Analysis of Cyber Crime in India under I. T. Amendment Act 2008 during 2012-2018

1Amit Sharma, 2Dr. Parag Garg.

1, 2Research Scholar, School of Law, Monad University, Hapur

Abstract: - Studying the characteristics of reported cybercrimes in India under the IT Act 2000 and the Indian Criminal Code (IPC) from 2012 to 2018, it makes an effort to examine the ongoing and newly emerging cybercrimes that took place during that time under the IT Act 2000 and the IPC, respectively. The internet is now widely used for all necessary tasks, including shopping, paying bills, paying taxes, transferring money, talking with people around the world, exchanging information, conducting business, and so on. The World Wide Web is the most significant initial source of information because it rapidly and efficiently gives each and every person the information they require through communication and sharing tools. The Internet is a well-known example of a network that is interconnected and enables transmission of any type of information to anybody using any network-connected device. Moreover, this paper attempts to analyse the new categories of crime that surfaced in 2017 together with the preventative actions implemented by the Indian government. It also offers best practices for avoiding pit holes.

The ease of usage on the one hand encourages more crimes, such as cybercrimes, to use the internet as a medium. This essay focuses on examining the development trends in internet usage as well as the risks that Indian users confront. The vulnerabilities of internet users are growing along with the usage of the internet.

The centre of global and technological evolution is information and Internet technologies. India is now ranked second globally in terms of internet users. With the aid of the internet, we can speak with almost anybody, anywhere in the world, at any time. The use of the internet has grown rapidly in India during the last several years.

Key Word: - Cyber Crime, IT Amendment Act 2008, Cyber Security

1. Introduction:-
Cybercrime is the concept for illegal computer usage. A new revolution in the world economy happened in the new millennium with the transformation from the physical to the digital sphere. Cybercrime, sometimes referred to as "online crime" or "computer crime," is any criminal conduct that is carried out online. Cybercrime is a relatively recent type of illegal behavior. Any illegal action that occurs or is carried out on or by means of computers, the internet, or any other technology recognised under the IT Act is referred to as cybercrime. In India, cybercrime constitutes the most widespread and efficient kind of crime and it has disastrous consequences. Criminals not only destroy society and create long-term harm to the government, but they also greatly and substantially hide their identity. Despite the fact that the term "cybercrime" has been defined in a few Indian court decisions, it has not yet been included in any laws or statutes that the Indian government has approved. Based on the exploit of modern society's increasing reliance on technology, cybercrime is an unstoppable evil. Computers and associated technology are becoming increasingly commonplace in daily life and are now highly sought by consumers. It is an infinite and incomprehensible medium. Whatever benefits the internet may have for us, it certainly has drawbacks. Emerging cybercriminals include those who engage in cyber terrorism, email spoofing, email bombing, cyber content, and cyber sabotage. If a regular crime is committed using the Internet, it may be considered a cybercrime.

2. Cyber Crime: -
Cybercrime is an unstoppable evil based on the misappropriation of modern society's increasing reliance on technology. Computers and other related technologies are becoming more prevalent in daily life, and they have become a much-desired convenience for users. Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwanted mass-surveillance, sextortion, child pornography, and child grooming. Some of the newly emerged cybercrimes are cyber-stalking, email bombing, cyber defamation, worms, polymorphic virus etc. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwanted mass-surveillance, sextortion, child pornography, and child grooming. Some of the newly emerged cybercrimes are cyber-stalking, email bombing, cyber defamation, worms, polymorphic virus etc. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Types of Cyber Crimes
Types of cybercrime include:

Email and internet fraud.
Identity fraud (where personal information is stolen and used).
Theft of financial or card payment data.
Theft and sale of corporate data.
Cyberextortion (demanding money to prevent a threatened attack).
Ransomware attacks (a type of cyberextortion).
Cybercrime involves one or both of the following:

- Criminal activity targeting computers using viruses and other types of malware. Criminal activity using computers to commit other crimes. Cybercriminals that target computers may infect them with malware to damage devices or stop them working. They may also use malware to delete or steal data. Or cybercriminals may stop users from using a website or network or prevent a business providing a software service to its customers, which is called a Denial-of-Service (DoS) attack. Cybercrime that uses computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images. Cybercriminals are often doing both at once. They may target computers with viruses first and then use them to spread malware to other machines or throughout a network. Some jurisdictions recognize a third category of cybercrime which is where a computer is used as an accessory to crime. An example of this is using a computer to store stolen data.

