**INTERNET SECURITY AND CYBER CRIME**

By: -

**KSHITIJ CHANDRA PANDEY**

1st Year, BA, LL.B. (Hons.)

INDORE INSTIUTE OF LAW

Mob.: -8887678753

E-mail:- kcpandey917@gmail.com



www.probono-india.in

**May 15, 2020**

# abstract

In this research paper researcher has tried to bring the fact about the Cyber Crimes and the Internet security. Researcher has tried to identify different types of cyber-crimes it affects and the recent laws or tackle it. Researcher has brought the fact about the how the young children are driven inside this type of crime and how they are sexually abused and harassed, it has also talked about the cyber-attacks done on the government machinery to fetch down the important data, also they attack on the sites of big multinational companies and commit economic cyber-crime. We will see in this research paper how the different countries maintain he group of hackers for doing the cyber-attacks on their enemy countries to fetch down the data of their exact machinery about their power and weaknesses. Also in this research paper we will find the how Americans use to tackle this modern crime and how they fight with the invisible criminals. Also here the exact data is present about these types of crimes happening in our society. This research paper mainly focuses on U.S.A and India. in this research paper researcher has defined the different terms which are related to the Cyber-crime and researcher has mentioned about the law which is present in India to tackle this problem. This is the role of Ministry of Women and Children development to tackle this. So, in this research paper researcher has tried to cover all the areas regarding this with the comparison of United States of America and India.

**Keywords**:- Cyber-Crime, Sexual Abuse, Hackers, Crime, Attack on Government Machineries, Multi-National Companies, Financial Cyber-Crime Introduction

# introduction

In olden days whenever a crime or assault use to take place it was basically a physical assault where the people who has committed the crime and the person against whom the crime is done know each other. But with modernization and with the introduction of [www.com](http://www.com) in our life everything has become easy, everything means everything it includes the crime too. With the introduction of Internet in 1983, life of the human being has changed a lot, everything has become easy for humans which includes sending message(mails), photographs, searching information etc. as we all know that everything has two sides, one positive and other negative the same has happened with the Internet too. When E- Mail started we started getting the fake messages of Nigerian Prince Death and donating his money to you has now turned to be more serious as it has included the sexual harassment, stocking, grooming, financial cyber-crime and etc etc….

Cyber-crime is an evil having its origin with invention of computer in today’s world where everything is computer based whether its refrigerator to nuclear plants everywhere computers are evolved. Major Cybercrime on economical basis includes the Citi Bank rip off. US $ 10 Million was fraudulently transferred from one account to another in Switzerland by a renowned hacker of Russia led by Vlamdir Kevin.[[1]](#footnote-2)

In this modern age online communication has become a norm, both the government and the normal citizens both are at high risk and are becoming victims of cyber-attack whether it includes the Hacking of Governments Site or the Twitter Handle of politicians or transferring money from one to another account. In modern era cyber-crime is not only limited to these particular areas but is also used as a tool for sexual harassment of specially girls, by stocking them, grooming them, blackmailing them and through all these at last sexually harassing them.[[2]](#footnote-3)

To fight with such a fast widespread crime like this it is the high time when we require a proper and advanced plan to stop and control this widespread. With advancement of time there has been extensive use of computers and internet in our life. When we talk particularly for India the use of internet has increased a lot and has spread to villages too. The internet is basically for betterment of life of the individual but it is not used by some in proper way and uses this mechanism for carrying illegal activities, for hacking ATM and etc. so in order to save this innocent people we need the group of extra ordinary people who can stop those hackers and give them punishment. There is the urge to implement some of the rules and regulations, to tackle and handle these crimes governing cyber space particularly known as cyber law[[3]](#footnote-4). Global security requires global cooperation with different countries. It the time when we should form a collaboration to fight with this invisible enemy, because this problem of Hacking is not only limited to India or China or Russia but the whole world is suffering because of this; it includes the hacking of Indian Home Ministry site, or interfering US general Elections, hacking of Doordharsan and etc, in an recent interview high official of communication notified that in India in year 2016,2017,2018 and till May 2019 199,172,110, and 25 government sites were hacked, this is turing to be a very serious problem which need to be resolved as fast as possible.

# what is internet security

Internet security is the part of computer security it is not only limited to a particular area or world wide web but includes all the aspects of security like network security as it applies to the different application which one have[[4]](#footnote-5). Its objective is to establish a particular rules and regulations to be used against the attacks of hackers on internet. In today’s world internet indicates a unsafe world for the people for exchanging confidential topics or instructions, which leads to the high risk of intrusion, such as online viruses, Trojan horse, worms and much more.

History of Internet security is not much old when we search we need not to go very back, in 1972; an engineer of Egypt M. Atalla filed US patent for remote PIN verification, which used encryption technology to assure telephone link security while dialing personal ID info. This would be transferred as encrypted data over communication on telephone network to backward locations for verifications. This was a precursor to Internet security and e commerce. At the NAMSB conference in January 1976 where the Alltas Foundation and Ramo Cooperation introduced the earliest products designed for dealing with Internet security. They announced an upgrade to its identikey security module. It added the capability of being processing online transactions, designed with the focyus of taking bank transaction online the identikey system was extended to shared facility operation. It was consisted and compatible with various switching networks. The interchange identikey device was released in 1976 and in 1979atalla introduced world’s first NSP i.e., NETWORK SECURITY PROCESSOR.

