Survey on Cyber Crime & Cyber Security

Archit Kapur[1], Himank Rastogi[2], Harshit Goyal[3], Dr. Preeti Sharma[4]

[1,2,3]B.Tech students, Department of Information Technology, Inderprastha Engineering College
[4]Associate Professor, Department of Information Technology, Inderprastha Engineering College

---

Abstract: The web is developing quickly. It has offered ascend to open new door in each field like – diversion, business, sports, training, and so on. It is generally evident that each coin has different sides, same for the web, it utilizes both bit of leeway and drawback. Cybercrime is developing as a danger. Overall governments, police divisions and insight units have begun to respond. Activities to control cross fringe digital dangers are coming to fruition. Indian police has started exceptional digital cells the nation over and have begun instructing the work force. This article depends on different reports from news media and things happening over the internet

1. Introduction

Internet today has become a very important part of our lives, in this modern era, we are capable of doing things we couldn't imagine doing before. We can access any information on our fingertips. The Internet has become a way of life of billions of people in this world due to the increasing dependency and reliance on human on these machines.

Internet as opened all possible ways to communicate via emails, video and audio conferencing, and many other IT solutions and has put forward in betterment of human mankind. The Wide use of the internet and IT technology has also given to several crimes i.e. cyber crimes.

India is one of the fastest-growing countries so, in Asia India has the second-largest internet users in country. The Internet has allowed people to use it anytime, anywhere but with this increasing use, it has given birth in many illegal activities.

2. Cyber Crimes

Cyber Crime is also known as computer crime, which is the use of a computer to fulfil illegal ends which include committing fraud, child pornography, stealing identities, fake passports, fake currency, violating privacy

Defining Cyber Crimes -

Cyber Crime is basically an attack on information about individuals, corporations, and government. The attacks basically take place on a virtual body that is the computer or on the designated servers.

Cyber Crime runs over a range of exercises. Toward one side are violations that include principal breaks of individual or corporate security, for example, attacks on the uprightness of data held in computerized safes and the utilization of wrongfully acquired advanced data to coerce a firm or person. At the other end are the crimes that disrupt the working of the internet. These include hacking, spamming, DDoS attacks which are basically used to create fear in the minds of the people.

3. Types of Cyber Crimes

Identity theft and invasion of privacy: Stolen credit cards can be used to reconstruct an individual's identity. When criminals steal these records, their main motive is to steal money from the card, causing great losses to the credit card companies and the holders of credit cards. Another trick which these people use is to sell this information to some other person who can use it in a similar fashion.

4. Internet Frauds:

4.1. ATM FRAUDS:

To access the account, the user provides the card and PIN number. The hijackers have developed ways to reduce all data from card magnetism and user PIN. Also, this information is used to create counterfeit cards and then used to withdraw cash from a casual account.

4.2. CHILD PORNOGRAPHY:

The possession of child pornography, defined here as images of children under the age of 18 involved in sexual activity, is illegal in the United States, the European Union, and many other countries, but it remains a problem that does not have an easy solution. The Internet also offers pedophiles an unprecedented opportunity to commit criminal acts by using "chat rooms" to identify and attract victims. Here the earth and the material world collide in a dangerous way. In many countries, state authorities now come as children to chat children; despite more information on the practice, leftists continue to interact with these "children" to meet offline.

4.3. DDOS ATTACK:

Distributing the DoS. Distributed attack (DDoS) occurs when multiple systems are filled with bandwidth or target system resources, usually one or more web servers. Such attacks are often triggered by numerous vulnerable systems (for example, a botnet) that flood the traffic-oriented system.

4.4. DRUG TRAFFICKING:

Darknet markets are used to buy and sell online entertainment drugs. Some drug smugglers use texting tools to record contact with drug mules. The Black Silk Road website was a major online drug store before it was shut down by legal practitioners

4.5. MALICIOUS SOFTWARES:

Malicious software, also known as malware, can enter your computer and do things without your permission, giving consumers full access to your data, devices, and applications. The malicious software was originally designed as a means of cyber hacking, breaching computers, or changing your domain and accessing your information. It is then adopted by criminals who open cyber attacks to steal valuable business and personal data by ransom, hack passwords to access bank accounts, or to track information to steal an identity.

4.6. VISHING:

Vishing (by voice or VoIP phishing) is a trick in which people are tricked into revealing sensitive financial or personal information to unauthorized organizations. Vishing works on sensitive information but doesn't always happen over the Internet and is done using voice technology. The most obvious attack can be by voice mail, VoIP (voice over IP), or by cellphone or cellphone.

4.7. SMS SPOOFING:

SMS i.e. short message service is a most commonly used service to send text messages from sender to receiver via mobile phone. SMS Spoofing is done by tampering the sender's address information. The message sent is not changed but the sender's address i.e. the mobile number is swapped with the alpha-numeric text. The message sent seems to come from a legitimate number so it's hard to check if the sender is real or not. If a user claims that the message received is spoofed then they should contact their service provider and legal law enforcement, so that they can track the real address of the sender.

