4th International Conference on Recent Developments in Science, Humanities & Management-2019
Institution of Engineers,Chandigarh (India) (ICRDSHM-19)
17th February 2019, www.conferenceworld.in ISBN:978-93-87793-70-5

CYBER CRIME IN INDIA: CAUSES & PREVENTIONS

Veerpal Kaur

Assistant Professor, Department of Compter Science,

Baba Farid Group of Institution, Bathinda, Punjab

Abstract

Cybercrimes are any crimes that involve a computer and a network. Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). The main causes of cyber-crime are Internet criminals almost never get caught, lack of legal evidence, lack of resources etc.Today, criminals that indulge in cyber-crimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work.

Keyword: *IT (Identity Theft), OPC (Online Predatory Crimes), LEA (Law Enforcement Agencies), LOR (Lack of Resources).*

Introduction of Cyber Crime

Cybercrimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime. Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.Common types of cybercrime include online bank information theft, identity theft (IT), online predatory crimes

(OPC) and unauthorized computer access. More serious crimes like cyber terrorism are also of significant concern.

Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. Even in the real world, crimes like rape, murder or theft need notnecessarily be separate. However, all cybercrimes involve both the computer and the person behind it as victims, it just depends on which of the two is the main target. Hence, the computer will be looked at as either a target or tool for simplicity's sake. For example, hacking involves attacking the computer's information and other resources. It is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification system.

• Computer as a tool

When the individual is the main target of Cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. Theseare the crimes which have existed for centuries in the offline. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace andapprehend.

• Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using he computer as a tool, these crimes requires the technical knowledge of the perpetrators. These crimes are relatively new, having been in existence for only as long as computers have - which explains how unprepared society and the world in general is towards combating these crimes. There are

ISBN:978-93-87793-70-5

numerous crimes of this nature committed daily on the internet. But it is worth knowing that Africans and indeed Nigerians are yet to develop their technical knowledge to accommodate and perpetrate this kind of crime.

Objectives of Study

"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones." The main objective of the study are as follow:

- To find out the causes of cyber-crime,
- To find the prevention of cyber-crime.

Research Methodology

For this study secondary data is used. As there are so many varieties of crimes that are committed on the internet daily, some are directed to the computer while others are directed to the computer users.

Types of Cyber Crime

1. Hacking
2. Theft
3. Cyber Stalking
4. Identity Theft
5. Malicious Software:
6. Child soliciting and Abuse

Causes Cyber Crime

Wherever the rate of return on investment is high and the risk is low, you are bound to find people willing to take advantage of the situation. This is exactly what happens in cyber crime.

ISBN:978-93-87793-70-5

Accessing sensitive information and data and using it means a rich harvest of returns and catching such criminals is difficult. Hence, this has led to a rise in cyber-crime across the world.

1. Internet criminals almost never get caught

The world is full of malicious individuals who have no problem skirting rules and laws, as well as taking property that belongs to other people. Bad people exist -- and the Internet is a very low-risk neighborhood in which they can run amok.There are tens of thousands of Internet criminals, almost none of whom get caught or prosecuted. If you're an Internet criminal, you have to be especially brazen for a long time and make mistakes before you get caught.You don't have to be a mastermind or user hacker. One of the most popular misconceptions is that you have to be hyper intelligent to get away with cyber-crime. The exact opposite is true. Most Internet criminals I've met (and chatted with online) are not particularly smart. They couldn't program a simple notepad application, and they certainly don't have to be as smart as the average defender.

2. Indefinite legal jurisdiction

Most Internet crime takes place across international borders. Law enforcement agencies (LEA) are always limited to jurisdictional boundaries. For instance, a city police officer in Billings, Mont., can't easily arrest someone in Miami, Fla. We have federal law enforcement agencies, which reach across city and state boundaries, but they can't easily traverse international boundaries.Sometimes law enforcement agencies of one nation work with another nation's law enforcement, but these occasions are rare. Plus, the really big ones involved with the majority of the Internet crime, like Russia, China, and the United States, certainly don't cooperate with each other.

