# Present trends of Cyber Crimes over E-Commerce and their solutions in India

*Astt.Prof. Anupam Mishra, Dept.of Management, Govt.Mohindra College, Patiala, Pb.
**Ms.Chinky Dhiman, Student, Dept.of Commerce, Govt. Mohindra College, Patiala, Pb.

## Abstract:

With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The number of users and their diversity in their makeup has exposed the Internet to everyone. Some criminals in the Internet have grown up understanding this superhighway of information, unlike the older generation of users. This is why Internet crime has now become a growing problem. Some crimes committed on the Internet have been exposed to the world and some remain a mystery up until they are perpetrated against someone or some company Cyber crime always involves some degree of infringement on the privacy of others or damage to computer-based property such as files, web pages or software. This paper is completely focused on cyber crime issue, trends and problem faced by Indian users and how cyber crimes can be minimized by formulating effective cyber crime laws in India. The paper also includes Indian cybercrime Statistics, cyber crime cells all over India and many more latest news. National level agencies can develop security guidelines and policy to prevent and safeguard of internet users from cyber crimes.

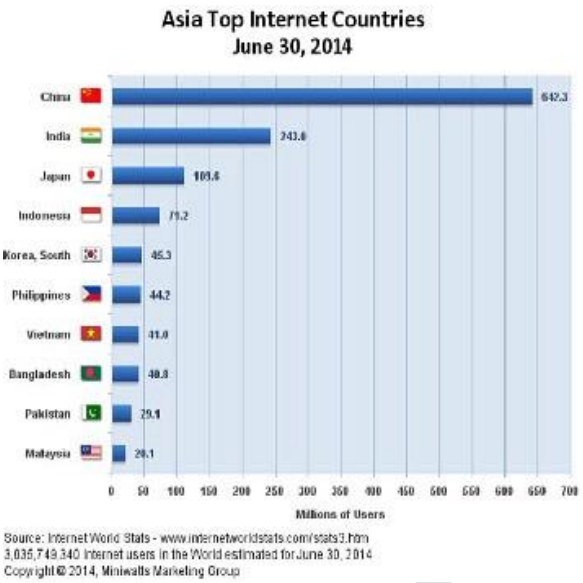
**Keywords**: E-commerce, Internet, Cyber world, Cyber crime, Cyber laws, Indian cybercrime Statistics, Cyber cells in India.

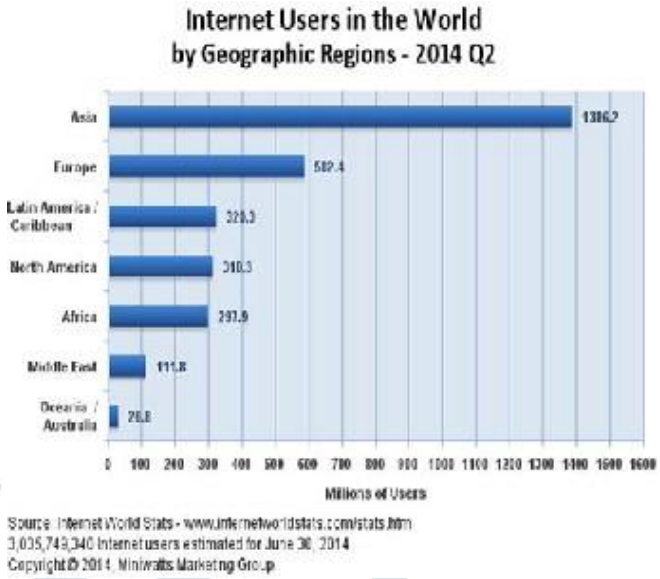
## INTRODUCTION:

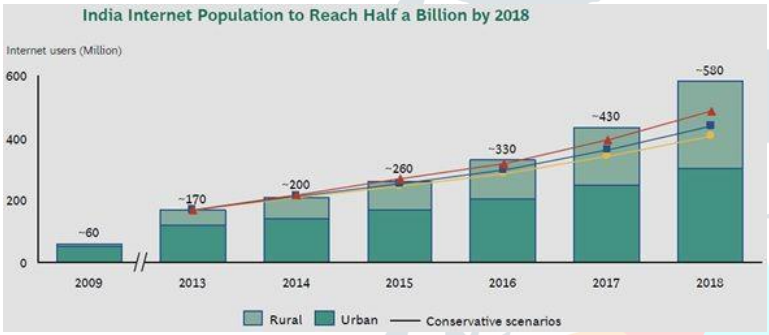
These days computer and internet becomes very common and necessary for our daily life. Back in 1990, less than 1,00,000 people were able access Internet worldwide. Now around 2,405,518,376 people are hooked up to surf the net around the globe. The present time of fast computing brings a new world known as cyber world. The increasing use of information technology facilitate common people to get information, store information, share information etc. The cyber world is an online world where users have a lot of information technology mechanisms to do personal activity as easily and freely as they can transact them in the physical world

Internet and World Wide Web works as a backbone for all online service and activities. Users can access these online services at anytime and from any where. Internet offers great benefit to society but present opportunities for crime also. Today e-mail and websites have become the preferred means of data communication. This includes not only educational and informative material but also information that might be personal.

The number of internet users in India is expected to reach 500 million by June 2018, said a report by the Internet and Mobile Association of India (IAMAI) and Kantar IMRB on Tuesday. The number of Internet users stood at 481 million in December 2017, an increase of 11.34% over December 2016 said the report titled, "Internet in India 2017."




## What is Cyber Crime?

As the use of internet is increasing, a new face of crime is spreading rapidly from in-person crime to nameless and faceless crimes involving computers. Cyber crime includes all unauthorized access of information and break security like privacy, password, etc. with the use of internet. Cyber crimes also includes criminal activities performed by the use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system, etc.

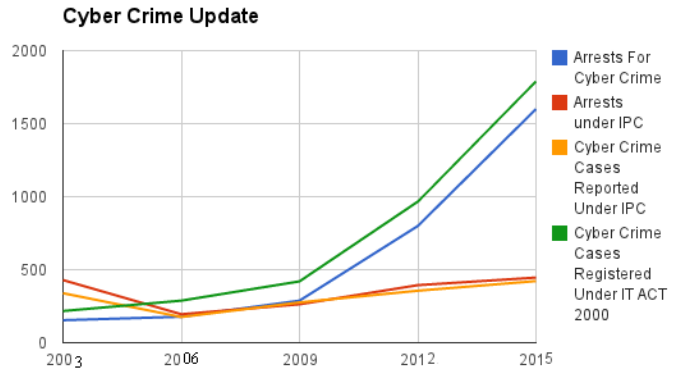
In tenth United Nations congress on "prevention of crime and treatment of offenders" which is devoted to issues of crimes related to computer networks, cyber crime was broken into two categories and defined as:

***a. Cyber crime in a narrow sense (computer crime*):** Any illegal behavior directed by means of electronic operations that targets
the security of computer systems and the data processed by them.
***b. Cyber crime in a broader sense (computer-related crime):*** Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

In news what we see as every day affair now-a-days is somewhat like - ------ ------ ------ ----- "**Hyderabad**: ***Many account holders of ……. Bank in the city have lost lakhs from their account in the last four weeks. Bank officials suspect a database hack or a massive cloning of debit cards. Around 22 account holders in one single branch alone, in Secunderabad, have lost money. After the devastated customers approached the bank the officials alerted their headquarters in Bangalore and have approached the National Payments Corporation of India (NPCI) to find out what went wrong. The bank authorities have***

***also decided to approach the Telangana police***. ….. … . This is not a odd news in some news paper but it is the news in major news papers. Few such concerns to quote in similar lines is ….