# threats involved

There are many threats which are evolved with this Internet security and to the internet users, the internet users may be tricked by the cookies and may force them to download the malicious software which may be the dangerous for their internet security. Such viruses come into force in the form of Trojan horse, worms etc. PHISHING is also very common attack which is being done to the online users to extract their sensitive information’s such as username password and credit card number. Phishing occurs when the culprit tries to pretend to be a real and trustworthy person and direct people to fake web and extract their all information from this, they first tries to impress people and attracts them towards fake gifts and ask their information and loot the money and live them bankrupt.[[5]](#footnote-6)

Other way is Application vulnerabilities these are used to access the internet resources may contain security vulnerabilities such as memory safety bugs or flawed authentication checks. The most dangerous of these bugs can give the attackers full control on your computer and can extract full information of your from this technique.[[6]](#footnote-7)

# choosing right internet security tactics

Internet security requires a combination of a lot of new and modern technologies, to safeguard the data properly and safely. It is very important for one to consider several types of net security and tactics to help keep your network secure. These includes:-

* Selection of browser:- each and every browser has its own security measure to insure the safety and security of its users, but there are many sites and browsers whose security are not that well and allow the hackers and cybercriminals to invade and exploit so it is our responsibility that we should use a safe and secure measures as it is only way to reduce the risk involved and to use the safe browser and internet.
* Multi-Factor authentication (MFA) :- Multi-Factor authentication is a method to control computer access by requiring several separate pieces of evidence to an authentication mechanism. Websites and email account can be made more and more secure by conducting two step authentication processes.
* Email Security :- Email security is one of the important field or area were we need to focus on, because Email is a wave through which major of viruses get entry in the form of Trojan horse, worms and etc. establishing a two layered and comprehensive email security strategy will help significantly reduce the exposer to new and emerging threats. Email can also be protected through by using cryptography.
* Firewalls: - Firewalls act as a filter and protector to the device allowing and rejecting the the access to any network. By using a specific rules and regulation for identifying if something is favorable or not, firewalls can prevent the harmful information’s from being entered and being stolen and keep malevolent code from being embedded into the network

As per the latest information from Global Information Security Survey – Indian edition, it has reported that the highest number of cyber-crimes have been reported in India, as per global ranking India ranks Number 2 in the term of targeted attacks. Though Banking and finance sectors suffer from highest number of cyber-attacks in India and in the sector such as manufacturing, healthcare and retail it is significantly low.

For businesses, cybercrime falls into two major areas. The first comes in form of attack on computer hardware through emails, viruses, botnets and network intrusion. The second type is in the form of financial fraud, it may include fraud, theft of information related to finance, and most common is phishing.

# origin of Cyber Crime

Many people won’t believe it or it may be very difficult for them to believe that the word HACK is not associated with computer or cybercrime at all, the word was used in 1960 were a student’s model train enthusiasts at MIT coined the term for the first time and describes it as the act of modifying a product or the procedure from is normal function and is to create problem in it. In simple terms hacking is the process in which one disturbs or changes the normal functioning of the device without being disturbing its normal procedure or by changing the whole device. A hacker is one who very cleverly changes the normal functioning of the device; he is one who finds the clever way to fix a problem with a product or to fix its problem.[[7]](#footnote-8)

However later this term hacker became intermingled with the malicious intent in the year 1970’s with the phenomenon known as phreaking, were extra ordinary tech savvy people use to disturb and subvert the computer system of that era. These hackers discovered the correct ID and tones that would result in free long distance services. They impersonated operators, duggs through telephone Co. garbage’s to find out the secret information’s and they performed endless and countless experiments on early telephone hardware in order to learn how to exploit the system. Law has to tackle difficulty with this sort of crimes, due in part of lack of legislation to aid in the criminal prosecution, and lack of technology became more sophisticated, so did the crime.

By 1980’s, cybercrime was an established channel which use to control and destroys the computer systems, it used to acquire information’s, and steal million of cash. With devastating increase in number of criminals of cyber there was the high need of establishment of new rules and regulation regarding this issue. The first law against the cybercrime was passed later in 1986 which was known as- The Federal Computer Fraud and Abuse Act- making destructive computer activities felony crime punishable by jail time and a huge fine will be imposed against them who will continue doing it.

Since those days, cybercrime have evolved a lot despite being reducing it has increased to a very great extent. New criminals range from single hacker to complex network of agents who are working day and night in unison to state-sponsored attacks across the globe. Threats are ever present as the world become more and more interconnected with each other each and every year, coupled with the emerging sectors (sectors related to the internet ) the opportunity for the criminals persists for the inventive and the daring hackers who are present across globe no matter whoever it/they may be either single hacker or a well-organized teams of hackers.

# the state of cyber crime today

In a recent US State of cybercrime survey, reported that three out four respondents recorded a security event during last 12 months, yet it was also reported that some of the organizations were suffering technology debts, which was estimated to be more than 1 trillion dollars. This clearly means that the companies are effectively spending on their IT Budgets on emerging businesses technologies while allowing the IT Infrastructure to ages into obsolesces until they cannot provide effective security functions.

