



# International Journal of Research Publication and Reviews

Journal homepage: [www.ijrpr.com](http://www.ijrpr.com) ISSN 2582-7421

## CYBER CRIME

*SRIJAN RAI<sup>1</sup>, MALOBIKA BOSE<sup>2</sup>*

<sup>1,2</sup> AMITY UNIVERSITY LUCKNOW CAMPUS

---

### ABSTRACT

In the past years there has been a significant growth in technology. Now a day's technology surrounds us for every moment of our life. Technology has made our lives easier than we can even imagine. One of the greatest achievements of technology has been the development of internet. Internet has been the biggest gift of mankind to the world. Internet has also made it easy for the criminals with sharp minds to fulfill their evil agendas without doing any physical harm to any person.

**KEYWORDS:** Technology, Development, Cyber security, Cyber criminals, Internet, Computers, Malicious, Wi-fi, Crime, Harm

---

### INTRODUCTION

The internet can be stated as the wider network that allows computer networks around the world to share information and talk to each other. This results in a mass of cables, computer, data centre's, routers, servers, repeaters, satellites and Wi-Fi towers that allows digital information to travel around the world.

It is this network of computer that allows you order products online and receiving them at home without doing any actual work. It helps you to stay connected to the world through the social media platforms and gives you day to day updates about what is going in the world around you. [1] (what is the internet?, 2020)

Soon after the invention of the internet people started facing the troubles related to cyber security as, the internet had some flaws in it as well. Cyber criminals started using internet for achieving their malicious agendas and to bring harm to the users of internet.

Under the Information and technology act, 2000, Cyber offences are the unlawful acts which are carried in a very sophisticated manner in which the computer is the tool or target or both. Cyber crime usually includes hacking. Publishing of information which is obscene in electronic form<sup>1</sup>. [2](lawctopus)

---

### ORIGIN OF INTERNET

The first workable prototype of internet came in the 1960s with the creation of Advanced Research Projects Agency Networks, also known as ARPANET. ARPANET used packet switching to allow multiple computers to communicate on a single network.

In 1970, Robert Kahn and Vincent Cerf developed transmission control protocol and internet protocol or TCP/IP which was a communications model that set standards for how data could be transmitted between multiple networks.

Vincent Cerf is also known as the father of the internet.

Internet took a more recognizable form when Tim Berners-lee invented the World Wide Web in 1989. The world wide web is often confused with the internet, but the world wide web is actually just the most common means of accessing data online in the form of websites and hyperlinks. This helped the internet become popular among the public and served as a crucial step in developing the vast trove of information that is used by most of us nowadays [3](History).

The web did help to popularize the internet among the public, and served as crucial step in developing a vast trove of information that most of us now access on daily basis.

---

<sup>1</sup> Information and technology Act, 2000

## ***PUNISHMENTS FOR CYBER OFFENCES***

As we all know that everything has its own pros and cons, same stands for the internet. Internet can be the most powerful resource humans have ever had if used wisely, and on their hand it can also be the most dangerous weapon if it is in the wrong hands. There have been incident in the past of people misusing internet for their own benefit. With the development in the field of technology the crimes related to the use of internet have also been increasing. Illegal activities done using computers or the internet come under cyber crimes which are punishable by law.

Cyber crime cases in our country have rapidly grown between the years 2014 to 2017, reports suggested. Cyber crime cases were 9622 and 11,592 to 12,317 during 2014, 2015 and 2016 respectively, the government stated.

During the question hours in Rajya Sabha, the members expressed their concerns over the safety of digital transactions, to which the Minister of electronics and Information and Technology stated that the government was alert to the challenges. He also stated that the government was working with the Interpol and CBI to identify Websites which had child pornographic material, something which is highly restricted and offensive.

Child pornography is any visual depiction of sexually explicit content involving a child which includes photograph or video. The Union cabinet approved to the amendments of the POSCO act, initiative of which was taken by the WCD Minister Smriti Irani, she conveyed the message that from now on their will be zero tolerance for child pornography and for that the definition of child pornography was necessary. Fine with the intent to transmit, possess any form of sexually explicit content in any form but failed to delete or destroy is at least RS.5000 toRS.10000 for repeated offenders. Fine for any person who transmits or distributes child pornography othe than the ones producing it as evidence in court would face imprisonment upto # years, previously the fine for possessing child pornography was RS 1000 to RS 3000. The union cabinet approved amendments to strengthen the POSCO act by adding death penalty for aggravated sexual assault on children.