- *Massive cloning of bank debit cards suspected in ….*
- *IT professionals duped of Rs 2.16 lakh …..*
- *Bank asked to pay 40L to Bizman for online fraud ….*
- *Houdini malware – just down load one program or some spam mail it will take care of sending your ID, Passwords, Card numbers, confidential information to outside.*
- *Organization servers are down for 2 days…..*
- *Customer disclosed his ID password over phone, as the caller informed that he is calling from bank .. within 5 minutes his account is empty.*




***Cyber Crime Trends***

## Cyber Crime and its impacts on E-commerce:

On one side where E-commerce is becoming integral part and imparting convenience into lives, it is suffering from cybercrime. E-Commerce involves transaction of Money and Information. Both of these things are of great importance for the businesses. It is said that theft of information is more damaging than the theft of money. Cybercrime is rapidly growing under covered business operated by criminals, who trade valuable stolen financial information from millions of innocent internet users every year, in online black market. Cyber criminals do cyber-attacks on the computer systems through malware or malicious software, these takes control of the computer and gets access to the sensitive information stored in it, without users knowing about it. In more simple words, cyber-crime is the use of computer resources to involve in unofficial or illegal acts. For example, telemarketing and Internet fraud, identity theft and credit card account thefts are considered to be cybercrimes when the unlawful activities are committed through the use of a computer and the internet. It brings serious threats to the integrity and existence of the businesses and thus makes the need of strong security methods and laws, a top most priority. Computer crimes covers a wide range of possible illegal activities. The crime can be generally be divided into two types of activities,

**a. Direct targeting of the computer network or devices**.

This includes

- Malware and malicious code.
- Denial of service attacks.
- viruses

**b. Crime facilitated by computer networks or devices.**

This includes

- Identity theft.
- Information warfare.
- Cyber stalking.
- Phishing scams.

## Types of Cybercrimes:

There are numerous types of cybercrimes. Some popular type of crimes are as below:-


***Hacking:*** **-** This is the most popular type of crime, which is related to unauthorized access to the computer system. The computer system in broken into so that the sensitive information can be accessed. This involves use of variety of criminal software by hackers to gain access of a person's computer without him realizing. This is different from ethical hacking.

***Data theft****:-* This simply means stealing data, for normal or illegal usage. This happens when a person violets copyrights and steals music, movies, games and software. This type of crime is costing the copyright industry a huge money. The legal system is working on making stronger laws that prevent people from unlawful downloading.

***Identity theft:-*** This is different from data theft. This produces a greater threat to the people using computer for transaction and banking services. This is used to steal money or buy things through accessing credit/debit card, bank account or any other sensitive information, by criminals in individual's name. This result into major financial loses or even vanishing the credit history.

***Cyber Stalking:-*** This involves use of computer system to harass the victim. It has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals, to harass another individual, group of individuals, or organization. The behavior includes false accusations, monitoring, the transmission of threats, identity theft, damage to data or equipment, the solicitation of minors for sexual purposes, and gathering information for harassment purposes.

***Malicious Software****:-* Network disruption is the main aim of such software. These software are used to gain access to system and steal sensitive information or Data resulting damage to the software present in the system.

***E-mail Bombing****:-* This is a form of net abuse comprising of sending large number of e-mails to an address. This is an attempt to flood the mail box or block the server where the account is hosted. These kind of e-mail bombs are simple to design and simple to detect and prevent.

***Data Bidding****:-* Data bidding relates performing unauthorized modifications to data stored in the computer system. This includes unlawful changing the documents used for data entry.

***Web Jacking****:-* Web Jacking is gaining access and taking control of others website, by hacker. The hackers can disfigure or even change the information on the site after web jacking. Normally this kind of crime is seen in fulfilling political objective or for demanding huge money from government organizations.

***Child abuse****:-* In this type of crime, the criminals solicit minors through chat rooms for the purpose of child pornography. Security agencies spend large budget and time monitoring chat rooms, to reduce and prevent child abuse and soliciting.

***Cyber Trespass****:* It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

***Cyber Trafficking:*** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.

***Cyber crime & Social Networking:*** Cyber criminals use social media not only to commit crime online, but also for carrying out real world crime owing to "over-sharing" across these social platforms**.** The risk associated with our identities. Identity theft can happen to anyone who exposes too much personal information online on various social networking sites. Get to know the security and privacy settings, and configure them to protect from identity theft. One in five online adults (21 percent) has reported of becoming a victim of either social or mobile cyber crime and 39 percent of social network users have been victims of profile hacking, scam or fake link.