3. Lack of legal evidence

Another huge impediment to successful convictions is the lack of official, legal evidence. Most courts accept "the best representation" of evidence recorded during the commission of a crime. But most computer systems -- and many networks in totality -- don't collect any evidence at all,

much less evidence that might stand a chance of holding up in court. I'm still surprised by the number of computers I investigate that don't, at a minimum, have event logging turned on.Even if more evidence was collected, most of it wouldn't stand up to a decent lawyer, assuming it would even be allowed in court. Collecting and preparing good legal evidence takes planning and commitment. Few organizations have the dedication or expertise.

4. Lack of resources (LOR)

Few victims or victim advocacy groups have the resources, technology, or funding to pursue Internet criminals. I know many people who have lost tens of thousands of dollars to fraudulent transactions, including car sales, stock trades, bank transfers, and so on. Unfortunately, the amount lost usually pales compared to the cost of the resources that would be needed to recover the funds.Many victims are too ashamed of their own gullibility to report the crime. If they do, a report will be taken -- and that's that. Your local enforcement agency isn't about to cross international boundaries to try and to recover your personal money. You can report it to the proper authorities, but rarely will they do anything to recover the damages or prosecute.

5. Cybercrime isn't hurting the economy enough

Lastly, the amount of Internet crime isn't hurting economies enough to raise a global red alert. Sure, Internet crime probably results in the loss of hundreds of millions -- or perhaps several billion -- dollars each year, but that amount of crime has persisted for a long time, well before the Internet.Most of today's Internet crimes are newer versions of crimes and scams that have been occurring for decades before the Internet was around. Take credit card fraud: Retail stores would once look up known fraudulent credit card numbers in little paper books that the credit card vendors handed out. Nigerian scams have been around, via paper letters, phone calls, or faxes, at least since the 1990s.

ISBN:978-93-87793-70-5

Prevention of Cyber Crime

Cybercrime prevention can be straight-forward - when armed with a little technical advice and common sense, many attacks can be avoided. In general, online criminals are trying to make their money as quickly and easily as possible. The more difficult you make their job, the more likely they are to leave you alone and move on to an easier target. The tips below provide basic information on how you can prevent online fraud.

- Keep your computer current with the latest patches and updates.
- Make sure your computer is configured securely.
- Choose strong passwords and keep them safe.
- Protect your computer with security software.
- Protect your personal information.
- Online offers that look too good to be true usually are.
- Review bank and credit card statements regularly.

Conclusion

As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cybercrimes. While law enforcement agencies are trying to tackle this problem, it is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid being a victim of cybercrimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet.

ISBN:978-93-87793-70-5

Reference:

- **Cyber Crime is here to stay**. Indian Express, January 2002 (http://www.asianlaws.org/press/cybercrime.htm)
- **Cyber-Crime… and Punishment? Archaic Laws threaten Global Information.**

  www.mcconnellinternational.com/services.cybercrime.htm, December, 2000
- Golubev's interview. http://www.crime-research.org/Golubev_interview_052004/
- Prof. Hammond, Allen. **The 2001 Council of European Convention on Cyber-Crime: an Efficient Tool to Fight Crimes in Cyber-Space?** June, 2001,COEConvention.Cyber-crime.pdfhttp://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.
- **Cyber Crime is here to stay**. Indian Express January 2002 http://www.asianlaws.org/press/cybercrime.htm
- Katz, Eli **Unisys Suite Aims To Detect Criminal patterns,** June 10, 2003

  http://www.computerworld.com/industrytopics/financial/story/0,10801,81979,00.html
- Sinrod, J. Eric. **What's Up With Government Data Mining?** September 6, 2004,
  http://www.ustoday.com/tech/columnist/ericjsinrod/2004-06-09-sinrod_x.htm
- **Cyber-Crime… and Punishment? Archaic Laws threaten Global Information.** December, 2000
  www.mcconnellinternational.com/services.cybercrime.htm,