4.8. WEB-JACKING:

Web-jacking is a terminology acquired by the term Gi-jacking. In such offense, the hacker procures control over someone else's website and can even hinder the information and data. This may be done to leak or obtain information due to some political affairs for e.g. the website of MIT(Ministry of Information Technology) was hacked by Pakistani hackers and the site of the Bombay crime branch was hacked to delete some secret data.

In this process, the hacker can also crack the password of the website and change it so the authentic owner loses control over the website. In the process of Web-jacking, the real website is never touched but the DNS that resolves the website URL to IP address is compromised. Basically when to give a URL then the browser sends DNS request to connect to the URL but when a website is Web-jacked, then the DNS request is triggered to different URLs very similar to the real one. The hacker may ask for a ransom to give control to the real owner or it can be done to defame the reputation or brand value of a company or an entity.

5. Cybersecurity:

5.1. Investigation:

The investigations start with the IP Address trace of the one who has committed the fraud. Criminal representatives, such as law enforcement officers, prosecutors, and judges, are responsible for protecting, reducing, detecting, investigating, prosecuting, and judging online crime. Some agencies responsible for cybercrime cases vary by country.

5.2. Awareness:

As technology and more people rely on the Internet to store sensitive information, such as banking or credit card information, criminals are more likely to steal this information. Cybercrime is becoming a threat to people worldwide. There is a growing awareness of how information is protected and the strategies that criminals use to steal information.

6. Role of Judiciary:

In a democratic country, the most important annex is the judicial system, which resolves the conflicts among parties. For the proper working of the judiciary, the rules of jurisdiction play an important role.

In the span of information and technology, criminals are using new technology to commit crimes. Therefore a different judicial approach is required toward the technological offense for the prevention of crimes.

In India, the cyber world is modulated by the Information Technological Act, 2000 also known as the IT Act. It was an upshot of the recommendation of the United Nations Commission of International Trade law, 1966. It defines and penalize the offense related to computer.

The Indian government ratified the IT act, 2000 with the goal to provide legal remembrance for the transaction carried out through electronic data interchange and other means of electronic communication. The IT Act was enacted for the very purpose of starting e-commerce, provides pursuance and penalties for violation of crimes.

This was the reason to include Chapters of Offense in information and technology act, 2000. It furnishes remedies for offense like illegal access, downloading, injection virus, denial of access.

Many cases arose in the period which alarmed the need of proper jurisdiction in the field of cybercrime

6.1. Bazee.com:

In December 2004 the Chief Executive Officer of Bazee.com was arrested for selling compact disk (CD) with offensive material on the website, and even the CD was sold in the market of Delhi.

6.2. State of Tamil Nadu c. Subhas Katti:

Governed by the Chennai court in 2004. The women who was separated from her spouse complained to the police department about a man who was sending her pornographic and annoying messages. The accused opened a fake email account in the name of the woman. The victim also received phone calls by people who believed that she was seeking for sec work. Then the victim was dropped by two years of rigorous imprisonment.

6.3. Air Force School Case:

The case was filed in the juvenile court, Delhi on the charge of cyber pornography. Many jurists say this was the first Indian cyber pornographic case. The student of Air Force Bal Bharti Schol, Lodhi Road, New Delhi was arrested in the April year 2001.

7. Conclusions:

It is observed from the previous studies with an increase in the IT industries cyber crimes has also increased. The true dilemma is that these crimes are committed by educated people who have a good knowledge of this technology, but not using their knowledge for human mankind but they use it for ill. There is a need for a proper understanding of the computer fundamentals for their use in a proper manner.

Thinking practically hacking or cyber crimes wouldn't just go away and hash truth is it will become stronger and stronger, so we should study the past crimes how they are committed so that we can save ourselves from future crimes.

Cyber-law is a little rusted and old on the other hand the hacker is evolving rapidly. So we need new and better laws so that they can save us from such crimes and safeguard our rights. The Internet has proved that it is a real gift to us neither of us can imagine our lives without the internet so we need to use it maturely.

Yet India has come forward with many laws for stopping cyber crimes but cyber law cannot be unvarying we need to update according to the new crimes that are being committed every day and it has to change with changing time.

8. References:

[1] Whitney Bolton,"The Growing Issues of Cybercrime in a Predominately Technological Age", Liberty University, October 2015.

[2] Gert Jan van Hardeveld, Craig Webber, Kieron O'Hara,"Discovering Cyber Fraud Methods", University of Southampton, May 2016.

[3] Reuver, M., Sørensen, C. & Basole, R. C. The digital platform: a research agenda,2017

[4] Dhatri Ganda, Pooja Kalola, Nirali Borad," World of Cyber Security and Cybercrime," Atmiya Institute of Technology and Science, Journals August 2018.

[5] Radanliev, De Roure, Cannady, Montalvo, Nicolescu & Huth, "CYBER RISK IMPACT ASSESSMENT", University of Oxford, April 2019.