Chapter 3
An Indian and Global Perspective on Cybercrime

K. S. Umadevi
VIT University, India

Geraldine Bessie Amali
VIT University, India

Latha Subramanian
University of Madras, India

ABSTRACT

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 advancement of technology has made us dependent on internet for all our needs. Internet has given us easy access to everything without moving from our place. Social networking, online shopping, storing data, gaming, online studying, online jobs, every possible thing that man can think of can be done through the medium of internet. However, with the development of the internet and its related benefits, the concept of cybercrimes arose. Cybercrimes are committed in different forms. In a report published by the National Crime Records Bureau, the incidence of cybercrimes under the IT Act has increased by 85.4% in the year 2011 as compared to 2010 in India, whereas the increase in incidence of the crime under IPC is by 18.5% as compared to the year 2010.

DOI: 10.4018/978-1-5225-8241-0.ch003

INTRODUCTION

Any sort of crime committed using a computer either as the object of the crime or as a tool to commit the offense is called cybercrime. In 2015 consumers in the UK reported a loss of more than 1.7 billion pounds due to cybercrime. This is way more than other serious crimes like illegal drug trafficking. This sharp increase in crime is due to the growth in e-commerce and online banking. In the last few years alone there have been hundreds of millions of cases of credit card theft; cases of compromise in Social Security Numbers and health care records. Crimes like these are committed by hackers who exploit the vulnerabilities in software which are sometimes caused by naive mistakes made by the people while using the software.

People committing cybercrime cannot be pinned down to a specific class of individuals. They may belong to any race, religion or sex. It could be a teenager from high school who just wants to impress his girlfriend or even a member of a terrorist group. Countries are now not only equipping their regular armies to fight crime but also their cyber army. In fact, the next world war might not be fought with weapons but with computers which could be used to shut down national water supplies, energy grids, and transportation systems.

By Google Security Princess Parisa Tabriz, an attacker can infect someone's computer in two ways. The first way is to deceive the person into installing a program on their computer. Many viruses are often disguised as security updates. The second way is to use the vulnerability in the software already installed in the system. In such a case the attacker doesn't even need permissions to install a virus. Once the virus is installed then the system's data is compromised. The attacker can then steal sensitive data like bank account details etc. He can also remotely monitor and control the computer. He can even create a digital army with millions of computers and plan a full-fledged attack and even take down websites. This kind of attack is called a Distributed Denial of Service attacks (DDoS).

A denial of service is when hackers overwhelm a website with too many requests. Most of the websites are ready to handle a large number of requests. But if the requests are in the order of billions and trillions then the servers will be overloaded and they stop responding. Hackers also send out a large number of spam emails which deceive the user into giving their sensitive information. Information such as passwords to bank accounts can be collected from unsuspecting users by making them logging into their bank accounts. This is called a phishing scam. Hackers then use the newly obtained passwords to steal money from bank accounts.