Research Paper Computer Science

Be aware from Cyber Crime

*Akanksha S. Patil

* MCA, University of Pune

Introduction:
An old adage tells us "Character is what you do when no one is watching." So it is with the Internet. Online, people can feel invisible and capable of doing things they normally wouldn't do in person or in public - things that they know might be wrong. As the Internet becomes an indispensable tool for everyday life.

National Research Council says "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

Cyber crime is nothing but computer crime or Internet crimes. It is a criminal activity committed on the internet. This is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money. It is *illegal activity committed on the internet. The internet, along with its advantages, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like e-mail espionage, credit card fraud, spams, and software piracy and so on, which invade our privacy and offend our senses. Criminal activities in the cyberspace are on the rise.*

Cyber crimes can be basically classified as:
1. Cyber crimes against persons.
I. Indecent exposure
II. Unauthorized access
III. Cheating & Fraud
IV. Defamation
V. Dissemination of obscene material
VI. Irritating via e-mails
VII. Email spoofing
VIII. Cyber-stalking

2. Cyber crimes against property.
I. Unauthorized access
II. Transmitting virus.
III. Computer vandalism
IV. Internet time thefts
V. Intellectual Property crimes
VI. Netrespass

3. Cybercrimes against Society
I. Pornography (basically child pornography).
II. Polluting the youth through indecent exposure.
III. Trafficking
IV. Financial crimes
V. Sale of illegal articles
VI. Online gambling
VII. Forgery

The Department of Justice categorizes computer crime in three ways:

1. The computer as a target - attacking the computers of others (spreading viruses is an example).
2. The computer as a weapon - using a computer to commit "traditional crime" that we see in the physical world (such as fraud or illegal gambling).
3. The computer as an accessory - using a computer as a "fancy filing cabinet" to store illegal or stolen information.

As the cases of cybercrime grow, there is a growing need to prevent them. Cyberspace belongs to everyone. There should be electronic surveillance which means investigators tracking down hackers often want to monitor a cracker as he breaks into a victim's computer system. The two basic laws governing real-time electronic surveillance in other criminal investigations also apply in this context, search warrants which means that search warrants may be obtained to gain access to the premises where the cracker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to gain unauthorized access and other evidence of the crime.

Different types of cyber crime:
1. Cyber Terrorism:
Here are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal.

2. Fraud:
Credit fraud is another common form of cyber crime. Certain computer viruses can log keystrokes on your keyboard and send them to hackers, who can then take your Social Security number, credit card number and home address. This information will be used by the hacker for his own means.

3. Spam:
The most common type of cyber crime is spam. While email spam laws are fairly new, there have been laws on the books regarding "unsolicited electronic communications" for many years

4. Cyber Bullying:
Harassment, or cyber bullying, is a growing problem among teenagers. Many countries in Europe and several states in the United States have laws to punish those who consistently harass somebody over the Internet.

6. Piracy:
Far and away the most talked about form of cyber crime is thievery. Yes, downloading music from peer-to-peer websites is illegal and therefore a form of cyber crime.

5. Drug Trafficking:
Believe it or not, drug trafficking is happen over the Internet. Many traffickers use encrypted email or password-protected message boards to arrange drug deals.

Scope of the study:
The research work highlighted the cybercrime and its effects on people, Government and different organization working in society. It also focuses on steps that are taken by Indian Government to prevent cyber crime.

Objective of the study:
The study helps to know hazards of cyber crime and explains different ways through which cyber crime can be spread. Following are the objectives of the study.

1. To analyze the cyber crimes.
2. To make people aware about cyber crime.
3. To study the initiatives taken for avoiding cyber crime.
4. To understand how it is dangerous to people, government and financial aspects.

Research Methodology
1. Type of research:
Since, the researcher has been carried out for analytical study of all the facts and figures of surveyed data and other information and observation. It would be more appropriate to call it a combination of descriptive, analytical and empirical type of research.

2. Research problems:
How cyber crime was born?
What are cyber crime and its hazards?
In what manner cyber crimes develop?
How different organizations come together and solve the problem of cyber crime?

Cyber Criminals:
The cyber criminals constitute of various groups or categories. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals:

1. Children and adolescents between the age group of 6 - 18 years:
The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove them, to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the Bal Bharati (Delhi) case was the outcome of harassment of the delinquent by his friends.

