|  |  |
| --- | --- |
|  | **2020** |
|  | ENGLISH ASSIGNMENT |

|  |
| --- |
| **Cyber Crimes in india** |

**Name: Rajalakshmanan. C**

**Unique Id: E0219054**

1.

1. This Graph represents the cybercrimes in states of India from 2011-2015 . A comparison between Persons Arrested and Cases Registered have been done among the states of India such as West Bengal, Rajasthan, Madhya Pradesh, Uttar Pradesh, Kerala, Karnataka, Andhra Pradesh, Maharashtra in this graph.
2. When we observe the bars of Cases Registered we can find a great difference among the states Madhya Pradesh and Maharashtra as Madhya Pradesh has a lowest Cases Registered that is of 1162 and The Maharashtra shows a highest Cases Registered which is 5935 among the years 2011-2015.But the Uttar Pradesh gets the second position in the list next to Maharashtra in Cases Registered bars. And West Bengal holds the last position in the count of persons arrested for the cyber crimes.
3. Although Maharashtra has the highest Cases Registered Uttar Pradesh stands the highest in the count of persons arrested and also stands second in cases registered. We get a clear view from the graph that the cases registered in the Uttar Pradesh are mostly solved as compared in Maharashtra .But in Madhya Pradesh the Cases registered and persons arrested are very close as compared from the Case of Uttar Pradesh .When we observe the moderate cybercrime areas such as Kerala, Andhra Pradesh, Rajasthan and West Bengal they are not mostly attacked by these crime .But in Karnataka cases registered are very high than the persons arrested which tells us that the cybercrime cases are not concentrated or solved in those areas.

2.

**Cyber Crimes** also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone. The Department of Justice divides cybercrime into three categories: crimes in which the computing device is the target, for example, to gain network access; crimes in which the computer is used as a weapon, for example, to launch a denial of service (DoS) attack; and crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally-obtained data.The number of cyber crime in India may almost double in 2015 the level of last year. At present, the number of cyber crime in India is nearly around 149,254 and is likely to cross the 300,000 by 2015 growing at compounded annual growth rate (CAGR) of about 107 percent. During 2011, 2012, 2013 and 2014, the total number of cyber crimes registered were 13,301, 22,060, 71,780 and 62,189 (till May) respectively, it said.

**Causes of Cybercrime:**

Cybercriminals always opt for an easy way to make big money. They target rich people or rich organizations like banks, casinos and financial firms where a huge amount of money flows daily and hack sensitive information.

Catching such criminals is difficult. Hence, that increases the number of cyber-crimes across the globe. Computers are vulnerable, so laws are required to protect and safeguard them against cybercriminals. We could list the following reasons for the vulnerability of computers:

* **Easy to access**– The problem behind safeguarding a computer system from unauthorized access is that there are many possibilities of making a gap in and break through the systems due to the complex technology. Hackers can steal access codes, retina images, advanced voice recorders etc. that can fool biometric systems easily and bypass firewalls can be utilized to get past many security systems.
* **Capacity to store data in comparatively small space**– The computer has the unique characteristic of storing data in a very small space. This makes it a lot easier for the people to steal data from any other storage and use it for own profit.
* **Complex**– The computers run on operating systems and these operating systems are programmed of millions of codes. The human mind is imperfect, so they can do mistakes at any stage. The cybercriminals take advantage of these gaps.
* **Negligence**– Negligence is one of the characteristics of human conduct. So, there may be a possibility that protecting the computer system we may make any negligence which provides a cyber-criminal the access and control over the computer system.
* **Loss of evidence**– The data related to the crime can be easily destroyed. So, Loss of evidence has become a very common & obvious problem which paralyzes the system behind the investigation of cyber-crime.
* **How to Tackle Cyber Crime:**
* It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. That is why commercial institutions and government organizations need to look at other methods of safeguarding themselves.
* The best way to go about is using the solutions provided by Cross-Domain Solutions. When organizations use cross domain cyber security solutions, they can ensure that exchange of information adheres to security protocols. The solution allows organizations to use a unified system comprising of software and hardware that authenticates both manual and automatic transfer and access of information when it takes places between different security classification levels. This allows seamless sharing and access of information within a specific security classification, but cannot be intercepted by or advertently revealed to user who is not part of the security classification. This helps to keep the network and the systems using the network safe.
* Cross Domain Solution offers a way to keep all information confidential by using safe and secure domains that cannot be tracked or accessed. This security solution can be used by commercial and governmental organization to ensure an impenetrable network while still making sure that users can get access to the required information easily.

Generally, Cyber Crime in India can be:

1. **Cyber Bullying**: It involves use of social networks to repeatedly harm or harass other people in a deliberate manner. It mainly includes online harassment of school children.
2. **Cheating by Personation**: Impersonation involves trying to assume the identity of another, in order to commit fraud/cheating, including false whois of a website.
3. **Identity Theft**: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person.
4. **Obscene Material**: Publishing material in the electronic form, which is lascivious or appeals to the prurient interest including pictures of private area of any person or sexual acts online.
5. **Offensive/Harassing Messages**: Sending of offensive messages through communication devices and/or social media. In such crimes, mostly women are the target.
6. **Defamation**: Online publishing of false statement that harms/damages the good reputation of an individual, group of individuals, brand or a product. Consumer Complaint websites are a good example here.
7. **Cyber Extortion**: Extortion is blackmailing another for obtaining, money, property, or services online. For example, defaming a company on a website and demanding money for removal of a complaint.
8. **Hacking**: Hacking is unauthorized attempts to bypass the security mechanisms of an information system or network. It is provided under Section 66 of Information Technology Act.
9. **Virus Attacks**: Viruses are spread by Cyber Criminals with an objective to hack into a computer system and/or to steal confidential/sensitive information.
10. **Publishing/Circulation of Rumours, especially hurting religious sentiments**: Social Media and Mobile messages are used as a tool to spread hatred messages, which may result in violence in a state or a particular part of the country.
11. **Phishing**: The act of sending email that falsely claims to be from a legitimate organization, specially Banks. This is usually combined with a request for information: for example, that an account will close, a balance is due, or information is missing from an account. The email will ask the recipient to supply confidential information, such as bank account details, PINs or passwords; these details are then used by the owners of the fake website to conduct fraud.
12. **IPR violations**: This involves [Software Piracy](http://www.itlaw.in/cyber-crime-in-india/software-piracy/) or otherwise Trademark and Copyright violations like copying of an existing website and/or its content/text is quite common, for which an injunction is required to be taken from court. Also misrepresenting one business with third party’s Trademark may be regarding as cheating.
13. **Skimming**: It involves fitting an ATM machine with a skimmer device which may reads and records the credit card details on to the device. It results in misuse of credit card and fraud.
14. **Financial Frauds**: This may be as a direct result of the above crimes like Hacking, Virus Attack, Extortion, Identity Theft, Skimming, etc.
15. **Cyberstalking**: Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization. It may include false accusations, defamation, monitoring, identity theft, threats, or gathering information that may be used to threaten or harass.
16. **Cyber Terrorism**: A cyber crime committed with an intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people.