Volume 10, May 2020 ISSN 2581-5504

"Evolution of Cyber Crime and Measures to Control it"

Gayathri . V
SASTRA Deemed to be University,
Thanjavur

****Nishitha Dattan. P***
SASTRA Deemed to be University,
Thanjavur

1. Abstract

In our generation there is a rapid development in all fields. Similarly, we can observe wide range of changes in crimes. In recent times, crimes on internet has been increased to a large extent which is also known as "cybercrime". One of the most important challenges in cybercrime is identifying and locating the person who has committed the crime. The reason for this accusation is instead of correct person user id, they may create fake ideas through which they will commit the crime. Today, the access to internet is unlimited to any person of any age from any place and can get access for internet. The contents in the internet are mostly inappropriate to the younger generation. This results in the isolation from their parents and also leads to psychological problems like committing suicide, depression which results in killing of others. The reason for their unusual behaviour is through online games which are not considered to be properly approved and dangerous which make them unable to differentiate between reel and real world. The personal data used by the people in social media like twitter, Facebook, Instagram, etc. are being illegally used by the owners of the application for their personal gain. Here we suggest some solutions for the above said crimes. As an individual the person should do the following. Increasing the fire wall protection. The steps for verification should be increased. From the side of government, the following measures can be taken, enacting new laws based on the current trend and situations. Increasing the awareness to all age groups. Regulating the contents and implement the restrictions for websites. Our paper discusses about the various kinds of crimes on internet. We suggest some measures to reduce the crimes and to make internet more useful.

2. Introduction:

The years are categorised based on the things developed in that period and it is called in that name. The 20th century is known as "technological age". Many advancements have been made in the technology and people are indulged with lot of information. The crimes are normally committed by the people in the previous days. As we are in the dynamic world the crimes are committed not only by people particularly by the machines or through machines. It is committed by computers and the crimes are known as "cybercrimes" or "computer crimes". In our generation it is hard to find out the correct person who has committed the crime. In order to protect the innocent person, the development in technology helps to punish the appropriate person. The crime rates are increased on internet than it is committed directly by the persons. It is hard to investigate and to punish the person aptly. To give equal justice punishments are widely discussed and laws are enacted to protect the people of country. Many sub divisions in cybercrime has been developed. The various solution to overcome the

Volume 10, May 2020 ISSN 2581-5504

problems are suggested. It is important to know the current trends and its impact in our present life.

3. Meanings:

Crime: The offence punishable by law.

Cyber: Through computers, virtual reality and information technology.

Cybercrime: The offence committed through computer or internet.

4. Evolution of cybercrime:

The cybercrime is usually committed with the help of computer. The crime has evolved during the development of computers. After the advancement of abacus, communication system has a wide spread extent. Computers are considered to be the better version for calculation. They are actually larger in size. In the later days, computers are used to store the information in files. Initially it is used by government companies and later by some financially larger firms for their business firms. Crimes are committed in the early times where the awareness in using computers did not widely spread among the people. Along with the development of websites cybercrime also reached a great height. The cybercrime has its origin from 80s and known to people by 90s and reached its maximum extent in the 20^{th} century and become more prominent and the crime rate reached its maximum limit in the 21^{st} century. In this period computer can be used both as a tool and target.

Computer as a target: In places where only one operating system is important and it has many sub systems. It is used by government in the places of military and storing confidential information regarding the functions and policies of government. If the hackers attack this single system the whole thing will be stolen or get destroyed. In these places' computers are used as target.

Computer as a tool: If individual is the only target computer can be used as a tool to threaten or to blackmail them.

5. Phases in the development of crime:

1971: It is period where "wire fraud" has been well accomplished. It is a crime committed through telephone. It is well known by the people that the telephones used in America has special tone. They wanted to create the tone using some crops which produces similar sounds. With the help of that they try to make free calls. The persons are called as "phreakers".

In the same year a scam occurred by e-mail which allowed for malware to be delivered in the person inbox.