2. Organised hackers:
These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives. Further the NASA as well as the Microsoft sites is always under attack by the hackers.

3. Professional hackers / crackers:
Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are van, employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

4. Discontented employees:
This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

Steps taken by Indian government against cyber crime:
With so much of our everyday communication and commercial activity now taking place via the Internet, the threat from cybercrime is increasing, targeting citizens, businesses and governments at a rapidly growing rate. The Indian parliament considered it necessary to give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which the Information Technology Act 2000 was passed and enforced on 17th May 2000.the preamble of this Act states its objective to legalise e-commerce and further amend the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Book Evidence Act1891 and the Reserve Bank of India Act 1934. The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000. So, that they may regulate and control the affairs of the cyber world in an effective manner.
Section 43 in particular deals with the unauthorized access, unauthorized downloading, virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person. This section provide for a fine up to Rs. 1 Crore by way of remedy. Section 65 deals with 'tampering with computer source documents' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Further section 67 deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with fine up to Rs. 2 lakhs.

Some cases of cyber crime in India:
1. 'Youth in jail for sending email threat', The Hindu, Friday Aug 10 2007.
2. 'Phishing for trouble', The Hindu, Wednesday, Jan 17 2007
3. 'Cyber crime Up Police found wanting', Chandigarh Tribune, Monday May 28 2001
4. 'Nasik Police play big boss for internet voyeurs', Hindustan Times, Sunday, Oct 28 2007
5. 'Losses due to cyber crime can be as high as $40 billion', The Hindu Business Line May 21 2007
6. 'Licenses mooted for Internet Cafes', The Hindu Business line Saturday, Aug 23, 2007.

List of steps you can take to avoid becoming a victim of cybercrime:
1. Education:
Educating yourself about the types of scams that exist on the Internet and how to avert them, you are putting yourself one step ahead of the cybercriminals.

2. Keep your system updated:
a. **Change default passwords and account names in place when your computer system was installed.**
b. **Use encryption software to protect customers' financial information from theft during transactions**
c. **Limit access of sensitive information to those who need to see it.**

3. Use a firewall:
Firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set.

4. Practice safe surfing:
When navigating the web, you need to take precautions to avoid phony websites that ask for your personal information and pages that contain malware. Use a search engine to help you navigate to the correct web address since it will correct misspellings. That way, you won't wind up on a fake page at a commonly misspelled address.

5. Shopping safe:
If you don't feel comfortable while buying or bidding or bidding on an item over the web, just to avoid purchasing such thing.

6. Need of strong password:
To understand why you need a strong password, you need to understand the risks of having your account compromised - namely, malware. Hackers, by simply guessing an account's weak password, can introduce malware into your website, which can:

- Redirect your website's visitors to a harmful website
- Install malicious content to your visitor's computer

Conclusions:

In the Present scenario life is highly dependent on internet. Internet is basic need because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of web site for different purposes. Looking at the full range of cybercrime, researcher has shown how the increase in personal computing power available within a globalized communications network has affected the nature of and response to criminal activities. The attempt has been made in this article to focus on what is cyber crime, prevention for cyber crime and steps taken by Indian government to avoid cyber crime. These offences involve not only the use of computers but internet and different tools and techniques.

Major cybercrimes reported in India are denial of services, defacement of websites, spam, computer virus and worms. Especially financial sectors face the problem of cybercrime widely.

REFERENCES

• Cyber crime: The Transformation of Crime in the Information Age By: David S. Wall (University of Leeds) | • Access Denied: The Complete Guide to Protecting Your Business on the Internet, by Cathy Cronkhite; Jack McCullough, ISBN: 0072133686, Aug 2001 | • Pawan Duggal,"Cyber Law": The Indian Perspective. | • Secret Software: Making the Most of Computer Resources for Data Protection, Information Recovery, Forensic Examination, Crime Investigation and More, by Norbert Zaenglein, ISBN: 1581600887, July 2000. | • Wikipedia | • www.crime-research.org/analytics/702/ | • www.thehindu.com/news. | • www.indianexpress.com/news. | • http://searchsecurity.techtarget.com