUES USED

In present study, the investigator was concerned with following techniques:

In the present study, the statistical technique Two-way Analysis of variance with 2x2 factorial design was applied in order to study the study of Cyber Crime Awareness among Teacher Trainees belonging to different gender and locality.

T) ANALYSIS AND INTERPRETATION OF DATA

Table A : Showing the summary of ANOVA for 2x2 Factorial Design

Source of variance	SS	Df	MS	F-ratio	Level of Significance
A (Gender)	57.6	1	57.6	0.60	Not significant
B (Locality)	313.6	1	313.6	3.27	Not significant
AxB	705.6	1	705.6	7.37	Significant
Within	3445.2	36	95.7		

Interpretation

The F- ratio for the factor ‘A’ Gender i.e. (Male and Female) came out to be 0.60 and the table values for significance are 4.11 and 7.39 at .05 and .01 level of significance against df 1 and 36 respectively. It means that there is no significant difference in the awareness of B.Ed. teachers trainee i.e. male and female teachers trainee towards cyber crime. Hence, hypothesis no. 1 stating that there is no significant difference in the awareness of B.Ed. teachers trainee i.e. male and female towards cyber crime stands accepted.

The F- ratio for the factor ‘B’ Locality i.e. (Rural and Urban) came out to be 3.27 and the table values for significance are 4.11 and 7.39 at 0.05 and 0.01 level of significance against df 1 and 36 respectively. It means that there is no significant difference in the awareness of B.Ed. teachers trainee belonging to different Locality i.e. (Rural and Urban) towards cyber crime. Hence, hypothesis no. 2 stating that there is significant difference in the awareness of B.Ed. teachers belonging to different Locality i.e. (rural and urban) towards cyber crime stands accepted.

The F-ratio for interaction AxB (Gender x Locality) has been found to be 7.37 which is more than the table value 4.11 at 0.05 level of significance. It indicates that under joint influence of gender (male and female) and locality (rural and urban) there is significant difference is seen the awareness of B.Ed. teachers towards cyber crime. Hence, Hypothesis no. 3 i.e. stands rejected.

U) CONCLUSIONS

The following findings are drawn on the basis of study:

- 1) There is no significant difference in the awareness of B.Ed. teacher trainees belonging to different gender (Male and Female) towards cyber crime.
- 2) There is no significant difference in the awareness of B.Ed. teacher trainees belonging to different locality (Rural and Urban) towards cyber crime.
- 3) Significant difference is seen in the awareness of B.Ed. teacher trainees towards cyber crime under joint influence of gender (Male and Female) and locality (Rural and Urban).

V) EDUCATIONAL IMPLICATIONS

One basic objective of educational research is to improve the educational sector by implementing findings of the research studies in it. Therefore, if a research work does not have point of implication mentioned separately, it is not considered as research work of education.

Cyber crime awareness is required since computer is prevalent and versatile device. It acts as a nervous system for every advancement in the society. Teacher trainees should be aware of while using their e-mail accounts, while using their Credit or Debit cards in public places and they should sign out from their account without forgetting. Cyber security is what helps to prevent issues like data breaches, cyber attacks and identity theft. It is used to protect yourself and your data from unauthorized access, modification and deletion. Thus cyber awareness enables us to be a victim of cyber crimes. The level of Cyber crime awareness of teacher trainees should be developed through various awareness programs. If the

teacher trainees are aware about cyber crimes then in future they will educate their students too. A unit regarding cyber crimes should be included in the B.Ed. curriculum. Symposiums and seminars regarding cyber crimes may be organised in colleges to create awareness. In schools and colleges, a separate subject on cyber crimes may be included to create awareness among students.

W) SUGGESTIONS FOR FURTHER RESEARCH

The present study has answered few questions but also led to some other questions. In the present study the investigator came across a number of issues on which work could be carried out in future.

Further research can be conducted on the line given below:-

- 1) The study was confined only to the sample of 200 B.Ed teacher trainees of Jammu district. Same type of work can be done on a large sample with more variables.
- 2) The present study cannot be final and comprehensive; more work can be done on different samples of different age groups.
- 3) The present study deals with teacher trainees, same type of work can be done on higher secondary school students, college students, university students and thus comparisons can be drawn.
- 4) The study can be carried out in other districts also like Kathua, Samba, etc.
- 5) Similar study may be conducted on some weaker sections of the society.