- Cyberattacks. These are targeted phishing campaigns which try to trick specific individuals into jeopardizing the security of the organization they work for. Unlike mass phishing campaigns, which are very general in style, spear-phishing messages are typically crafted to look like messages from a trusted source. For example, they are made to look like they have come from the CEO or the IT manager. They may not contain any visual clues that they are fake. Online Scams Online scams are basically scams that happen online. Whether that’s tricking you into giving out personal details online by an ad popping up telling you have won something and asking for your card details to pay for shipping. Sadly, you’ll never receive anything but you’ll start noticing weird transactions coming from your bank account.

Examples of cybercrime

Here are some famous examples of different types of cybercrime attack used by cybercriminals:

- **Malware**
  - A malware attack is where a computer system or network is infected with a computer virus or other type of malware. A computer compromised by malware could be used by cybercriminals for several purposes. These include stealing confidential data, using the computer to carry out other criminal acts, or causing damage to data.
  - A famous example of a malware attack was the WannaCry ransomware attack, a global cybercrime committed in May 2017. WannaCry is a type of ransomware, malware used to extort money by holding the victim’s data or device to ransom. The ransomware targeted vulnerability in computers running Microsoft Windows. When the WannaCry ransomware attack hit, 230,000 computers were affected across 150 countries; Users were locked out of their files and sent a message demanding that they pay a Bitcoin ransom to regain access. Worldwide, the WannaCry cybercrime is estimated to have caused $4 billion in financial losses. To this day, the attack stands out for its sheer size and impact.

- **Phishing**
  - A phishing campaign is when spam emails, or other forms of communication, are sent with the intention of tricking recipients into doing something that undermines their security. Phishing campaign messages may contain infected attachments or links to malicious sites, or they may ask the receiver to respond with confidential information. A famous example of a phishing scam took place during the World Cup in 2018. According to our report, 2018 Fraud World Cup, the World Cup phishing scam involved emails that were sent to football fans. These spam emails tried to entice fans with fake free trips to Moscow, where the World Cup was being hosted. People who opened and clicked on the links contained in these emails had their personal data stolen.
  - Another type of phishing campaign is known as spear-phishing. These are targeted phishing campaigns which try to trick specific individuals into jeopardizing the security of the organization they work for. Unlike mass phishing campaigns, which are very general in style, spear-phishing messages are typically crafted to look like messages from a trusted source. For example, they are made to look like they have come from the CEO or the IT manager. They may not contain any visual clues that they are fake. Online Scams Online scams are basically scams that happen online. Whether that’s tricking you into giving out personal details online by an ad popping up telling you have won something and asking for your card details to pay for shipping. Sadly, you’ll never receive anything but you’ll start noticing weird transactions coming from your bank account.

3. **Malware**

Malware is the contraction of malicious software onto your system. It’s a piece of software written with the intent of causing harm to data and devices. Malware is the overarching name for different types of viruses such as a ‘Trojan’ and ‘spyware’. Malware is often done through a range of viruses that will get into your computer to cause havoc, by damaging your computer, tablet, phone; so the culprits can steal credit card details and other personal information.

4. **Email Bombing**

An email bomb is more a form of internet abuse. Email bombing is an overload of emails directed to one email address, this will cause the person receiving the emails server to become sluggish or even crash. They may not necessarily be stealing anything from you but having a sluggish server can be a real pain and hard work to fix.

5. **Virus Dissemination**

This is particularly sneaky form of cybercrime. It not only gets a piece of malware (a virus of some sort) onto one part of the victim’s system, but it spreads across other pieces of software. Without a full and proper quarantine process and safe environment to test in (a sandbox), the next time you open a piece of undiagnosed-as-infected software, the process starts all over again.

6. **Logic Bombs**

Logic bombs act in the same way as a virus, but are small programs or sections of a program, which are triggered by an event. This event can be a certain date or time, a certain percentage of disk space filled, the removal of a file and so on. A program could then delete critical sections of code, rendering your software as useless. The people who implement logic bombs are most commonly installed by insiders who already had access to the system.
7. Theft
Internet theft is the broad term for any type of theft that happens over the internet, this can be done through many ways such as fake ads, fake emails, viruses and snooping. The aim of internet theft is to steal your personal information and use it to then steal money out of your bank account or make purchases using your details.