Volume 10, May 2020 ISSN 2581-5504

[1]**1980:** "captain zap" is the first person to be convicted in a cybercrime. His original name is "Ian Murphy". A big firm called "AT &T" was hacked by him and he changed the internal clock to charge off – hours rate at peak times and 1000 hours of community service and 2.5 years of probation, slap on the wrist. The scam paved the way for the movie "sneakers".

[2]**1982:** "Elk Cloner" is a virus that spread through floppy disks. It is written by a 15-year-old boy for fun. It affected the functioning of "Apple II" operating system. It paved the way for virus attacks.

In the 90s the world wide web has been developed and it is used by all people. The crimes committed by the people are categorised based on their years.

[3]**1990:** In this year there are two famous gangs where they started to hack one and other for fun. After sometime they started to hack common people in order to steal their personal information. It resulted in "credit card theft" and "wire fraud".

[4]**1993:** "Kevin Paulson" is convicted for hacking the phone systems. He is punished for 5 years and a first person who created a ban on internet. He particularly selected the telephone lines used by the customers calling for radio station called "LS" radio to assure that every person who is calling will definitely win in that contest. At one period he is in the 'most wanted' list and then he was arrested.

1994: A student in UK uses the "blue boxing" and "commodore amiga" personal computer online program and he uses this information to hack the nuclear weapons, NASA. They allowed the black hat hackers to access the world wide web to strap that information.

The number of hackers has been greatly increased in number during this period. The next attack which is wide spread due to advancement in technology. It has its origin from the year 2000.

2000: Online attacks spread like a forest fire in the internet world. Credit card details are made as online and it results in the stealing of information and reduces the use of CD. Fake news causes 50% damage to all information that are stored in computer. The email is not considered to be safe as many unwanted messages will destroy the computer. It happens due to the development of many viruses. The people felt that usage of email should be banned for a certain period of time.

2002: "Shadow Crews" is a website launched to teach how to commit multitude of crimes and it longed for 2 years. It teaches how not to be get caught. The head of this is black hat hackers. Nearly 28 persons are arrested. It is shut down by a secret operation.

[1]https://www.washingtonpost.com/news/the-switch/wp/2015/08/05/this-80s-era-criminal-hacking-law-scares-cybersecurity-researchers/
[2] https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/
[3] https://www.scribd.com/doc/300646487/Fraud-and-Scams-in-Banking-Sector
[4] https://www.le-vpn.com/history-cyber-crime-origin-evolution/

Volume 10, May 2020 ISSN 2581-5504

[5]**2003:** "SQL Slammer" is considered to be the fastest spreading virus. It multiplies and affects 75,000 machines within 10 minutes.

[6]**2007**: The wide spread of malwares and theft has been increased to a million times. The damage caused is increased to billions.

2017: "Wanna Cry" is a software virus that spreads itself and multiplies and affects the operating systems. It is the main incident to be noted in that year.

The above said are considered to be a time phase where internet crimes have been gradually evolved. At present we can face many advancements in the internet world. The crime rate has multiplied in the great numbers. One important solution which prevailed in the previous years was the use of "VPN" which is nothing but virtual private network. It helps to protect the information in houses and business firms. Another important solution which was established by the government is the "cyber security". A man who invented the email again has sown the seed for cyber security by developing a program called "reaper" against the program called "creeper". It became known to all by the "Morris Worm". The two are considered to be the important solutions among all from the early time.

The countries are arranged in descending order based on their crime rate. China has ranked first, United States, Turkey, Brazil, Russia. These are considered to be top five countries where cybercrime occurs. As a luck we did not attain the first five positions. But comparing to the previous years, the crimes are increased like global warming in our present generation. Within 10 years we can see many advancements in technology with new crimes on internet. Apart from known crimes on internet many new crimes have developed and its explanation can be seen here.

6. Categories of crime on internet:

The main aim of all crimes is to earn money or to make more profits by the way of threatening or by looting. In the internet world also to earn property or to defame or to threaten the people by earning more money to live a well organised and rich life. The main of a person is to lead a rich life and to earn higher than what they expected as the world is changing into a new phase people started to think in a higher order than required. [7]The crimes on internet can be categorised as crimes against people, property and government.