There are many security deficiencies which are found in the organizations most susceptible cybercrime:

* Reactive or not planned cyber security spending by the countries.
* No assessment of the security capabilities of their third-party provides.
* Lack of understanding and/or assessment of supply-chain risks.
* Inadequate or nonexistent mobile device management and security.
* Lack of thorough employee security and awareness
* Insider threats and risk not adequately.[[8]](#endnote-2)

Despite of so many challenges, criminals are not stopping and cybercrime is increasing with the geometric rate. As per a survey around 900 attacks are detected per financial companies on an average, and also there are more than 9000 phishing attempts which are being detected on technology companies on an average. Phishing sites are targeting all the major technology players as well. The giant companies such as Google, Apple, Facebook, and yahoo are well the targets. When we see further, as well as Drop box, where insidious phishing sites could actually dupe users into uploading their files to cybercriminals who are doing such act.[[9]](#endnote-3)

As per one more research, on an average 85,000 malicious IPs are launched each and every day, bringing the average reputation score of all URLs worldwide to 65 percent. It is not only the case of one or two countries, whether we see United States of America or Russia, or throughout Asia. The result for all this is that the users have chances of 30% chance of phishing in one single year.[[10]](#footnote-9)

Cybercrimes are not only limited to the desktops alone; mobile devices have proliferated in recent years, and with them different kind of viruses enter into the device. Because of such open market space, the android platform is the home of various malware in particular. In an recent survey conducted 72% of the applications which are present on OS are suspicious, unwanted and dangerous for the device which may contain the malicious like Trojan with it.

As many of the experts possess that internal attack of cybercriminals are more dangerous than external one but we need to know that external attack of cybercrime is equally dangerous and sensitive in nature. Insider risk can be mitigated with robust employee awareness and security trainings. The biggest question arises is that, why does this behavior among the organizations persists? Data shows the fat that many decision makers and the organizations does not have full understanding of the extent or the seriousness of the threat which exists. Over the course of more than one year, business that have been fallen victim of the cyber criminals tends to the security measures more seriously than other who have not suffered any attack from the cyber criminals. Businesses with more than one thousands of laborers and employees also take cyber-crimes more seriously than others and have more processes in place to mitigate risk internally as well as externally.

# impacts

Attacks on American businessperson and organization increased by 176% in 2014- that is 138 successful attacks each week. Cybercrimes threatened the critical infrastructure of businessperson and the organizations and the governments across the globe, and can harm civilians in myriad ways. It is also estimated hundreds of billions of dollars have been lost from the globe economy, due to cybercrime, and unfortunately there is no signoff it showing down.[[11]](#footnote-10)

Cybercrime take in many forms such as:-[[12]](#footnote-11)

* Direct financial loss
* Damage to the company and brand reputation
* Loss of the sensitive data
* Mitigation and recovery costs
* Regulatory penalties
* SLA breaches
* Loss of jobs
* Sexual Harassment which includes stocking, grooming etc.

# direct financial loss

Cybercrime has emerged as one of the biggest enemy for the financial industry in today’s world it is greatly affecting the financial industry. Each and every day crimes are committed against the leading companies of the world whether they are giant such as Google, Microsoft or any other small organizations. Cybercrime cause a huge loss to the economics – to the tune to the close of 600$ billion. As per McAfee, when it comes to the cybercrime, European economy is hugely affected because of this, almost 84% of its GDP is affected because of these cybercriminals.

The influx of cyber-crime on the economy could be attributed to many factors, including easy accessibility of tools used to infiltrate the financial system of the country, these criminals adapted the new system of of technologies to do the crime against the companies and organizations, the expansion of new cyber-crime centers, and the high-tech system of of intelligence and the sophisticated system is used by these modern cybercriminals.[[13]](#footnote-12)

Raj Sawami, chief scientist, believes on the fact that cybercriminals are underreported by At least 95% which skews the $600 billion assessment and could mean costs are much more higher. The institutions need to protect themselves at every cost. With IP being so important it is costly to do the business in this digital era with maintaining high privacy level.

The question here is what type of cyber-crime has the greatest economic impacts?

Stolen IP and confidential business information online fraud, manipulation and the cost of securing network after hacking are some of the most devastating effects to the companies right now. Regulator and authorities can work together to deal with cybercrime, and try to implement a uniform system of security measures and defenses in technology. In addition, working as a team to place pressures on international state sanctuaries that protect cybercriminal’s is imperative.[[14]](#footnote-13)

# loss of sensetve data

Cyber criminals tend to make the loss of the sensitive data present in the desktop or any other electronic medium. In today’s competitive world many countries used this tactics of cyber-crime against their enemy country to get the sensitive data of their bout their infantry and etc., so that they may use it during the warfare or to increase the diplomatic pressure on them. Recently we may see many attacks on United States of America government sites by Chinese hackers. In today’s world almost each and every country has its own well organized team of hackers. Each one of them use against each other to steal their secret information, information about their country, their tactics, about their military and etc.

In the year 2017 when India bought the Scorpio submarine and received first of its kind, than within 1 week the system of the submarine was hacked, because of which India returned the submarine back to France. The dough was on Pakistan that they have hacked the system, also in the same year in month of November, the site of of Defense Ministry was also hacked, not only Ministry of Defense, Home Ministry was also hacked. Also the Chief opposition party President, Mr. Rahul Rajiv Gandhi’s twitter Id was also hacked. These are some of the example which came into limelight there are many other cases which does not come into news as will put down the image of the famous political leaders and the country.