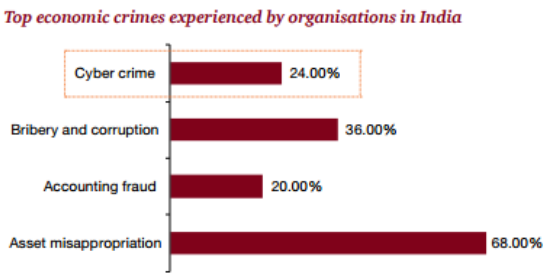
***Intellectual Property Crimes:*** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

***Bot Networks:*** The word botnet made from the two words robot and network. A cyber crime called 'Bot Networks', when hackers remotely take control upon computers by using malware software. Computers can be co-opted into a botnet when they execute malicious software. A botnet's originator can control the group remotely

***Transmitting Virus:*** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to
other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
From the above literature it is evident that the cybercrime is the biggest threat to the E-commerce.

## Recent Trends of Cyber Crime in India:

It is also pertinent to mention here that today's Business is totally depending on Cloud technology, Internet, mobile phones and social media for e-commerce and business solutions and there was no banking activity without the use of these Information technology routes. Around 85% of the commercial transactions and 60% of banking transactions are online which emphasizes the need for Cyber Security. Cyber crimes on various organizations are not equal. Understanding the motives, methods and people behind the attacks gives clear picture of Cyber Security trends.




With increasing mobile and internet penetration in the country, cyber crimes have also increased proportionately. Between 2011 and 2015, more than 32000 cyber crimes were reported across the country. More than 24000 of these cases are registered under the IT Act and the remaining under the various sections of IPC and other State Level Legislations (SLL).

### Cyber Crimes Legislations

Cyber Crimes in India are registered under three broad heads, the IT Act, the Indian Penal Code (IPC) and other State Level Legislations (SLL). The cases registered under the IT Act include,

- Tampering computer source documents (Section 65 IT Act),
- Loss /damage to computer resource/utility (Section 66 (1) IT Act),
- Hacking (Section 66 (2) IT Act),
- Obscene publication/transmission in electronic form (Section 67 IT Act),
- Failure of compliance/orders of Certifying Authority (Section 68 I T Act),
- Failure to assist in decrypting the information intercepted by Govt. Agency (Section 69 IT Act),

- Un-authorized access/attempt to access to protected computer system (Section 70 IT Act),
- Obtaining license or Digital Signature Certificate by misrepresentation / suppression of fact (Section 71 IT Act),
- Publishing false Digital Signature Certificate (Section 73 IT Act),
- Fraud Digital Signature Certificate (Section 74 IT Act) and
- Breach of confidentiality/privacy (Section 72 IT Act).

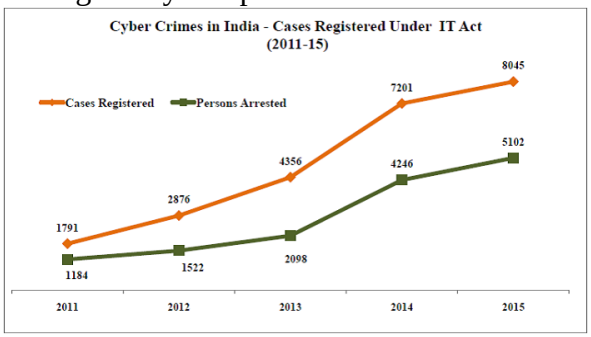
On the other hand, cases are also registered under the IPC and those include,