Crimes against government is considered to be an attack on nation sovereignty. It involves hacking, confidential information, cyber warfare, cyber terrorism and pirated software.

Crimes against people includes cyber harassment, stalking, credit card fraud, cyber trafficking, spoofing, identity theft, online libel or slander and phishing which is a common attack against the individual users.

[5] https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/
[6] https://www.le-vpn.com/history-cyber-crime-origin-evolution/
[7] https://www.swierlaw.com/faqs/what-are-the-three-types-of-cyber-crimes-.cfm

Volume 10, May 2020 ISSN 2581-5504

Crimes against property involves DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement and IPR violations. It happens through computer and server.

Hacking: The information is accessed by a person through an unauthorized way. It is done through cracking of passwords. The hacking can be done on a single system or on multiple systems. It is always with bad or malicious intent to steal the confidential information and stealing the funds and monetary resources. The person who is well versed in doing this process is known as "hackers". The hackers can be categorised as white hats, black hats and grey hats.

In a similar way, hacking can be done in mobile and is called as "mobile hacking". It happens by hearing the voice messages, telephonic conversations to force the victims to do what they wanted. It is also known as "phone tapping". It has increased by the widespread use of android or smart phones.

Phishing: It is considered to be a kind of hacking. The major victims for this are the banks. It functions by copying the original website. Apart from the original users the other members without any doubt gathers the personal information like pass words, credit card details. It is punishable by law.

Pharming: It is a scam with a bad motive or intent. The personal computer has the malicious code in their respective computers. It misleads the person if they click that code without their knowledge and makes them to access the fraudulent websites. It is also known as "phishing without lure".

Malvertising: The websites are full of advertisements. If the person clicks that with or without their knowledge they will be directed to fake or fraudulent website. Sometimes automatically the malwares will be downloaded.

Virus: To corrupt the information on the website. This happens if they click into the website without their knowledge. It is a self-replicating process. It includes all kinds of worms.

Ransomwares: It is considered to be a malware attack. It encrypts the file and steal many confidential and personal information with the help of 'public key'.

Logic bombs: It is neither virus nor worms. It is also called as "slag". It has malicious code. If it is designed to activate in a particular time, it is known as "time bomb".

Cyber terrorism: It involves destruction of infrastructure as a whole and involves affecting all parts of system includes hardware and software with an evil code that is already present in the computer. It spreads automatically.

Web jacking: It is operated by a single person to steal the information of a person, password and other related things. It will direct the victim to share all their information to the head of web jacker which help them to threaten others and to earn more money.

Volume 10, May 2020 ISSN 2581-5504

Cyber extortion: In this type of crime, the person threatens in order to earn money. They will send messages and emails saying that the service is denied and it occurs repeatedly. Until the person is paying the amount demanded by the hackers, they will not provide the service promptly.

Pirated Software: A original software is shared or circulated to millions of users without a proper authorised license. Without any legal means it is copied and used for many illegal purposes.

Cyber Warfare: It used by the states or country in the military services for stealing other persons information without their knowledge for the personal gain or for the country benefit.

Cyber Harassment: In the way of emails, and messages by sending that person photos and threatening them. Text harassment in the way of texts. It may be in the form of letters too.[8] It is also called as "cyber bullying" or "online harassment".

Cyber Stalking: It involves the use of electronic media which involves the following of persons through online without their knowledge. It includes harassment, embarrass, threatens the victims. The information in social media helps these types of stalkers to make unwanted calls to the victims.

Credit Card Fraud: The term includes both stealing that is theft and fraud by electronic mode. The cards include both credit and debit cards used for online transactions which is wide spread in the recent times. It can happen if the card is stolen or if the person shares the pin number to the unauthorised persons. It is committed by the person to defraud the huge sum of money or to make many purchases without that person knowledge.

Identity theft: It is committed by persons in order to make other persons to suffer loss or any disadvantage. Instead of the original person by using his name or identity or any other person identification in online to earn money.

Online libel or slander: Libel or slander is a form of defamation in torts which is punishable. It is also known as "cyber defamation". It involves spreading of fake or false information in the internet in the social media.