8. Social Media Hack & Spamming
Social media hacking is often done as a joke, like the attack by the people who hacked Burger King’s twitter account. And many celebrities that are hacked may end up following people they wouldn’t usually or put random statuses. Even though for the average Joe seeing a celebrity or brand post weird stuff can be amusing, it’s an invasion of privacy. However a hacker can also spread unwarranted content that can be distressing to people who view this content, it can also cause your account to be reported and shut down. Social media spamming comes when a person makes a fake account and becomes friends or followed by the average person. This then gives the fake account the freedom to spam inboxes with bulk messaging; this can be done for spreading malware. Spamming can also spread malicious links created with the intent to harm, mislead or damage a user or their device. Clicking on the malicious link, which may be advertising a new iPhone or weight loss treatment, means you could be downloading malware which can lead to the theft of personal information. Another dark side of social media is the ability for malicious accounts to spam your output by constantly replying with negative messaging. A form of trolling. Whilst you can easily report such behavior to the social media platform and they should remove the user, or you can block them from seeing your content, it’s easy for people to set up new bot accounts in minutes and begin their attack again. Some people have too much time on their hands.

9. Electronic Money Laundering
Money generated in large volumes illegally must be laundered before it can be spent or invested. One way to launder money is to do it electronically through messages between banks which is known as a ―wire transfer‖. It had previously seemed impossible to monitor or screen wire transfers as they occur due to the tremendous volume on transactions going through on a day to day basis, however banks are clamping down on the issue and filing away any suspicious activity.

10. Sales & Investment Fraud
By sourcing the contact details and available account information for savings or investment account holders, fraudsters can adopt the persona of an investment broker. They will then contact customers to entice them with easy and profitable opportunities, but they seem a lot more trustworthy because they talk about accounts you already own and real results. Think of it as a more thorough phishing scam.

11. Eavesdropping & Surveillance
Eavesdropping without the consent of the parties is a crime and can be done online or over the phone. The most common way to eavesdrop is to wiretap, which is the practice of connecting a listening device, usually to a telephone line, that allows the criminal to monitor conversation secretly. As new technologies are introduced computers can now be hacked for eavesdropping and surveillance. As a random tip, take a look at, Facebook head man, Mark Zuckerberg's painfully simple defense against would-be webcam voyeurs, connection requests. Cybercriminals who are carrying out cyber extortion may use the threat.

12. Software Piracy
Nowadays, thanks to the internet, you can find almost any movie, song or software for free online. Software piracy is the unauthorized use and distribution of computer software. Even though using pirated material may seem good because it’s free, it comes with a range of risks. These risks include: Trojans, viruses, worms and other forms of malware. But it’s also stealing as no proceeds go to the producers of the content.

13. Data Diddling
Despite the humorous name and seemingly innocuous action compared to other cybercrimes in this list, data diddling is the action of skewing data entries in the user's system. The results can be huge, however. They might include adjusting financial figures up or down marginally, or it could be more complex and make an entire system unusable.

14. Salami Slicing Attack
A salami slicing attack, as funny as it sounds, makes sense once explained. It’s a technique used by cyber criminals to steal money or resources a tiny bit at a time, so there initially isn’t a noticeable difference to the bank account. The criminal will do this to a number of different sources which accumulates to a considerable amount stolen over time. Salami slicing attackers generally use this technique to steal money.

15. Hacking
In simple terms, a hacker is an intruder who accesses your computer system without your permission. Hackers do this for a number of reasons, whether that's for greed, fame or power, as it shows people they are clever enough to get into something they shouldn't have. However, some will be able to break into systems and steal personal banking information and corporation financial data. Hackers tend to be computer programmers and have an advanced understanding of computers.

16. Cyber Stalking
There are many cases of cyber stalking across the world and it’s especially common with teenagers and young adults. Usually the victim and the stalker know each other. The victim is usually subjected to online harassment in forms of a barrage of online messages and emails. The aim of online stalking is to make the victim miserable or exert control as a perverse way of being in contact with the victim, just like ordinary stalking.

17. Cyber Bullying
Cyber bullying is similar to cyber stalking, however, the barrage of messages can be harmful, abusive, and wholly offensive. Cyber bullying can also be done by posting images and videos online that will offend the victims. It can also be excluding people online, creating fake accounts to post harmful or distressing content, and again sending abusive messages. Overall it is bullying but
online usually through social media channels.