BIBLIOGRAPHY


- Aggarwal, J.C., (1991). *Educational research*; New Delhi: Man Singh Publications.
- Alharbi, T. and Tassaddiq, A. (2021). Assessment of Cyber security awareness among Students of Majmaah University. *Big Data Cogn. Comput*, 5(2), 23.
- Allport, G.W. (1935). *Attitude in C. Murchison* (ed.) A hand book of social psychology. New Delhi: Worester Mass Clark. University Press.
- Arpana. & Chauhan, M. (2012). Preventing cyber crime: A study regarding awareness of cyber crime in Tricity. *International Journal of Enterprise Computing and BusinessSystems*, 2(1), 2-7. ISSN (Online): 2230-8849.
- Bandakkanavar, R. (2022). Causes of Cyber crime and Preventive Measures. Retrieved from <http://krazytech.com/technical-papers/cyber-crime>
- Best, J. W., and Kahn, J. V. (1992). *Research in education*. New Delhi: Percentile Hall of India Pvt. Ltd.
- Characteristics of Cybercrime. Retrieved from https://lawpage.in/cyber_laws/crime/characteristics
- Chaudhari, M., Dulgaj, B., Valvi, K., Valvi, M., Dive, N., Kothwal, S., Shaikh, T. (2021). A study to assess the Awareness regarding Cybercrime and cyber safety among undergraduate students from selected Nursing Institute of Nashik City. *International Journal of Advances in Nursing Management*, 9(1), 84-86.
- Dashora, K. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences*, 3(1), 240-259.
- Garba, A. A., Siraj, M. M. and Oatman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in

- Nigeria. *International Journal of Electrical and Computer Engineering (IJECE)*, 12(1), 572-584.
- Goel, U. (2014). Awareness among B.Ed teacher training towards cyber-crime: A study. *Learning Community*, 5(2&3), 107-117.
- Hasan, M. S., Rahman, R. A., Abdillah, S. F. H. B. T., & Omar, N. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. *Journal of Social Sciences*, 11(4), 395-404.
- Ismailova, R. and Muhametjanova, G. (2016). Cyber crime risk awareness in Kyrgyz Republic. *Information Security Journal: A Global Perspective*, 25(1-3), 32-38.
- Jamil D. and Khan M.N.A. (2011), Data Protection Act in India with Compared To the European Union Countries. *International Journal of Electrical & Computer Sciences*, 11(6), 11-15.
- Koul, L. (1997). *Methodology of education research*. New Delhi: Vikas Publishing House Private Limited.
- Manasrah, A., Akour, M. and Alsukhni, E. (2015). Toward improving university students awareness of spam email and cybercrime: Case study of Jordan, *First International Conference on Anti-Cybercrime (ICACC)*, 1-6.
- Mehta, S. and Singh, V. (2013). A Study of Awareness of Cyber laws in the Indian Society. *International Journal of Computing and Business Research*, 4(1). ISSN (Online): 2229-6166.
- Mokha, A. K. (2017). A Study on Awareness of Cyber Crime and Security. *Research J. Humanities and Social Sciences*, 8(4), 459-464.
- Punjabi, R. (2019). Cyber Crime Awareness among B.Ed. Students. *Think India Journal*, 22(40).
- Sharma, R.A. (2000). *Fundamentals of educational research*, Meerut: Loyal Book Depot.
- Verma, L.K., and Sharma, N.R. (2008). *Advanced statistics in education and psychology*. Jammu : Narendra Publishing House.

Yu, S. (2014). Fear of Cyber Crime among College Students in the United States: An Exploratory Study. *International Journal of Cyber Criminology*, 8(1), 36-46.

Zwilling, M., Klien, G., Lesjak, D., Wiechtek, L., Cetin, F. and Basim, H.N. (2020). Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82-97.

Appendix-A

 <p style="font-size: small; text-align: center;">T. M. Regd. No. 564838 Copyright Regd. No. © A-73256/2005 Dt. 13.5.05</p> <p style="text-align: center;">Dr. S. Rajasekar (Annamalainagar)</p>	<p style="text-align: center;">Consumable Booklet of CCAS-RS (English Version)</p>
---	--

Please fill up the following informations :		Date							
Name of the teacher trainee _____									
Father's name _____									
Date of Birth									
College _____									
Management of College / School : University / Self financing / Government									
Gender		:	Male / Female						
Location		:	Rural / Urban						
Qualification _____									
Attended computer classes		:	Yes / No						
Having own Computer		:	Yes / No						
Browsing period		:	Everyday / Twice a Week / Occasionally						

INSTRUCTIONS						
<p>This scale consists of 36 statements and it provides five columns bearing the headings Strongly Agree (SA), Agree (A), Undecided (UD), Disagree (DA), Strongly Disagree (SD), against the statements. Read each statement carefully and place a <input checked="" type="checkbox"/> mark against it in the appropriate column you think describes you the best. You are requested to give responses to all the statements. There is no right or wrong answer. There is no time limit but you have to give the answer immediately. Your responses will be kept confidential.</p>						
SCORING TABLE						
Page	2	3	4	z-Scores	T-Scores	Interpretation
Total						
Total Scores						

Estd. 1971	www.npcindia.com	☎:(0562) 2601080
NATIONAL PSYCHOLOGICAL CORPORATION		
UG-1, Nirmal Heights, Near Mental Hospital, Agra-282 007		