In this changing world we need to focus on our net security we are planning to make India Digital but the time we will not secure our network we won’t be successful in this and won’t achieve the target of digitalization.

Some of the cyber-attacks in India are as follow:-

* SIM Swap Fraud (Navi Mumbai, 2018)
* Cyber attack on Cosmos Bank (Pune, 2018)
* ATM System Hacked of Canara Bank (Kolkata,2018)
* Attack on Wipro(2018)[[15]](#footnote-14)

# Sexual Harassment which includes stocking, grooming etc

Businesses have seen a significant and exponential growth in their scope with growing technology and its innovative application to multiple facets of businesses. In a environment where the firms are able to attain technology and to increase potential in such a way that it is cheaper, it has become possible to run the firm firmly, even from the confines of one’s own house. This have been mostly possible because of the lockdown era where almost all of the business are closed and the employees are working from home and they use such technology such as what Sapp, Facebook, Instagram, meet, team for the mode of communication. This has led to many serious problems in the society because improvement in technology cannot change the mentality of the people in the society.

Online sexual harassment which is popularly known as digital harassment is just a detrimental to a person as in-person sexual harassment. In fact they are just the same side of the coin people use to differentiate between them. In fact it should be understood by the people and the employers especially, that online sexual harassment and in-person sexual harassment are not two different types of harassment but merely an extension of one another. Behind the screen it is mentality of the people who are harassing that they would not be known and feel they are safer and act more braver than they are and because of which it is more harmful in action.

As per the data eight out of ten people in India have experienced some form of sexual harassment, with almost 41% of women facing sexual harassment in India on internet India ranks one of the top country in this malicious act.[[16]](#footnote-15)

In an online survey of sample size of 1035 people in the year 2017 from the Tier 1 cities of the Country Indiato under the exposure of online harassment in India. The most common type of sexual harassment which was found that is abuse and insult by the harasser which was reported by 63% of the participant. Which was followed by malicious gossips 59% threats and asking nudes 54% trolling 50% attacks/abuses from the coordinate group 49%. So we may say that 41% of the women has suffered sexual harassment as per reported cases, another online and as per one another data four out of ten women in America suffers from Sexual harassment, and 62% of them consider it to be serious problem of its kind. Also per one data, 28% in 2018, 22% in 2016, 25% in 2014 of 1000 18plus Americans were bullied badly, harassed and threatened on the social media with the cheaper data plan and easy associability to the social media by the common people, and with the advancement in technology and the situation like such were each and every people use social media and communicate with each other daily and continues there is high probability that the online harassment or the sexual harassment would be higher in Number than what is shown in the data because in the present sample of data were only 1035 samples were taken that too from tier 1 cities so there is high probability that the number would be more and more because many such cases are not reported properly as the people are unaware of the law and the regulations, and also many such people to maintain their self-esteem and respect in society don’t come forward and complain to such acts done.

Law has always found it very difficult to find the and catch up the speed of the technology. Recently the office of special inspector general police, Maharashtra cyber has issued an advisory warning that admins of the WhatsApp group along with the users will be punished for posting objectionable posts in the group. While disinformation’s and the false rumors on media group is an increasing and legitimate problem, such advisory seems to have no basis of law as more detailed in a recent Live Law Article published.[[17]](#footnote-16)

Most of the organizations during this lockdown are closed down and the management is running via online mode like WhatsApp and other online modes. Inappropriate communications between the employees can find its way into the communication in private as well as in public in group chat. In such a case the group admin would not be libel under the act, only such person who are sending messages of such would be libel under sexual harassment of women at workplace(prevention, prohibition and redressal)Act 2013. It would be the responsibility of the employer to take note of such instances, find ways to prevent it and to ensure that inappropriate instances are appropriately addressed by the law. [[18]](#footnote-17)

# online child abuse

Online Child abuse is a kind of cyber-crime and child abuse which is not happening face to face but via online mode, in online child abuse the face to face contact is not necessary nor it requires physical contact. However, online abuse can result in negative face to face consequences in the form of rapes, forcible sexual harassments and abuse and etc., in the United States of America, online child abuse is recognized as a form of child abuse by the National Society of the Prevention of Cruelty to Children.

Online abuse may occur to the child not only via cyber bulling, grooming, and sexual abuse, but it requires the use of World Wide Web or cellphones and internet, increasing its significant with changing world. The victim may be somehow stranger or the old victim who was previously attacked by these criminals and now they have informed other and the other people were also doing same with the old target. In the report a presented by the Data and the Society Research Institute and the Centre for Innovation Public Health shows in its research that the 72% of the users of Internet in United States of America have witnessed the the some or other form of online harassment or the other kind of abuse, while the other 47% of the women have experienced it. Though the data did not differentiated between the genders but at the same time it also shows that the wider rate of risk was with the women.