Cyber trafficking: It involves trafficking of humans for exploitation, forced labour and forced sex-oriented practices in order to earn more. The business dealings happen through online by using codes. It helps them to earn more profit and it is punishable also.

DDoS attacks: The full form of DDoS is "distributed denial of service attack". It is operated from a single source. There may be multiple victims and also from different regions. It involves blocking of any particular website for certain period may be permanently or temporarily. It also restrains the person from using that website further by the user. It has its origin from DoS. If the one system is made safe, remaining systems will automatically become safer. The "botnet attack" can also happen by using a single system.

[8] https://ifflab.org/how-to-prevent-cyber-bullying-anti-cyber-bullying-laws-in-india/

Volume 10, May 2020 ISSN 2581-5504

Cyber Vandalism: It involves modifying or adding or deleting the content on the internet without the proper authority or license. It is done with bad intent by editing the content. It affects millions of users and corrupts the young person minds. It is penalised under the law.

Copy right infringement: It is nothing but "piracy". The creator or the publisher should get the copy right for that product. Otherwise it will be pirated or another person will use it. He uses it in the form of distributing, displaying or publishing. Only the owners have the right to do all the things. If it is done exclusively without that person consent is called as piracy.

We can consider the example of films. Before it is released in theatres it is pirated in websites called 'Tamil rockers. It affects the film producers to the large extent and make them to suffer huge loss. It affects many workers at the smaller level and makes them to earn less.

Cyber theft: Cyber theft in IP involves stealing of patent rights, trade secrets and copyrights without their permission by using internet and computer. It helps them to earn the ownership and to earn to the maximum extent.

Spoofing: It is also known as "computer spoofing". The meanings are deceiving, hide or to trick. This is done by hiding one-person true identity. It involves "IP Spoofing" which involves sending of messages by using a fake identity. It will send messages as it sent from the trusted person for the victim to whom the message is sent.

Social engineering: The cyber criminals will deal with you directly through phone calls. They will act in a manner that they are well established firm. They will be friendly with you until the trusty relationship builds between you both. It will continue till the victim share the personal information with them.

Data diddling: The expected output is modified or removed or altered by coding a virus program. It is a simple type of hacking and can be done by all people. It is used in stealing the money from the big firms by the accountants by not entering the correct value in the books. It is nothing but fraud and is held to be punishable.

Child pornography: The abusing of child is an offence. The child labour is also an offence. If any person forcing the child to work and while working takes any image and uploads or spreads in the website. It is considered as child pornography. The persons should be penalised properly.

The above said is the main topic prevailing in the recent trend. The persons who are watching the child pornography at the online websites are punishable and a law was enacted for this purpose. The list has been taken and persons are punished according to their crime rate.

7. Most important cyber-attacks in the year 2019:

- ✓ The Facebook user data leaks and published by a famous website called Amazon cloud computing.
- ✓ The capital one breach uses 100 million customers credit card details.

Volume 10, May 2020 ISSN 2581-5504

- ✓ The canava hack occurs in a designing website and steals the information of credit card details and passwords.
- ✓ The quest diagnostic breach is called as health care data breaches and shares nearly 12,000 patients to unauthorised users which helps them to access that person security numbers and to earn profit.
- ✓ The Door Dash Hack uses 4.9 million users which uses the person credit card number "cvv", password, history of phone calls, email address, delivery address, profile names which is again looting a huge some of money from their home and bank accounts.

The five are considered to be the major attacks in the year 2019 in the "cyber world".

The above said are some of the crimes in this period and to some extent it is explained. In future time, we may have wide spread advancement in all fields particularly in technology. At the same time double the proportion, the crimes on technology particularly on internet. The world is developing towards a new phase called "cyber world". Everything will be made online except the human's basic needs. Crimes will increase with a greater speed. Steps should be taken in order to prevent the crimes and further suggestions are given below along with certain laws and acts has been discussed.