18. Identity Theft
Identity theft is one of the most common types of cybercrime. The main reason identity theft occurs is with the view of creating fraud for financial gains. Criminals usually steal identity information of others such as credit card information, addresses, email addresses and more. With this information they can pretend to be someone else and create new bank accounts.

19. Child Soliciting & Abuse
Child soliciting and abuse online is a type of cybercrime where criminals solicit children via chat rooms for the purpose of pornography. It can also come in forms of material that shows or describes sexual abuse towards children. A child is regarded as someone who is under the age of 16. This type of cyber crime is heavily monitored by the police. It can be a threat to companies as well as individuals because the perpetrators may be looking to adopt another persona online.

20. Ransom ware
Ransom ware affects many companies and has recently affected the NHS and other big corporations all over the world. Ransom ware enters your computer network and encrypts files, meaning you don’t have any access to them. The attacker will send you a notification demanding a large sum of money for you to then get your data back. The criminals aim is that they will get enough people to pay to ransom fee to get a quick buck.

Why You Need To Protect Yourself
Cyber criminals are out there and will do anything to make money and steal useful information. As we are becoming more digital, we are opening ourselves up to more and more types of cybercrime. There are many ways to protect yourself from cyber-attacks. Protecting yourself will make you less vulnerable to cyber-attacks and therefore prevent you from getting your personal information stolen, robbed, having your data encrypted and so on. Types Of Cybercrime That Are Committed Against Women:

Amongst the various cyber-crimes committed against individuals and society at large, crimes that are specifically targeting women are as follows: –
1. Cyber-stalking- In Cyber Stalking, stalker access the victim’s personal information like name, family background, telephone numbers and daily routine of the victim and post them on the websites related to dating services with the name of victim.
2. Harassment via e-mails- One form may include Harassment through e-mails includes blackmailing, threatening, bullying, constant sending of love letters in anonymous names or regular sending of embarrassing mails to one’s mail box. Indian Penal Code, Criminal Procedure Code and select sections of IT Act deal with the protection from cyber-crime.
3. Cyber Bullying- Cyber bullying is willful and repeated harm inflicted through the use of computers, cell phones or other electronic devices, by sending messages of an intimidating or threatening nature. India is third behind China and Singapore in online bullying.
4. Morphing- Morphing is editing the original picture by an unauthorized user. When unauthorized user with fake identity downloads victim’s pictures and then uploads or reloads them after editing is known as morphing. It was observed that female’s pictures are downloaded from websites by fake users and again reposted/uploaded on different websites by creating fake profiles after editing them. This amounts to violation of I.T. Act, 2000. The violator can also be booked under IPC also for criminal trespass under Section 441, Section 290 for committing public nuisance. Section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail and under Section 501 for defamation.
5. Email spoofing- A spoofed e-mail may be said to be one, which misrepresents its origin [Legal India]. It shows its origin to be different from its actual source. E-mail spoofing is a popular way of scamming online.
6. Cyber Defamation- Cyber tort including libel and defamation is another common crime against women in the net. Although this can happen to both genders, but women are more vulnerable. This occurs when defamation takes place with the help of computers and/or the Internet when someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person’s friends.

Motive behind cyber crime: A motivation involved in cyber crime depends on criminal’s intent and need. Following are the common motives behind cyber crimes:
1) Monetary Profit – Like many offline crimes, cyber crimes are also motivated by the desire for financial gain.
2) Political Motive – Internet is used by extremist and radical groups for propaganda, to attack the websites and network of their opposite groups.
3) Sexual Impulses – Sexually deviant behaviour is illegal and is considered harmful. People view porn sites to fulfill their immoral desires and needs.
4) Entertainment – Many cyber crimes are done for fun and enjoyment unlike other cyber crimes, in which internet is means to an end. For cyber criminals such as hackers, fun is both a means and an end.
5) Emotional Motivators – Cyber criminals who use anger as motivation are spurned lovers, fired employees, business associates or someone who feels cheated. Revenge is much better planned than anger and it could be more dangerous because cyber criminal has more time to think and plan his tracks which often reduces the possibility of being caught.