Government across the globe has tried to acknowledge the importance of recognizing and combating the online abuse against the children in different countries. In the United States of America this effort is led by the Internet Crimes Against the Children Task Force. This task force includes of 61 people engaging with the 4500 federals, state and the local law enforcement agencies al with the goal of combating online abuse of children.[[19]](#footnote-18)

# cyber bullying

Cyber bullying or the internet bullying, occurs when an individual or group of electrically active people use to distribute false, or negative information about the person which causes humiliation and distress to him is known as cyber bullying. This information may be some confidential information’s or the private information which is related to her/his personal life. Cyber Bullying may happen with any kind of device which is able to connect with the internet like; Desktop, laptop, mobiles, tabs etc. and it does not require any kind of physical meeting or activities, it does not require perpetrator to be in the same vicinity of the victim. A research conducted by the researchers of the Canada found that the children who were victims of the cyber bullying and also bullied in school were more likely to bully other over cyberspace.[[20]](#footnote-19)

Studies found out that there has been significant increase in number of cases of online bullying though number of cases were not reported, these cases are not reported because the victims have the feeling of guilt, incompetence or despair. More than 37% of the victims of the cyber bullying does not report to the abuse done to them. According to the statistics of the cyber bullying from the I safe foundation an Non-Government Organization, more than 50% of the adults have been victim of the online cyber bullying, where one third of them are threatened online.[[21]](#footnote-20) This does not differentiate between the Boys or the Girl, Boys and Girls both are equally harassed. Of the cases which were reported of cyber bullying in them 25% of them repeated the same again. The Hardford County Examiner reported that far more than 50% of child victim hid the issue from their parents which this incident of cyber bullying took place with them.[[22]](#footnote-21) In 1 out of 10 cases of cyber bullying took place in them the nude and damaging pictures were taken of them without their permission and with the same blackmailing was done of the people, in these cases of cyber bullying was done majorly of the girls, we can also say the number of victims in cyber bullying the girls are more than the comparison with the boys.[[23]](#footnote-22) There are many tends which shows that this number of people or this age of the people are targeted by these cyber criminals in majority. Some research says that young age of LGBTQ community is targeted and some other says that the school age children’s are especially targeted of these e cyber bullying. [[24]](#footnote-23)

As per a study conducted in the year 2011 it found mainly four main reasons which was reasons for targeting other over the internet: informal social control, entertainment, social control and dominance. Informal social control means applying pressure on the other person to change his/her behavior. Entertainment which is commonly known in simple language trolling, intentionally, humiliating, annoying or bothering someone for the purpose of eliciting an emotional response of eliciting an emotional response for the bully’s enjoyment and for the enjoyment of the people who visit or see that meme or the post made on the people without his/her permission. Dominance means the attempts of hurting someone, humiliating someone, or gaining access to their personal information of their life like secrets, explicit photos, messages etc., perpetrators of the trolling are known as the trolls which is included and accessible in the part of the cyber-crimes.

As mentioned above cyber-crime or cyber bullying is common between the age of the people below eighteen years of age, the school boys and girls are the primary target of the cyber bullies, victims of the cyber bullying often feel negative about themselves after being bullied. It is very common act of the victims because they start remaining very alone and in afraid all kind of negative thoughts start developing in their mind, this is all because it has negative effect on their self-esteem. Cyber bullying affects the mental status of the people who have suffered that, a research says that the victims who are below eighteen don’t inform to their parents just because they think that their parents won’t understand or they will target their own ward. This fear infiltrates in their mind and they don’t say to their parents. This creates more tension in their mind because of which they go to depression and because of which they also conduct suicides. These criminals mainly target the girls, the young girls who are acting more frank and become easy target of the criminals. Biggest is example of the cyber bullying is the Blue Whales Game, in which they totally divert the mind of the players by giving them some tasks and at last they make them to do suicide by making them afraid and by threatening them.

# grooming

Grooming is the phenomenon which occur on or offline. When the grooming occurs online, however, this is frequently done without the knowledge or compliance of any adult. When children can use the internet without supervision, there is more room for potential abuse.[[25]](#footnote-24)Online grooming can be taken in many of the things.[[26]](#footnote-25)The most important thing in this is that they build a trusting relationship with the child and when they think that their relationship is strong and the child has started trusting him then he/she engage in either online or in person sexual relationship. The internet is used as a medium of to lead a child to potential sexual behavior grooming can also be used in other kind to exploit the child and to earn money by blackmailing them by threatening them to expose their private photos or videos. The two forms may be used by the blackmailers with groomers convincing them to send the nude and the videos which is not appropriate and to perform the sexual activities and blackmailing them, the victim, by threatening to release to release information about them.[[27]](#footnote-26)

Online grooming occurs in variety of way. Mostly they occur in the chat rooms or the social networking sites the criminal’s use of make the initial contact with the person who is the victim. Groomers may use the social networking sites such as dating sites, photo-sharing apps, and other gaming apps to out their victims. After establishing a trust worthy relationship with them which is a kind of online relationship, the groomer turns conversation to more personal matters, frequently sexual topics. Groomers finding the right time starts the sexual topics and sex chat with the victims send nude photos or videos, start the sexual video chat via webcam, or persuade the victim to meet the sexual acts. Groomers in maximum cases they are not the strangers, they can be family member or the relatives or the cousins they use the medium of internet to strengthen the old relationship then after they think they are successful they start sex chat and the exploitation of the child.

Grooming and the overall line abuse of the small or the teen children is an issue of growing concern in the modern technology era. Victims of the online grooming are frequently young teens, with the majority of the victims being between the age of 12 and 15. In the year 2012 literature review of research in the area conducted by various English scholarly institutions. It was later on found that 9% of the internet user today aged between 12 and 17 reported unwanted online sexual solicitations or the attempted grooming.