8. Acts enacted in India for cyber safety:

Information technology act, 2000 is the primary law in India which was enacted to control cybercrime and to regulate the electronic commerce.it is based on the UNCITRAL (United Nations commission on international trade laws) model of law on international commercial arbitration recommended by the general assembly of the UN by a resolution on 30 January 1997. [9]The UNCITRAL Model Law provides a pattern that law-makers in national governments can adopt as part of their domestic legislation on arbitration.

9. Main features of IT Act 2000:

- ✓ This act recognises electronic signatures and electronic records and gives a legal framework to the electronic commerce.
- ✓ This act defines the cybercrimes and provides punishment for them.
- ✓ Controller of certifying authorities was formed for the issuance of electronic signature by this act.
- ✓ A cyber appellate was established to deal with the issues relating to this new law.
- ✓ Various sections in the Indian penal code act1860, Indian evidence act 1872, Bankers book evidence act 1891, Reserve bank act 1934, were amended by this act.

10. Information Technology Amendment Act 2008:

A major amendment was bought to the IT act in 2008. It included section 66A according to which sending offensive messages are punishable. It also included section 69 through which authorities were given power of interception or monitoring or decryption of any information

[9] https://en.wikipedia.org/wiki/UNCITRAL_Model_Law_on_International_Commercial_Arbitration

Volume 10, May 2020 ISSN 2581-5504

through computer resources. It also added provisions relating to child pornography, cyber terrorism, and voyeurism.

After this amendment was passed the government faced criticism that the section 66A was unconstitutional as it violated the fundamental right of freedom of speech and expression guaranteed under article 19(1) of the Indian constitution. In the case of Shreya Singhal v union of India, the Supreme Court held that the section 66 A of the information technology act is unconstitutional on the ground of being violative of article 19(1) of the Indian constitution.[10]

11. Why these laws are not effective:

The main reason why these acts are not effective is that the offender cannot be traced easily. Because it is like finding a pin in a large ocean. The number of users on the internet is growing day by day.it becomes very difficult to find out the culprit out of the millions of people who are on the internet. Sometimes the offender may also use fake ID and access the internet. And another difficulty is that the person may have done that crime through some other persons ID.so there comes the question weather to punish the person under whose ID the crime has been committed or to punish the person who actually committed the crime.

Regarding the unauthorized websites if the government bans one website, they easily create another website with different domain. So, the government should go along with the technological experts and find solution to these kinds of problem. Sometimes imposing restriction on social media bring out problems such as violation of right to privacy and the security of the data collected. As we have seen earlier the section 66A of the IT act has also been struck down as it violated freedom of speech. All the people expect more freedom which makes it difficult for the government to impose restrictions.

The jurisdiction becomes a major problem in the cybercrime because the victim may be in one place and the offender may be in some other place. So, the law must be very clear on its jurisdiction and make sure that the offenders are punished where ever they are. People are unaware of the cyber law which is already existing. They do not know how to approach the court in the case of cybercrimes. And also, the teen agers who are a victim sometimes lacks maturity on how to handle such situation and end up their lives. We suggest that these young children are given counselling on how to handle such situation and the parents must also be given guidelines on how to protect their children against such ill effects of social media. In cyber law IT act is the only act which was enacted by the government till date. But in today's world were the cybercrimes are growing at a huge rate, we suggest that the laws are also upgraded in order to deal with the developing crimes in the internet.

12. Steps need to be done:

In order to reduce the growing rate of cybercrime the following steps can be taken.

