Cyber Crime and its prevention

Introduction

To be very precise, cybercrime is a criminal activity that involves a computer, networked device or a network. Cybercrime is not just limited to destroy the system, but is also aimed to generate profit for the cybercriminals. Some of the cybercrimes involves direct damage to the computers or devices or sometimes even disable them. This damage is done to the computers or the networks by either spreading the malware, illegal information, images or any other irrelevant materials. The cybercriminals infect the devices with virus, which can even spread to other devices and even to entire networks. In broader aspect, cybercrime is divided into three categories:

1. Target cybercrime: The crime in which a computer is the target of the offense.
2. Tool cybercrime: The crime in which a computer is used as a tool in committing the offense.
3. Computer incidental: The crime in which a computer plays a minor role in committing the offense.

The vital target here is with regards to finance. These include ransomware attacks, internet fraud, identity fraud as well as to steal financial account or payment card information. These cybercriminals are involved in personal data as well as corporate data theft and earn profits by reselling. Especially in such pandemic like situations wherein people have settled for remote work routines, cybercrimes are expected to grow more.

History

During the earlier times when cyberspace came into lives of the people, the IT members explored much about the development of this technology, which showed their far sightedness regarding the potential danger in the near future. The earlier records show that the encryption and decryption of information was in existence since 1900 BC. History of hacking was traced back in the 1870's. But the difference between today and back then is that, cybercrimes earlier were committed by highly educated technology experts, like programmers, engineers, administrators and those who have new technology knowledge. In the 70's, child pornography became the legal challenge. During 80's personal computers were not even known to the normal people. In the early 1990's law enforcement agencies started working on the activities. The Act was passed in 1994 and amended later in 1996. This Act prohibits unauthorized access to computers to commit espionage, unauthorized access to non-public government computer, computer fraud, damage to computer, trafficking in passwords, threats to damage a computer.

Evolution

This evolved from a Morris Worm to the ransomware. In the year 1997, Cybercrimes and viruses were initiated, that includes attack of Morris Code Worm and other. In 2004, attack of Malicious code, Torjan, Advanced worm etc. In 2007, including Identifying thief, Phishing etc. In 2010, there DNS Attack, Rise of Botnets, SQL attacks etc. In 2013, Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransomware attack etc. At present, there are Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Android hack, Cyber warfare etc.

Kinds Of Cyber Crimes

1. **Hacking**

It means unauthorized access to a computer system. Section 66 of Information Technology,Act,2000 provides that "Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking." Punishment for hacking is 3 years imprisonment or fine up to 2 lakh or both.

2. **Virus, Trojans And Worms:**

Viruses spread to the computer system. Trojan Horse is malicious, security breaking program which is designed for the particular function but it provides an unauthorised access to the target computers. A Computer Worm is a self – contained program that is able to spread functional copies of itself or its segment to other computer systems. They do not have to attach themselves to a host program.

3. **Cyber Pornography:**

Internet has provided a medium for the facilitation of pornographic crimes. Now the pictures, images and full motion video clips are also available on the internet and on certain restricted website.

4. **Cyber Stalking:**

It is harassing by the cyber criminal to the victim through phone calls, written messages, etc. sometimes it also includes serious violent acts such as physical harm, etc.

5. **Cyber Crime Related To Finance:**

It includes financial or monetary gains by illegal means. For example: Online auction frauds, jobs offer, credit card crimes etc.

6. **Phishing:**

Here the websites are usually created for stealing the personal information such as password, credit card details, etc.

7. **E-Mail Bombing:**

This includes sending huge volumes of emails in an attempt to overflow the mailbox. Also the email address of victim is shared with multiple spammers.

8. **E-Mail Spoofing:**

It is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message. It is done by changing path of email, Reply-To field etc.

9. **Logic Bombs:**

It is a programming code inserted intentionally which is designed to explode at a certain circumstances or after some time. When explodes, it deletes or corrupts the data of the target system.

Case Study

a) **The Bank NSP Case**

In this case a management trainee of a bank got engaged to a marriage. The couple used to exchange many emails using the company's computers. After some time they had broken up their marriage and the young lady created some fake email ids such as "Indian bar associations" and sent mails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

b) **Parliament Attack Case**

The Bureau of Police Research and Development, Hyderabad had handled this case. A laptop was recovered from the terrorist who attacked the Parliament. The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir. However careful detection proved that it was all forged and made on the laptop.

Cyber Law

Cyber Law came into picture to take control over the crimes committed through the internet. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices.

Cyber Law in India

Owing to the need and seriousness of the Cyber Crimes, Hon'ble Parliament of India enacted ***Information and Technology Act, 2000*** which was notified on 17 October, 2000. This act deals only in cases with cyber crimes and crimes related to electronic commerce.

The Information and Technology Act, 2000 explicitly provides the legal framework for the electronic governance by giving identification to the electronic records and digital signatures, it also expressly defines penalties for culprits after commitment of the cyber crime. It statutorily had also established a Cyber Appellate Tribunal to resolve the disputes especially related to Cyber Crimes and Online Frauds.

The statutory provisions of ***Indian Penal Code, 1860*** especially in the crime of Fraud, Criminal Intimidation, Cheating, Breach of Trust, Abetment of Suicide via Blackmailing, etc. may be charged on accused having regard to the circumstances, and discretionary powers of the Court, however it must be noted that a person cannot be punished twice for the same offence, as it will violates his Fundamental Right ensured under Article 20 (2) of the Indian Constitution i.e. Double Jeopardy.

Steps to prevent Cyber Crimes

- Never to disclose personal information publicly on websites.
- Sharing of photographs should be avoided, because there have been incidents of photographs being misused.
- One should also avoid using bank and card details on unsecured websites.
- Computers should have a firewall to protect it from hackers.
- Computers should also have anti-virus installed.
- Cyber Experts have suggested to shop only at secure websites.
- Passwords should be strong which are difficult to guess. One must change passwords or update the same, so there will be less chances of being target of cybercrime.
- Parents should use parental control software to limit the usage of their children, so that children do not surf unwanted dangerous websites.
- One must ensure that all the social media accounts of a person should be set to private account.
- The users should use secure mobile devices.
- One should also not save their passwords, pin numbers, own address or any other personal details on their mobile device.
- For businesses, one must protect the data to avoid to be hacked by criminals.

- Businesses and corporates should use encryption for most sensitive files such as tax returns or financial records, also take regular backups and store the data in different location.
- Public Wi-Fi should be avoided to use, especially financial or corporate transactions.
- One should avoid being scammed, like one should not open mails from unknown origins.

Conclusion

The rise and growth of these newly developed technologies, has also brought in many cybercrimes in recent years. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. The Government of India has enacted IT Act, 2000 to deal with cybercrimes. As we are more dependent on technology, no doubt there will be law breaking but the law makers also have to take extra efforts to curb the situation and make sure that the technology grows but in a healthy manner. The Law makers, Internet suppliers and the users, all three are expected to take efforts and abide by the Law.