# sexual abuse

Sexual abuse, which is commonly known as molestation, is abusive sex behavior by one person upon the other who is mainly the teens. It is often perpetrated using the force or by taking advantage of another. When the se of the force is of short term and of short duration, or is infrequent, it is known as sexual assault. The offender is commonly known as a sexual abuser or the molester. The use of a child or the three individuals younger than the age of consent, for the sexual stimulation is referred to as child sexual abuse or the statutory rapes.[[28]](#footnote-27)

The victims of this type of sexual abuse are girls and the women in majority while there are many few cases where boys are found to be victims. Spousal sexual abuse is a kind of house violence which is done to threat unwanted sexual contact or the forced sex by a women husband or ex-husband, it may constitute rape, depending on the jurisdiction, may also constitute an assault. [[29]](#footnote-28)

Child sexual abuse is a form of a child abuse I which a child is abused for the sexual satisfaction of an adult or the adults. It may include direct sexual contact, the child or the adult or otherwise an older person who is nearly old aged engaging in indecent exposer to a child with intent to gratify their own sexual desires or to the intimidate or groom the child, and asking him/her to engage into the sexual activities like pornography to a child, or using to produce the child pornography.[[30]](#footnote-29)

Effects of the child sexual abuse includes shame, self- blame, depression, anxiety, post-traumatic stress disorder, self-esteem issue, sexual dysfunction chronic pelvic pain, addiction, self-injury dysfunction, attempt of suicide, borderline personality disorder and propensity to re-victimization in adulthood.[[31]](#footnote-30)Child sexual abuse always leads to the suicide of the child.[[32]](#footnote-31)

# how the cyber-crime be prevented

Many Multi-National Companies suffers difficulty in tackling the problem of cyber-crime; not only they need to ensure their clients’ endpoints are at most secure and safe, also they need to safeguard their own servers, system and the devices as well from the cyber-criminals. Therefore, they need to have fast and the effective and easily deployable antivirus and also the anti-malware software’s in the place that will also optimize efficiency and keep their users safe at the same time.

Further, the multi-national companies need to be sure that the proper backup and disaster recovery systems are in such a place that on servers and on the users endpoints should be the unthinkable happen as a result of the attacks by the cyber criminals. Downtime may result in the damage of the reputation as well as the clientele of the multi-national companies, so the system need to be prepared, secure, and can be easily restorable in the events that a user clicks on the phishing links on a phishing links and the unleashes dangerous and malicious codes. [[33]](#footnote-32)

Multi-national companies today are not only limited to securing SMB computers –the explosion of devices, from the smartphones to the tablets, have created have tremendously increased the demand for the electronic c devices and mobile device management (MDM) to separate the password policies are enforces, anti-virus software’s tools are upgraded. SMSs are increasingly looking for to the MSP to be at the forefront of combating cyber-crime so they can focus on moving their business forward.[[34]](#footnote-33)

# india: government launches online complaints mechanism to fight sexual harassment

In India the Ministry of women and child development in the year 2017, November 6, launched an online mode of filing the complaint management system for the women who are doing work in both the public and the private sector and in different Multi-National Organizations to file the complaint against the sexual abuse and the sexual harassment in the workplace.

The online complaint management system popularly known as the SHE BOX was launched by then Women and Child Development Minister Shri Mati Maneka Gandhi Ji, Minister launched to ensure the effective implementation of the Act known as Sexual Harassment of Women at Workplace Prohibition and Redressed Act, 2013.

Sexual Harassment is any unwelcome Act or the behavior as explained above thoroughly, here is brief about it:-

* Physical contact or advance
* Any other physical, verbal or non-verbal conduct of the sexual nature.
* Making sexual colored comments

Sexual harassment at workplace can take in various methods, some of them are as follow:-

* Unhealthy way of touching, hugging and kissing
* Staring or leering
* Suggestive comments and the jokes
* Unwanted requests to go out
* Intrusive question about another person’s private life or the body parts
* Behavior that would also be an offence under the criminal law, such as physical assault, incident exposure, sexual assault, stalking or obscene communication.

WHAT IS SHE-BOX?

The Woman and Children Development Ministry has made it very mandatory for all the organization to set up the internal complain committee to ensure the safe environment for all the working women, All the complaints lodged by women will be monitored by the women and children development ministry to ensure that necessary action is taken by the ICC of the organization.[[35]](#footnote-34)

A complaints can be registered by any women by accessing the online portal, once the complaint has been submitted to the portal of the ministry launched site, it will be directly submitted to the ICC of the concerned organization or the form related, through this portal, WCD Ministry as well as the complaints can monitor the progress of the inquiry conducted by the Internal Complaint Committee (ICC).[[36]](#footnote-35)

HIGHLIGHTS/FEATURES OF THE SHE-BOX

It includes:-

* Speedier response to complaints the ability of women working in the government as well as the private organization to lodge a complaint.
* The eligibility of those who want to file a written complaint with the concerned ICC constituted under the SH act to fill their complain though the portal
* The option of interaction with the WCD Ministry with an assured time bound response
* The assurance of protecting the dignity and safety of the customer[[37]](#footnote-36)

# conclusion

In this era of technology, the role and usage of net is increasing worldwide apace, so it becomes straightforward for cyber criminals to access any knowledge information |and data} with the assistance of their knowledge and their experience. Cyber-crime is associate degree unlawful act or a menace that has to be tackled firmly and effectively. there's a requirement to make additional awareness among the folks and essentially users of net concerning cyber house, various varieties of cyber-crime and a few preventive measures as “Prevention is often higher than cure”, thus it's seriously suggested to require some previous precautions whereas in operation the web. Security these days is changing into a distinguished and major concern. within the following paper, some security problems square measure introduced, threats, Trojans, and attacks over net. laptop security becomes crucial in several of the technology-driven industries that operate the pc systems. laptop security is nothing quite laptop safety. infinite vulnerabilities associate degreed laptop or network based mostly problems square measure acts as associate degree integral a part of maintaining an operational business.