Reasons for the Growth of Cyber Crime against Women in India:
The transcendental jurisdiction of Internet causes the major threat to the society in the form of cybercrime. The main victim of this transgression can be considered women and children. The study shows that we have 52 million active internet users in India which reached at 71 million in the year 2009. Among them working women net users are 8 percent and 7 percent nonworking women in the year 2009 and 37 percent usage of all users accessing internet through cyber cafe. It is very common phenomenon that the important information of the net surfer is being disclosed easily by the owners of cyber cafe and then it is used for illegal purposes.

Although acquaintance with technology is positive aspect that can be considered important for the development of any country but at the same time it is becoming the source to increase the crime rate with technology against the weaker section of the society.
The reason for the increasing cyber crime rate against women can be categorized into two folds; legal and sociological reasons. Legal Reasons: The object of the IT Act is crystal clear from its preamble which shows that it was created mainly for enhancing commerce hence it covers commercial or financial crimes i.e. hacking, fraud, and breach of confidentiality etc. but the drafters were unaware about the safety of net users. Cyber defamation, email spoofing, cyber sex, hacking and trespassing into one’s privacy is domain is very common now days but IT Act is not expressly mentioning them under specific Sections or provisions13. Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women and children for instance modesty of women is protected under Section 506 and rape, forceful marriage, kidnapping and abortion against the will of the woman are offences and prosecuted under IPC. Indian constitution guarantees equal right to live, education, health, food and work to women. But the same modesty of women seems not to be protected in general except for Section 67 which covers cyber sex in Toto. Sociological Reasons: Most of the cyber crimes remain unreported due to the hesitation and shyness of the victim and her fear of defamation of family’s name. Many times she believes that she herself is responsible for the crime done to her. The women are more susceptible to the danger of cyber crime as the perpetrator’s identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Women still do not go to the police to complain against sexual harassment, whether it is in the real world or the virtual world they prefer to shun off the matter as they feel that it may disturb their family life.

Suggestions for women not becoming victim of cyber crime: Prevention is always better than cure. A citizen should take certain precautions while operating the internet and should follow certain preventive measures for cyber crimes which can be defined as: Identification of exposures through education will assist women to meet these challenges. One should avoid disclosing any personal information to strangers via e-mail or while chatting. By empowering women and making them hesitation free and bold in complaining about the crime. By tightening security of internet. One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day. Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt policies in regard of this. Encryption technology should be used. Web servers running public sites must be physically separately protected from internal corporate network. Intrusion management should be made. False email identity registration should be treated as an offence. Use of voice-recogizer, filter software and collar-ID for protection against unauthorized access. Formation of special cybercrime investigation cell for Hi-tech crimes. E-judiciary and video-conferencing for speedy justice. Appointment of cybercrime reporters or cyber law journal. Generally, cybercrime is on the rise. According to Accenture’s State of Cybersecurity Resilience 2021 report, security attacks increased 31% from 2020 to 2021. The number of attacks per company increased from 206 to 270 year on year. Attacks on companies affect individuals too since many of them store sensitive data and personal information from customers. A single attack – whether it’s a data breach, malware, ransomware or DDoS attack - costs companies of all sizes an average of $200,000, and many affected companies go out of business within six months of the attack, according to insurance company Hiscox. Javelin Strategy & Research published an Identity Fraud Study in 2021 which found that identity fraud losses for the year totalled $56 billion. For both individuals and companies, the impact of cybercrime can be profound – primarily financial damage, but also loss of trust and reputational damage.

I.T. Amendment Act 2008:- As the present universe is surrounded by the power of new mantra name “Information technology”. With the appearance of the IT Act most of the countries have switched over to paper based governance to e-governance. The Government of India then passed its first cyber law, THE INFORMATION AND TECHNOLOGY ACT OF 2000, which provides a legal infrastructure for e-commerce in India. The IT Law takes into consideration, the legal semantics and know-how while also simultaneously governing relevant data, software, and details on the digital age. Even though it's not under any particular ambit of law, it manages to cover vast areas of intellectual property, data protection, and privacy under its ambit. The Act protects the field of e-commerce, e-governance, e-banking while also covering penalties and punishments in the field of cybercrimes. The above Act was further amended in the form of the IT Amendment Act, 2008.

3. Cyber Security:-

Indian Cyber Situation-India ranks 3rd in terms of the highest number of internet users in the world after USA and China, the number has grown 6-fold between2012-2017with acompondannualgrowthrate44%. India secures as pot amongst the top 10spam-sending countries in the world alongside USA India was ranked among the top five countries to be affected by cybercrime, according to a 22October report by on line security firm”SymantecCorp”.