The RBI also had registered a total of 13083, 16468, 13653 and 12520 cases of frauds involving credit cards in 2014-15, 2015-16, 2016-17 and quarter April-September 2017 respectively. [4](cyber crime cases)

Anyone, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to three years and shall also be charged with a fine which may extend to RS.1 lakh<sup>2</sup>. [5](qoura)

---

## **CYBER CRIMES: WAYS USED BY THE CRIMINALS**

There are a lot of methods by which cyber criminal can get into your devices and steal information which is valuable to you and can use it for their own benefits. These criminals don't even need to move from their places to harm you. Cyber crimes are one of the most harmful crimes that a criminal may attempt. It may not harm you physically but can cause mental stress and financial trouble.

Phishing scams- Phishing is a practice in which a cyber criminal attempts to gain sensitive information such as card or bank details from a person. India is one of the countries in which phishing scams are very popular and it keeps on growing. In April itself India has faced more than 2,152 phishing attacks, which is the 4<sup>th</sup> highest globally.

According to IFSEC Global India lost an approximate of \$225 million in phishing attacks in 2013 due to which India emerged as the top nation in APAC region in terms of phishing attacks by volume, closely followed by Australia and china [6] (IFSECGLOBAL).

Jamtara, a small town in Jharkhand is also nicknamed as the phishing capital of India because of the fact that there were numerous incidents across the country related to phishing whose centre point came out to be this small town.

Phishing is a punishable offence under Information and Technology act, 2000 with penalty up to 1 Crore.

There is many more type of cyber crimes, one of which is Identity Theft Scams. Identity theft is the use of someone else's identity, mainly for the purpose of financial benefits or for the disadvantage of the victim.

The term identity theft was coined in 1964.

Identity theft contributes to 28 percent of overall frauds in India. Delhi and west Bengal have the highest rates of frauds followed by Punjab, Uttar Pradesh, and Haryana. [7](blogleaders).

Identity theft can take place in many ways, for example:

### **PHARMING**

It refers to the practice in which the cybercriminals installs malicious code on a particular computer or a server, misdirecting the user to a fraud website without their consent or knowledge. It disguises fake and fraud websites as the legitimate and trusted ones [7](blogleaders).

### **Credit Card Skimming**

This type of fraud is very popular in India. Crooks often use a small device to steal the credit card details which includes card number, expiry date, and the security number. The small device used in the process is known as 'Skimmer'. When the victim uses his/her card on an ATM machine in which the crook has installed the skimmer all the data which is present on the magnetic strip of the card gets copied into the skimmer. The criminal

---

<sup>2</sup> Sec.66c of information and technology act 2000- Punishment for identity theft.

then uses this information to make fraudulent transactions and to withdraw money. Once the information is stolen the thief can make a cloned card to make a number of transactions. The victims are often unaware of the theft [8](indiaonline).

The government of India has been taking many steps to catch the cyber criminals and has been successful many times, but these criminals have also evolved with time and have started using the dark web to remain anonymous.

The Dark web is the encrypted part of the internet that cannot be tracked. The cyber criminals have started using the dark web to buy software's that help them to remain anonymous while they carry out their malicious crimes.

The dark web is part of the deep web which is the non-indexed part of the World Wide Web which cannot be accessed using a normal browser such as Google and requires encrypted networks such as Tor browser.

The dark web is also used for the sale and purchase of several illicit products such as weapons and drugs. Cyber criminals also appear to be shopping here [9](economictimes).

The cyber criminals use bit coin as the mode of transaction on the dark web as bit coin is untraceable. Dark web is the complete opposite of the normal websites we visit on a daily basis. All those things or services that are legal in the society are available on the normal websites. On the other hand, anything which is not meant to be available on the websites is made available on the dark web.

Fake document, fake passport, assassination, drugs, and weapons everything is available on the dark net.

The Indian Government has taken several measures against the cyber criminal to protect our countries resources and people from these criminals.