# REFRENCES

* < http://en.m.wikipedia.org/wiki/online\_child\_abuse> accessed on 1st May 2020.
* < http://en.m.wikipedia.org/wiki/online\_child\_abuse> accessed on 1st May 2020.
* Cyber Crime and Security –

IJARCSS<http://ijarcsse.com/Before\_August\_2017/docs/papers/Volume\_6/4\_April2016/V6I4-0201.pdf>accessed 01 May 2020

* Internet security - Wikipedia<https://en.wikipedia.org/wiki/Internet\_security>accessed on 01 May 1, 2020
* <https://www.isafe.org/outreach/media/media\_cyber\_bullying> accessed on 01 May 1, 2020
* <https://www.isafe.org/outreach/media/media\_cyber\_bullying > accessed on 01 May 1, 2020
* <https://en.m.wikipedia.org/wiki/Cyberspace>accessend on 1st MAY 2020.
* <https://en.m.wikipedia.org/wiki/National\_Society\_for\_the\_Prevention\_of\_Cruelty\_to\_Children>accessed>on may 2020
* <https://en.m.wikipedia.org/wiki/National\_Society\_for\_the\_Prevention\_of\_Cruelty\_to\_Children> ACCESSED ON MAY 2020
* <https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/india-sexual-harassment-online-complaints.aspx>accessed on May 2020.
* <[https://en.m.wikipedia.org/wiki/National\_Society\_for\_the\_Prevention\_of\_Cruelty\_to\_Children>accessed](https://en.m.wikipedia.org/wiki/National_Society_for_the_Prevention_of_Cruelty_to_Children%3eaccessed) on may 2020
* <merchantriskcouncil.org>accessed on 3 May 2020
* <economicstimes.in>accessed on May 2020.
* <https://www.interpol.int/en/Crimes/Cybercrime>accessed on May 2020
* Vatsalchorera<poshatwork.com>accessed on May 3, 2020
* Vatsalchorera<poshatwork.com>accessed on 4 May, 2020
* <cac task force program>accessed on 4 May 2020.
* <https://www.interpol.int/en/Crimes/Cybercrime>accessed on May 2020
* <https://economictimes.indiatimes.com/tech/internet/newslist/60870273.cms>accessed onMay 2020.
* <https://economictimes.indiatimes.com/tech/internet/newslist/60870273.cms>accessed on May 2020
* <https://economictimes.indiatimes.com/tech/internet/newslist/60870273.cms>accessed on May 2020
* <https://economictimes.indiatimes.com/tech/internet/newslist/60870273.cms>accessed on may 2020
* < https://en.m.wikipedia.org/wiki/Online\_child\_abuse> accessed on 4 May 2020.
* <https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html>accessed on May 2020
* <https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html>accessed on May 2020
* <https://capmh.biomedcentral.com/articles/10.1186/s13034-019-0292-1>accessed on May 2020
* < https://en.m.wikipedia.org/wiki/Online\_child\_abuse> accessed on 5 May 2020.
* <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html>aceesed on 6th May 2020.
* <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html>aceesed on 6th May 2020.
* < http://www.continuum.net/resources/mspedia/cybercrime-and-security-overview> accessed on 6 May 2020
* < http://www.shrm.org/resourcesandtools/legal-and-compliance/emplyement-law/pages/india-sexual-harassment-online-complaints.aspx> accessed on 6 May 2020
* < http://www.shrm.org/resourcesandtools/legal-and-compliance/emplyement-law/pages/india-sexual-harassment-online-complaints.aspx> accessed on 6 May 2020.
* < http://www.shrm.org/resourcesandtools/legal-and-compliance/emplyement-law/pages/india-sexual-harassment-online-complaints.aspx> accessed on 6 May 2020

# ABOUT THE AUTHOR

Kshitij Chandra Pandey is a first year law student from Indore Institute of Law, Indore. He has a strong academic background, and he has published various Articles in NyayDisha research paper in Corpus Juris and others journal. He has keen interest in Constitutional Law, Contract Law and Corporate Law. He wants to choose Judiciary as his future and has kept Corporate as a secondary option.