Cyber attacks in India-

UNION BANK OF INDIA HEIST-Through a phishing email sent to an employee, hackers accessed the credentials to execute a fund transfer, swindling Union Bank of India of $171 million, Prompt action helped the bank recover almost the entire money.

WANNACRY RANSOMWARE-The global

Ransomware attack took its toll in India with several thousand computers getting locked down by ransom-seeking hackers. The attack also impacted systems belonging to the Andhra Pradesh police and state utilities of West Bengal.

DATA THEFT AT ZOMATO-
The food tech company discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an ‘ethical’ hacker—who demanded the company must acknowledge its security vulnerabilities—and put up for sale on the Dark Web.

**PETYA RANSOMWARE**

The ransomware attack made its impact felt across the world, including India, where container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai’s Jawaharlal Nehru Port Trust got affected.

**Future. Technology to be Designed with Security**

- Security innovation must deliver more capable solutions to keep pace with threats.
- Platforms and security standards must be open to promote Collaboration and accelerate adoption.
- Technology and security providers Must be trustworthy in the creation and operation of their products.
- Products and services must be Hardened to resist compromise and make security transparent to users.
- Security must protect data wherever it exists or is used, for all parties and devices across the compute landscape.

**Steps to Cyber Security**

- Protect networks against external and internal attack. Manage the network primer. Filter out unauthorized access and malicious contents. Monitor and test security controls.
- Produce relevant policy and establish anti-malware defences. That are applicable and relevant to all business areas. Scan for malware across the Organization.
- Establish a monitoring strategy and produce supporting policies. Continuously monitor all I CT system and networks. Analyse logs for unusual activity that could indicate an attack.
- Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.
- Produce user policies covering acceptable and secure use of the organization’s systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

**Conclusion & Suggestion**

Over the last three decades, computer technology has become an entirely ubiquitous component of modern life. The increasing dependence on technology to support and manage our lives has created unparalleled opportunities for crime and misuse. In fact, most forms of crime now involves technology in some way, whether through the use of cell phones and text messages or more novel applications of technology to commit crimes that are not otherwise possible outside of digital devices. Cyber space offers a plethora of opportunities for cyber criminals to cause harm to innocent people. Indian women citizens are still not open to immediately report the cyber abuse or cyber crime. The biggest problem of cyber crime lies in the modus operandi and the motive of the cyber criminal. Cyber space is a transit space for many people, including offenders. While people do not live in cyber space, they come and go like any other place. This nature provides the offenders the chance to escape after the commission of cyber crime. Many websites and blogs provide security tips for the safety of women and children in the net. But still then cyber crime against women is on rise. As they are the easy target and they can be victimized easily i.e. why women are made the main target. In reality it is seen many chat friends enjoy teasing their women friends by words such as “sexy”, “attractive” which are the virtual beginning of cyber obscenity. They slowly take their female friends into confidence and start discussing about their own problems like a true friend. Hence in many occasions they are successful in turning the net friendship into a strong bond and gradually proceed to send obscene or derogatory remarks. If the recipient shies away, the sender of such messages would become more encouraged to continue. The problem would be solved only when the victimized woman then and there report back or even warn the abuser about taking strong actions. In order to avoid the cyber-crime we should not engage in conversation with people we don’t know. People on the other end of the computer may not be who they claim to be. We must keep our passwords protected and do not keep sensitive material on the computer as that can be accessed by the hacker. If anything seems wrong, contact law enforcement immediately. Women should always be alert while using internet and should not open any site which can lead them into trouble. They should not engage in chat chat with strangers in order to protect themselves from being victimized. Even our government is also taking action like it is planning for setting up the NIC -CERT (National Informatics Centre-Computer Emergency Response Team) to combat cybercrime in India and the home ministry proposing to set up the Indian Cyber Crime Coordination Centre (I4C), the government is hoping to beef up India’s cyber security network. Lastly I would like to say that „to remove cybercrime is my plan, I know my friends if we join hands together surely we can”.

**REFERENCES:**

1. The Hindustan Times, New Delhi dated 23 dec 2003
8. Vishwanath Paranjape, Legal dimensions of cybercrimes and preventive laws, Pg no.33, Central law Agency, Allahabad, edn., 1st, 2010
10. The Hindustan Times, New Delhi dated 23 dec 2003