Information and technology Act, 2000 is an Act passed by the Indian Government on 17<sup>th</sup> October, 2000. It is the primary law in India dealing with cybercrime and electronic commerce [10] (wikipedia).

Hacking with computer systems:

Section 66 provides that whoever with the intent to cause or knowing that he is likely to cause wrongful damage to the public or any person destroys, deletes or alters any information residing in a computer resource, commits hacking.

(2). whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to RS. 2 lakhs or both.

The other offences included in the IT Act 2000 are as follow:

1. Tampering with the computer source documents.
2. Hacking
3. Publishing of information which is obscene in electronic form.
4. Penalty for Misrepresentation.
5. Confiscation
6. Penalty for breach of confidentiality and privacy [11](lawctopus).

The Government of India has also established cybercrime cell portal which a victim may seek help at the time of facing any criminal issue involving the internet or computers.

This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

The official website for cyber crime cell of India is [cybercrime.gov.in](http://cybercrime.gov.in) [12](cybercrime).

If you ever have any problems due to cybercrime you just have to go to the official website of cybercrime cell.

You need to fill up a form regarding your issue you are facing due to any cyber criminal activity and they will guide you and help you solve the problem and conduct any necessary investigation.

---

## CONCLUSION

People should also become more serious and responsible towards cybercrime as they are towards day to day crimes, such as robbery or homicides. You should also protect yourself from cyber stalking. Cyber stalkers show advances on a person repeatedly despite clear indication of disinterest by such person. They use internet, email, social media or any other form of electronic communication for stalking. You should always disable the location services for social media platforms such as face book and in instagram. Cyber awareness for the public is very important now days. The internet has brought joys to our live and has made our lives much easier, but also has many dark sides. The cybercriminals are always into finding ways to hack into people's computer to cause harm to the others and benefit to them.

Cybercriminals are all around us and will always be trying to manipulate the technology for their purpose. We all need to follow the guidelines of the cyber cell while surfing the internet and stay away from the websites that seem suspicious or ask for unnecessary personal information.

---

#### REFERENCES

---

- [1] "theguardian," [Online]. Available: [www.theguardian.com](http://www.theguardian.com). [Accessed 23 june 2020].
- [2] "Lawctopus," [Online]. Available: <https://www.lawctopus.com/>. [Accessed 23 april 2020].
- [3] "History," [Online]. Available: <https://www.history.com/>. [Accessed 21 april 2020].
- [4] "ndtv," [Online]. Available: [www.ndtv.com](http://www.ndtv.com). [Accessed 23 june 2020].
- [5] "quora," [Online]. Available: [www.quora.com](http://www.quora.com). [Accessed 23 june 2020].
- [6] "ifsecglobal," [Online]. Available: [www.ifsecglobal.com](http://www.ifsecglobal.com). [Accessed 23 june 2020].
- [7] "blog.pleadings," [Online]. Available: <https://blog.pleadings.in>. [Accessed 23 june 2020].
- [8] "indiainfoline," [Online]. Available: [https://www.indiainfoline.com/article/research-articles-personal-finance/what-is-card-skimming-113111500866\\_1.html](https://www.indiainfoline.com/article/research-articles-personal-finance/what-is-card-skimming-113111500866_1.html). [Accessed 26 june 2020].
- [9] "economic times," [Online]. Available: <https://m.economictimes.com>. [Accessed 26 june 2020].
- [10] "wikipedia," [Online]. Available: <https://en.wikipedia.org>. [Accessed 26 june 2020].
- [11] "lawctopus," [Online]. Available: <https://www.lawctopus.com>. [Accessed 26 june 2020].
- [12] "cybercrime.gov," [Online]. Available: [cybercrime.gov.in](http://cybercrime.gov.in) . [Accessed 26 june 2020].
- [13] "economictimes," [Online]. Available: <https://m.economictimes.com>. [Accessed 25 june 2020].
- [14] "wikipedia," [Online]. Available: <https://en.wikipedia.org>. [Accessed 25 june 2020].
- [15] "cybercrime.gov.in," [Online]. Available: <https://cybercrime.gov.in>. [Accessed 25 june 2020].