[10] https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

Volume 10, May 2020 ISSN 2581-5504

- In individual level a person can try to avoid these kinds of cybercrimes by creating strong passwords. And also, by not sharing the passwords with others. Creating strong passwords may prevent others from accessing your accounts. And also, many people tend to share them passwords with strangers. It is advisable to not share the passwords to others unless it is necessary. It would be more secure if the passwords are frequently changed and is difficult to find.
- Another method to secure your data is to increase the firewall settings in the computer.
- Firewall is a barrier between the internet and the computer. It is a security guard which prevents others form accessing your computer without your permission. Hence increasing your firewall settings can keep you protected from the unwanted contents in the Internet. Updating your anti-virus can also protect your computer from being hacked and avoid unnecessary contents from the internet. Now a days the hackers are so fast that as soon as a virus update has been released, they try to find bugs in that and hack it. So, it is safer to update your anti-virus to the latest update version.
- The verification process can also be increased in your computer so as to ensure that no one access your device without your knowledge. For example, if you open your mail id in new device then immediately a notification should come to your phone saying that my mail I'd has been accessed through some other new device. So, increasing the verification process will protect your Id from being used by others and it will also make sure that no one access your Id without your knowledge.
- At government level the following measures can be taken.
- New laws can be enacted in accordance with the current trend and situation. As laws keep on evolving according to the changes in the technologies, new cyber law acts must be enacted in order to cope up with the technological changes. But the main problem here is that the technology keeps on changing at a rapid rate. And the laws are getting implemented at a lower rate. So, we need to speed up the process of implementing the laws according to the speed of changing technology. And the next thing the government has to do is to create awareness among the people about the cyber-crimes which are happening and to teach them to be secure against such crimes. Mostly rural people who lack awareness about the technologies fall prey to those who want to use their unawareness and mint money from innocent people. So, the government should educate the rural people about the pros and cons of the digitalization. So that can make best use of the digital platform and not become victims of cybercrime. We must create awareness not only to rural people but also to all age groups of people. Because many young children are being misguided by the contents in the Internet so it is necessary to educate the young generations on the harm effects of social medias. They must make best use of it for their life and not to get spoilt by the internet. Awareness programs can be conduct in the schools by the government and also parents can be given guidance on how to prevent them children from the Ill effects of the internet. Government can also impose restrictions and regulate the contents in the internet so that people of all age group can use the

Volume 10, May 2020 ISSN 2581-5504

internet. But restriction has to be imposed in such a manner that it does not infringe the freedom of others. Reasonable restrictions can be imposed on the contents in the internet. By regulating the contents in the internet, the government can make sure that users are protected against the unwanted and misleading contents.

13. Cyber Security Strategies:

There are various cyber security strategies which the organisations may build. Some of the strategies are listed below to protect them against cybercrimes.[7]

Ecosystem: Ecosystem consist of automation, interoperability and authentication. Creating a strong ecosystem may prevent the computer from cyber-attacks like malware, hacking, insiders attack, equipment theft etc.

Framework: An assured framework allows updates to the infrastructure. It also makes the business and the government to work together. It is also called as enabling and endorsing.

Open standards: It allows businesses to use proper security settings. It improves economic growth and technological development.

IT mechanisms: Promoting IT mechanisms is a great way to fight cybercrime. Its measures include end-to-end, association-oriented, link-oriented, and data encryption.[11]

E governance: It is the service providing ability on the internet. Developing this technology is an important part in cyber law.

Infrastructure: It includes electrical grid and data transmission lines. It is the most important part in the cyber-crime otherwise your infrastructure will be vulnerable to cybercrime.[12]

14. Conclusion:

We would like to conclude by saying that the cyber space is a big platform to showcase them talents. But it is sometimes misused by people for doing crimes. The government must take action against such crimes by creating a separate special wing in the police department to deal these matters as fast as possible. And also, they must use the latest technologies to find out the offender and punish accordingly. As law evolves along with the development in the technology the government must make new laws according to the changes in the society. In today's word almost all activities be it business or communication happen online in Internet. We have to make sure that the online space is safe and secure for its users. The new laws we make must focus on regulating the contents in the internet and to punish the offenders who use cyber space as a tool for committing crimes.

Finally, we must create awareness among the users of the internet about the cybercrimes and also, we must also bring changes in the judiciary in order to deal with cybercrimes. The parents must also make sure that their children are watching useful things and not get

[11] http://www.techedify.info/cyber-law/
[12] https://www.upcounsel.com/cyber-law

Volume 10, May 2020 ISSN 2581-5504

corrupted by the inappropriate contents. Mostly the teen agers became a prey to the hackers. It also helps to raise the economic position of our country to another level. It is important to make sure to create “safety cyber world with advancements”. So, we must make the cyber space free from insecurities and make it a useful platform for the future generation to grow.