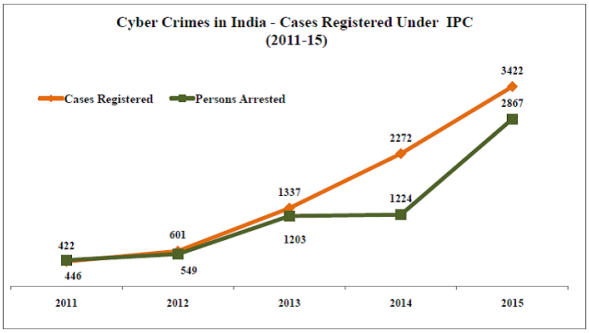
- Offences by/against Public Servant (Section 167, 172, 173, 175 IPC),
- False electronic evidence (Section 193 IPC),
- Destruction of electronic evidence (Section 204, 477 IPC),
- Forgery (Section 463, 465, 466, 468, 469, 471, 474, 476, 477A IPC),
- Criminal Breach of Trust (Section 405, 406, 408, 409 IPC).
- Counterfeiting Property Mark (Section 482, 183, 483, 484, 485 IPC),
- Tampering (Section 489 IPC) and
- Counterfeiting Currency / Stamps (Section 489A to 489E IPC).

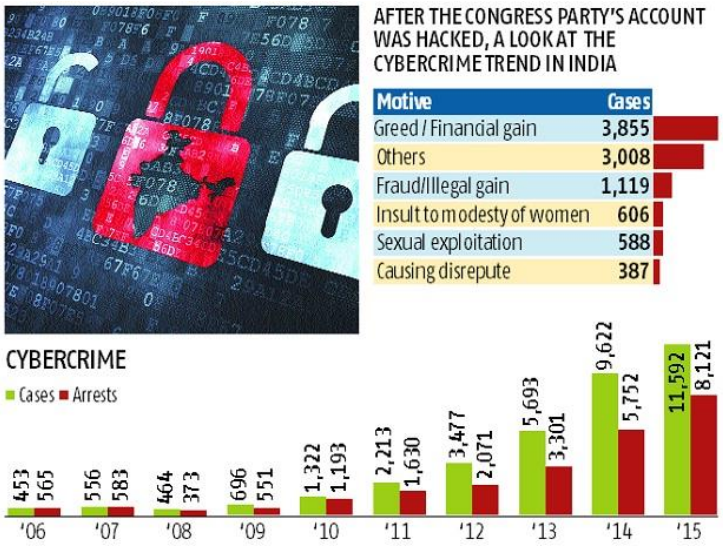
**Cyber Crimes up by more than 3 times in 5 years:**

| Year | IT Act | | IPC | |
|---|---|---|---|---|
| | Cases Registered | Persons Arrested | Cases Registered | Persons Arrested |
| 2011 | 1791 | 1184 | 422 | 446 |
| 2012 | 2876 | 1522 | 601 | 549 |
| 2013 | 4356 | 2098 | 1337 | 1203 |
| 2014 | 7201 | 4246 | 2272 | 1224 |
| 2015 | 8045 | 5102 | 3422 | 2867 |
| Total | 24269 | 14152 | 8054 | 6289 |

The numbers of cases registered under the IT Act and IPC have been growing continuously. The cases registered under the IT act grew by more than 350% from 2011 to 2015. There was almost a 70% increase in the number of cyber crimes under the IT act between 2013 and 2014. The cases registered under the IPC increased by more than 7 times during the period between 2011 and 2015. Similar trend is observed in the number of persons arrested. The government also acknowledges the increase in the number of such crimes and that the introduction of technologies, devices including smart phones and complex applications, and rise in usage of cyber space for businesses has resulted in such an increase.