1. <<http://en.m.wikipedia.org/wiki/online_child_abuse>> accessed on 1st May 2020. [↑](#footnote-ref-2)
2. < http://en.m.wikipedia.org/wiki/online\_child\_abuse> accessed on 1st May 2020. [↑](#footnote-ref-3)
3. Cyber Crime and Security - IJARCSS<<http://ijarcsse.com/Before_August_2017/docs/papers/Volume_6/4_April2016/V6I4-0201.pdf>>accessed 01 May 2020 [↑](#footnote-ref-4)
4. Internet security - Wikipedia<<https://en.wikipedia.org/wiki/Internet_security>>accessed on 01 May 1, 2020 [↑](#footnote-ref-5)
5. <https://www.isafe.org/outreach/media/media\_cyber\_bullying> accessed on 01 May 1, 2020 [↑](#footnote-ref-6)
6. <https://www.isafe.org/outreach/media/media\_cyber\_bullying> accessed on 01 May 1, 2020 [↑](#footnote-ref-7)
7. <[https://en.m.wikipedia.org/wiki/Cyberspace>accessend](https://en.m.wikipedia.org/wiki/Cyberspace%3eaccessend) on 1st MAY 2020. [↑](#footnote-ref-8)
8. [↑](#endnote-ref-2)
9. [↑](#endnote-ref-3)
10. <[https://en.m.wikipedia.org/wiki/National\_Society\_for\_the\_Prevention\_of\_Cruelty\_to\_Children>accessed](https://en.m.wikipedia.org/wiki/National_Society_for_the_Prevention_of_Cruelty_to_Children%3eaccessed)>on may 2020 [↑](#footnote-ref-9)
11. <https://en.m.wikipedia.org/wiki/National\_Society\_for\_the\_Prevention\_of\_Cruelty\_to\_Children> ACCESSED ON MAY 2020 [↑](#footnote-ref-10)
12. <https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/india-sexual-harassment-online-complaints.aspx>accessed on may 2020. [↑](#footnote-ref-11)
13. https://en.m.wikipedia.org/wiki/National\_Society\_for\_the\_Prevention\_of\_Cruelty\_to\_Children [↑](#footnote-ref-12)
14. <merchantriskcouncil.org>accessed on 3 May 2020. [↑](#footnote-ref-13)
15. <economicstimes.in>accessed on may 2020. [↑](#footnote-ref-14)
16. <https://www.interpol.int/en/Crimes/Cybercrime>accessed on May 2020 [↑](#footnote-ref-15)
17. Vatsalchorera<poshatwork.com>accessed on 3 May 3, 2020. [↑](#footnote-ref-16)
18. Vatsalchorera<poshatwork.com>accessed on May 4, 2020. [↑](#footnote-ref-17)
19. <cac task force program>accessed on 4 May 2020. [↑](#footnote-ref-18)
20. <https://economictimes.indiatimes.com/tech/internet/newslist/60870273.cms>accessed on may 2020>accessed on may 2020 [↑](#footnote-ref-19)
21. <https://economictimes.indiatimes.com/tech/internet/newslist/60870273.cms>accessed on may 2020>accessed on may 2020 [↑](#footnote-ref-20)
22. <https://economictimes.indiatimes.com/tech/internet/newslist/60870273.cms>accessed on may 2020 [↑](#footnote-ref-21)
23. <[https://www.interpol.int/en/Crimes/Cybercrime>accessed](https://www.interpol.int/en/Crimes/Cybercrime%3eaccessed) on May 2020 [↑](#footnote-ref-22)
24. <https://economictimes.indiatimes.com/tech/internet/newslist/60870273.cms>accessed on may 2020>accessed on may 2020 [↑](#footnote-ref-23)
25. <[https://en.m.wikipedia.org/wiki/Online\_child\_abuse>accessed](https://en.m.wikipedia.org/wiki/Online_child_abuse%3e%20accesed)on 4 May 2020. [↑](#footnote-ref-24)
26. <https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html>accessed onmay 2020. [↑](#footnote-ref-25)
27. <https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html>accessed on may 2020 [↑](#footnote-ref-26)
28. <[https://kidshelpphone.ca/get-info/what-online-sexual-exploitation-and-abuse>accessed](https://kidshelpphone.ca/get-info/what-online-sexual-exploitation-and-abuse%3eaccessed) on May 2020 [↑](#footnote-ref-27)
29. <https://kidshelpphone.ca/get-info/what-online-sexual-exploitation-and-abuse>accessed on May 2020 [↑](#footnote-ref-28)
30. <[https://capmh.biomedcentral.com/articles/10.1186/s13034-019-0292-1>accessed](https://capmh.biomedcentral.com/articles/10.1186/s13034-019-0292-1%3eaccessed) on May 2020 [↑](#footnote-ref-29)
31. <[https://en.m.wikipedia.org/wiki/Online\_child\_abuse> accessed](https://en.m.wikipedia.org/wiki/Online_child_abuse%3e%20accesed) on 5 May 2020. [↑](#footnote-ref-30)
32. <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html>aceesed on 6th May 2020. [↑](#footnote-ref-31)
33. <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html>aceesed on 6th May 2020. [↑](#footnote-ref-32)
34. <http://www.continuum.net/resources/mspedia/cybercrime-and-security-overview>accessed on 6 May 2020 [↑](#footnote-ref-33)
35. <<http://www.shrm.org/resourcesandtools/legal-and-compliance/emplyement-law/pages/india-sexual-harassment-online-complaints.aspx>> accessed on 6 May 2020. [↑](#footnote-ref-34)
36. < http://www.shrm.org/resourcesandtools/legal-and-compliance/emplyement-law/pages/india-sexual-harassment-online-complaints.aspx> accessed on 6 May 2020. [↑](#footnote-ref-35)
37. < http://www.shrm.org/resourcesandtools/legal-and-compliance/emplyement-law/pages/india-sexual-harassment-online-complaints.aspx> accessed on 6 May 2020. [↑](#footnote-ref-36)