CYBER CRIME

Shubham Verma ,Dr.Devesh Katiyar , Mr.Gaurav Goel , Abhishek Dixit ,Shubham Yadav

DR SHAKUNTALA MISRA NATIONAL REHABILITATION UNIVERSITY

DR SHAKUNTALA MISRA NATIONAL REHABILITATION UNIVERSITY

DR SHAKUNTALA MISRA NATIONAL REHABILITATION UNIVERSITY

DR SHAKUNTALA MISRA NATIONAL REHABILITATION UNIVERSITY

Shri P. L. Memorial P. G. College Barabanki

Abstract- Cybercrime is a crime that involves computers and networks. Computer crime is the meeting of any computer at a criminal place or committing a crime with a computer. Network is not involved in computer crime. Obtaining personal information and using it incorrectly. It is also a cyber crime to take away or steal someone's personal information from the computer.Computer crimes are also committed in many ways such as stealing information, erasing information, manipulating information, giving somebody else information or stealing or destroying computer parts. There are many sorts of cyber crime like spam email, hacking, phishing, virus infestation, getting someone's information online or keeping an eye fixed on anyone in the least times.

Introduction- Cybercrime is a type of crime in which the computer is an object of crime (hacking, phishing, spamming) and is used as a tool to commit any crime or crime, such as theft of information , identity theft, online fraud, child pornography, hate crimes etc. The cybercriminals that carry out this cybercrime are called. These Cybercriminals use computer and Internet technology to access personal information, business trade secrets etc. and at the same time they also use the Internet to do many malicious work. They use computers for this purpose. Criminals who do these illegal activities are also called as hackers or crackers. Cybercrime is also known by many as computer crime. Some common types of this cybercrime are online bank information theft, identity theft, online predatory crimes (child pornography) and unauthorized computer access etc.

Design - Cyber crimes are broadly divided into three categories, which are crime against

1. Individual

2. Property

3. Government

Many different types of methods are used in each category and together these methods are different from one criminal to another.

Individual: In this type of cybercrime it can take many forms such as cyber stalking, distributing pornography, trafficking and "grooming". As of now, many law enforcement agencies are taking cyber crime very seriously in this category and are also succeeding in arresting such criminals internationally by joining with many different institution.

Property: Just as criminals can steal our things, property in our real world, in the virtual world also cyber criminals can steal the bank details, login details, credit card and debit card details of the victim, and misuse them. Huh. Due to which you may face financially problem. Together some people make scammy sites and cheat people. Some send offers and malicious software through email, upon opening, your computer goes under the control of those hackers.

Government: Although it is not very common, but if crime is against a government then it is called Cyber Terrorism. If it is properly implemenation, then it can hack government websites, military websites, even official websites. They have the potential to shake the economic condition of a country.

Procedure- The procedure for reporting cyber crimes is more or less the same as for reporting any other kind of offence. The local police stations are often approached for filing complaints even as the cyber crime cells specially designated with the jurisdiction to register complaint. In addition, provisions have now been made for filing of 'E-FIR' in most of the states. In addition, the Ministry of Home Affairs is additionally launching an internet site for registering crimes against women and youngsters online including cyber crimes.If a police headquarters refuses to register the complaint, a representation could also be given to the commissioner of police/superintendent of police. If in spite of that action is not taken, the next step could either be a private complaint before the concerned court or a writ before the high court. In general, there's still tons of inertia in registration and investigation of cyber crimes. This does affect collation of electronic evidence and containment of damages, whether the offence is against an individual or business.

.

Objects- The objective of the India Cybercrime Centre will be to coordinate various efforts pertaining to cybercrime prevention and regulation in India. It aims to supply assistance to law-enforcement agencies and contribute to the fight against cybercrime in India. It will also aim to act as a centre for the emerging cybercrime jurisprudence that's evolving in India. The India Cybercrime Centre also will engage in providing training and capacity building amongst the varied stakeholders. It is expected that the India Cybercrime Centre are going to be the focus in Indian efforts against cybercrime. It will also aim to primarily provide more distinct approaches on the way to affect emerging cybercrimes. It would also aim to support various enforcement agencies in India at the Central and State level in building legal capacity for detection, investigation, and prosecution of cybercrimes as also for cooperation with various international players.

Conclusion- In short, cybercrime is developing as a serious threat. Governments, police departments and intelligence units around the world have begun to react against cyber crime. Many efforts are also being done internationally to curb cross-border cyber threats. Indian police have started special cyber cells across the country and have started educating people, so that they gain knowledge and protect themselves from such crimes