## Cybercrime statistics a big picture:

One thing the previous few years have taught us that cybercrime is one issue that should not be ignored. The following "big picture" stats should help put the growing threat of cybercrime into perspective:

- Globally, cybercrime was the **2nd most reported crime** in 2016. (*Source:* PWC)
- In proportion to the total number of crimes, cybercrime now accounts for more than 50% of all crimes in the UK. (*Source:* National Crime Agency)
- An attacker resides within a network for an average **146 days before detection**. (*Source:*Microsoft)
- Between April and June 2017, **over 11,800 people reported incidents of cybercrime** to the Australian Cybercrime Online Reporting Network. (*Source*: ACORN)
- A University of Maryland study found that hackers are attacking computers and networks at a **"near-constant rate"**, with an average of one attack every 39 seconds. (*Source*:University of Maryland)
- Most network intrusions—**63 percent—are the result of compromised user passwords** and usernames. (*Source:* Microsoft)
- In their 2017 Annual Cyber security Report, Cisco found that globally, 8 percent of malicious email attachments were **docm files** (a type of Microsoft Word XML file that executes macros). (*Source:* Cisco)
- **18 million new malware samples** were captured in In Q3 2016. (*Source:* Panda Security)
- According to Gartner, by 2020, 25 percent of cyber attacks against enterprises will **involve IoT devices**. (*Source*: Gartner)
- At 91.6 percent, **"Theft of Data" continues to be the chief cause of data breaches** in 2016 counting total by identities stolen. "Phishing, Spoofing, and Social Engineering" were a distant second at 6.4 percent. (*Source:* Symantec)
- **The U.S. had the most data breaches of any other country**, by a large margin. There were 1013 data breaches in the U.S. in 2016. By comparison, second place U.K. had just 38 breaches. (*Source:* Symantec)
- The number of ransom ware families increased from 30 in 2015 to 98 in 2016, revealing the distinct focus by cyber criminals on **using ransom ware to extort money from businesses and individuals.** (*Source:* Symantec)

*The **average ransom ware demand also increased significantly**, from $294 in 2015 to $1,077 in 2016. (Source: Symantec)*

- Ransom ware developers have been increasingly demanding popular crypto currency bitcoin in recent years, due to its improved privacy over fiat currencies. However, more **private coins such as monero and Zcash are set to become popular with cybercriminals** in 2018, due to their improved privacy over bitcoin. (*Source:* Bloomberg)
- **Mobile platforms are one of the fastest-growing targets** for cyber criminals. Symantec identified 18.4 million malware detections in 2016, a 105 percent increase of 2015. (*Source:*Symantec)
- In 2017, Wikileaks released a stash of over 8,000 classified CIA documents. (*Source:* New York Times)
- That same year, hackers released 2GB of emails from French presidential candidate Emmanuel Macron. (*Source:* Reuters)
- In 2016, **70% of all financial fraud in the UK was done through remote purchases** using stolen information or cards. (*Source*: FFA UK)
- There may be **3.5 million unfilled cyber security jobs by 2021**. (*Source*: Cybersecurity Ventures)
- Cyber security company RSA predicts mass data breaches will continue to play a large role in cyber security threats. (*Source*: RSA)
- Most cybercrime is now mobile. Over 60% of online fraud is accomplished through mobile platforms. Additionally, 80 percent of mobile fraud is accomplished through mobile apps instead of mobile web browsers. (*Source*: RSA)
- McAfee finds that the average number of records lost to hacking in 2017 was 780,000 *per day*. (*Source*: McAfee)
- Up to 0.80 percent of the world's GDP is now being lost to cybercrime. (*Source*: McAfee)

## Cyber Crime Cells in India:

To solve cyber crime cases, Indian police developed cyber crime investigation cells all over India. These Cyber Crime cell investigates in respect of cases pertaining to hacking, spread of virus, pornography, manipulation of accounts, alteration of data, software piracy, creation of false Web sites, printing of counterfeit currency, forged visas, theft of intellectual property, email spamming, denial of access, password theft, crimes with cell phones and palmtops, cyber terrorism etc.. The following table shows the phone numbers and email address of few cyber crime cells operational in India:

**Table-:** List of cyber crime cells all over India.

| | |
|---|---|
| **Assam -** CID HQ,Dy.SP.<br>Ph: +91-361-252-618, 9435045242<br>E-mail: ssp_cod@assampolice.com | **Chennai -** Assistant Commissioner of Police<br>Ph: +91-40-5549 8211<br>E-mail id: s.balu@nic.in |
| **Bangalore -** Cyber Crime Police Station<br>Ph: +91-80-2220 1026, 91-80-2294 3050<br>Email: ccps@blr.vsnl.net.in, ccps@kar.nic.in | **Hyderabad -** Cyber Crime Police Station<br>Ph: +91-40-2324 0663, 91-40-2785 2274<br>Email:<br>cidap@cidap.gov.in, info@cidap.gov.in |
| **Pune-** Deputy Commissioner of Police(Crime)<br>Ph: +91-20-26123346, 91-20-26127277<br>E-Mail: crimecomp.pune@nic.in | **Thane -** Police Commissioner Office<br>Ph: +91-22-25424444<br>Email: police@thanepolice.org |
| **Delhi -** CBI Cyber Crime Cell:<br>Ph: +91-11-4362203, 91-11-4392424<br>Email: cbiccic@bol.net.in | **Mumbai -** Cyber Crime Investigation Cell<br>Ph: +91-22-22630829, 91-22-22641261<br>Email: officer@cybercellmumbai.com |
| **Jharkhand -** IG- CID, Organized Crime<br>Ph: +91-651-2400 737/ 738 | **Himachal Pradesh -** CID Office ,<br>Ph: +91-94180 39449<br>Email:soodbrijesh9@gmail.com |
| **Haryana**<br>Joint Commissioner of Police<br>Email: jtcp.ggn@hry.nic.in | **Uttarakhand -** Special Task Force Office<br>Ph: +91 135 2640982, 91 94123 70272<br>Email: dgc-police-us@nic.in |

| | |
|---|---|
| **West Bengal** - CID, Cyber Crime<br>Ph: +9133 24506163<br>Email: occyber@cidwestbengal.gov.in | **Orissa** - CID, Crime Branch<br>Ph: +91 94374 50370<br>Email: splcidcb.orpol@nic.in |
| **Bihar** - Cyber Crime Investigation Unit<br>Ph: +91 94318 18398, Email: cciu-bih@nic.in | **Punjab** - Cyber Crime Police Station<br>Ph: +91 172 2748 100 |
| **Meghalaya** - SCRB, Superintendent of Police<br>Ph: +91 98630 64997<br>Email: scrb-meg@nic.in | **Kerala** - Hitech Cell, Police Head Quarters<br>Ph: +91-471 272 1547, 91-471 272 2768<br>Email: hitechcell@keralapolice.gov.in |
| **Gujarat** - DIG, CID, Crime and Railways<br>Ph: +91-79-2325 4384, 91-79-2325 0798 | **Jammu** - SSP,Crime<br>Ph: +91-191-257-8901<br>Email: sspcrmjmu-jk@nic.in |
| **Orissa** - CID, Crime Branch<br>Ph: +91 94374 50370<br>Email: splcidcb.orpol@nic.in | |

*Source: http://infosecawareness.in/cyber-crime-cells-in-india)*

## How to protect yourself against Cybercrime:

Anyone using the internet should exercise some basic precautions. Here are 11 tips you can use to help protect yourself against the range of cybercrimes out there.

1**. Use a full-service internet security suite**

For instance, some reputed security suite provides real-time protection against existing and emerging malware including Ransom ware and viruses, and helps protect your private and financial information when you go online.

**2. Use strong passwords**

Don't repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 10 letters, numbers, and symbols. A password management application can help you to keep your passwords locked down.

**3. Keep your software updated**

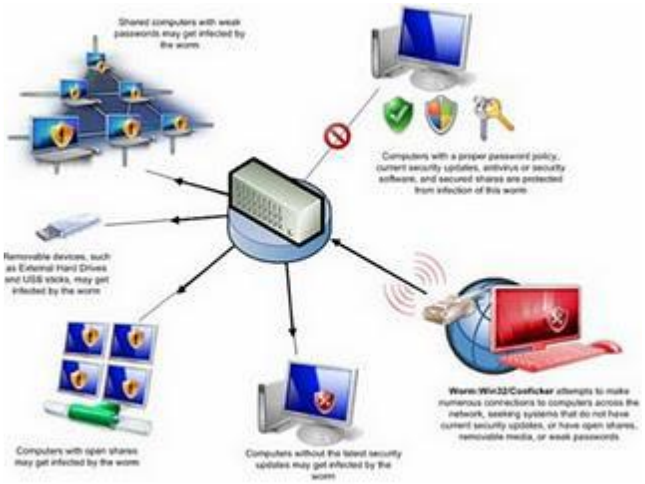
This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.