Sr. No.	STATEMENTS	RESPONSE					SCORE
		Strongly Agree	Agree	Undecided	Dis-agree	Strongly Disagree	
1.	It is always better to make use of current antivirus software in your computer.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
2.	One should not reveal his/her mobile number while chatting through internet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
3.	Sending threatening MMS/SMS to other mobile is not a crime.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
4.	Sharing your password to anyone is dangerous	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
5.	Sending obscene/pornographic text or images through SMS or MMS is not an offence.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
6.	Pirated software should not be installed into the mobile phone or computer.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
7.	It is not advisable to hand over your mobile phone to the unauthorized service centre to rectify the defect if any in your mobile phone.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
8.	Releasing unauthorized information on internet is legal.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
9.	It is always a must to sign out after you finish your e-mail session	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
10.	It is advisable to respond to an unknown number through your mobile phone.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
11.	Locking the mobile phone by using a password after every use is preferable.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
12.	It is advisable to make use of anti spyware software in your computer.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
Total Score Page 2							<input type="text"/>

Sr. No.	STATEMENTS	RESPONSE					SCORE
		Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	
13.	Unknown MMS/SMS received should always be opened.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	• <input type="text"/>
14.	Sending your photos through internet to unknown email addresses is dangerous.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
15.	Using the copyrighted image /text without prior permission is not an offence.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	• <input type="text"/>
16.	Taking photographs through mobile phones in Hotels or other public place without prior permission is legal.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	• <input type="text"/>
17.	It is better to verify whether your mobile phone is having a valid IMEI number or not.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
18.	Visiting unsecured websites will harm your computer.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
19.	One should not keep the blue tooth device active always if it is not in use.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	• <input type="text"/>
20.	Security code should be used to prevent your mobile phone from misuse.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
21.	It is better to protect your computer with a suitable password.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
22.	Withdrawing money from ATM through others is not dangerous.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	• <input type="text"/>
23.	Changing the PIN number at least once in fifteen days is preferable.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
24.	It is advisable not to purchase a mobile SIM for somebody in your ID.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
25.	Spreading Trojan horses through e-mail is legal.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	• <input type="text"/>

Total Score Page 3



Small, illegible text located below the red 'x' icon in the top left corner of the frame.

Appendix –B

Raw scores of male

S.No.	Scores	S.No.	Scores
1.	121	26.	119
2.	119	27.	113
3.	118	28.	120
4.	124	29.	105
5.	111	30.	102
6.	110	31.	122
7.	113	32.	114
8.	121	33.	100
9.	129	34.	111
10.	124	35.	109
11.	117	36.	125
12.	111	37.	109
13.	108	38.	119
14.	116	39.	122
15.	124	40.	126
16.	103	41.	116
17.	100	42.	105
18.	99	43.	96
19.	92	44.	104
20.	100	45.	113
21.	106	46.	102
22.	100	47.	106
23.	110	48.	107
24.	111	49.	125
25.	111	50.	110

Raw scores male

S.No.	Scores	S.No.	Scores
51.	107	76.	125
52.	101	77.	120
53.	120	78.	123
54.	121	79.	118
55.	109	80.	107
56.	114	81.	116
57.	114	82.	109
58.	107	83.	119
59.	100	84.	123
60.	120	85.	117
61.	97	86.	121
62.	96	87.	134
63.	97	88.	125
64.	113	89.	112
65.	113	90.	118
66.	115	91.	110
67.	112	92.	113
68.	118	93.	98
69.	97	94.	119
70.	115	95.	118
71.	107	96.	100
72.	105	97.	106
73.	124	98.	98
74.	117	99.	97
75.	113	100.	92

Appendix –C

Raw scores female

S.No.	Scores	S.No.	Scores
1.	98	26.	100
2.	109	27.	102
3.	106	28.	103
4.	130	29.	97
5.	117	30.	102
6.	117	31.	92
7.	106	32.	95
8.	126	33.	94
9.	98	34.	102
10.	87	35.	98
11.	116	36.	103
12.	114	37.	98
13.	106	38.	98
14.	119	39.	102
15.	108	40.	111
16.	100	41.	100
17.	98	42.	106
18.	103	43.	103
19.	99	44.	109
20.	108	45.	84
21.	90	46.	100
22.	115	47.	110
23.	80	48.	84
24.	114	49.	105
25.	82	50.	96

Raw scores female

S.No.	Scores	S.No.	Scores
51.	92	76.	94
52.	81	77.	110
53.	115	78.	92
54.	95	79.	101
55.	94	80.	100
56.	110	81.	102
57.	120	82.	103
58.	78	83.	108
59.	132	84.	108
60.	93	85.	93
61.	111	86.	92
62.	105	87.	94
63.	79	88.	99
64.	82	89.	70
65.	110	90.	95
66.	100	91.	76
67.	86	92.	82
68.	99	93.	114
69.	84	94.	107
70.	111	95.	103
71.	115	96.	97
72.	109	97.	63
73.	95	98.	72
74.	100	99.	84
75.	100	100.	92