**4. Manage your social media settings**

Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better. For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

**5. Strengthen your home network**

It's a good idea to start with a strong encryption password as well as a virtual private network. A VPN will all traffic leaving your devices until it arrives at its destination. If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data. It's a good idea to use a VPN whenever you a public Wi-Fi network, whether it's in a library, café, hotel, or airport.



**6. Talk to your children about the internet**

You can teach your kids about acceptable use of the internet without shutting down communication channels. Make sure they know that they can come to you if they're experiencing any kind of online harassment, stalking, or bullying.

**7. Keep up to date on major security breaches**

If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.

**8. Take measures to help protect yourself against identity theft**

Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. How? You might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That's why it's important to guard your personal data. A VPN — short for virtual private network — can also help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

**9. Know that identity theft can happen anywhere**

It's smart to know how to protect your identity even when traveling. There are a lot of things you can do to help keep criminals from getting your private information on the road. These include keeping your travel plans off social media and being using a VPN when accessing the internet over your hotel's Wi-Fi network.

**10. Keep an eye on the kids**

Just like you'll want to talk to your kids about the internet, you'll also want to help protect them against identity theft. Identity thieves often target children because their Social Security number and credit histories frequently represent a clean slate. You can help guard against identity theft by being careful when sharing your child's personal information. It's also smart to know what to look for that might suggest your child's identity has been compromised.

**11. Know what to do if you become a victim**

If you believe that you've become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the Federal Trade Commission. This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future. If you think cybercriminals have stolen your identity.These are among the steps you should consider,

(i) Contact the companies and banks where you know fraud occurred,
(ii) Place fraud alerts and get your credit reports and
(iii) Report identity theft to the FTC.

## Conclusion:

Cyber Crime is serious, aggressive, growing and posing major threat to the economy and nation. In this modern era of technology, the role and usage of internet is increasing worldwide rapidly, therefore it becomes easy for cyber criminals to access any data and information with the help of their knowledge and

their expertise. Cyber crime is an unlawful act or a menace that needs to be tackled firmly and effectively. There is a need to create more awareness among the people and basically users of internet about cyber space, diverse forms of cyber crime and some preventive measures as "Prevention is always better than cure", so it is seriously advised to take some previous precautions while operating the internet. Cyber Space Security Management has already become an important component of National Security Management, Military Security Management, Scientific Security Management and Intelligence Management all over the world. Yet India has taken a lot of steps to stop cyber crime but the cyber law cannot afford to be static, it has to change with the changing time.

## References :

1. Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India ,New Delhi, India.

2. Cyber Law & Information Technology (2011) by Talwant Singh, Additional District & Sessions Judge, New Delhi, India.

3. Introduction to Indian Cyber Law (2008) by Rohas Nagpal, Asian School of Cyber Laws, Pune, India.

4. Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India.

5. B. Patki S. Lakshminarayanan S. Sivasubramanian S.S. Sarma (Authors are with Department of Information Technology, Government of India) Cyber Crime Information System for Cyberethics Awareness ssarma@mit.gov.*in*

6. NCRB report on crimes in India for 2016.

7. http://www.cyberlawsindia.net/cyber-india.html

8. Ajeet Singh Poonia Et al., Cyber Crime: Practices and Policies for Its Prevention.

9. en.wikipedia.org/wiki/Cyber_crime.

10.Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India.

11. http://www.ic3.gov/ "Internet Crime Report 2015"

12. https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

13.https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html

14.https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-expected-to-reach-500-million-by-june-iamai/articleshow/63000198.cms