International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 6 1531 – 1534

Awareness and Protection Against Cyber Threats

Madhulika Singh
Department of Information Technology
Pacific Institute of Management, Pacific University
Udaipur, India
madhulika.singhr@gmail.com

Arun Kumar Singh
Department of Electronics and Communication
Graphic Era University
Dehradun, India
aruns444@gmail.com

***Abstract*—** The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and destroy important files, read and misuse their e-mail, steal their credit card details from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. Abuse of computers has given birth to new Crime as Cybercrimes. Due to this an act was passed known as IT ACT 2000 to regulate, monitor and minimize the cybercrimes over Internet. This paper describes various types of cyber crime and, available laws and security tips to protect us from these types of crimes.
.

*****

I. INTRODUCTION

Internet is the playground of Hackers and Malicious programs with the growing variety of mobile devices, social networking sites, and online offers, it is important to protect yourself and your computer. Due to the advance technology of the Internet, the government, private industry and the everyday computer user have fears of their data or private information being comprised by a criminal hacker. With anonymously growing of Internet it has become necessary to make a body that has controls over the traffic flowing over Internet. Because one can misuse it and can commit crimes. India also has Cyber Law.

II. INDIA IT ACT 2000

The Information Technology Act, 2000 was passed as the Act No. 21 of 2000, got approval on 9th June and was made effective from 17th October 2000.
The Act basically deals with the following issues.

1) Legal Recognition of Electronic Documents
2) Legal Recognition of Digital Signatures
3) Offenses and Contraventions
4) Justice Dispensation Systems for Cyber Crimes.

III. INTERNET CRIMES AND FRAUDS

Internet crime is most often thought of as a crime that is committed with the aid of a computer. Yet the computer has various roles in high tech crime as tool and as target [6].
Common Internet crimes and frauds includes

1) Cellular telephone fraud
2) Data alteration
3) Data destruction and sabotage
4) Data extortion
5) Data theft
6) Desktop counterfeiting
7) Disclosure of confidential data
8) Electronic letter bombing
9) Identity theft
10) Internet consumer fraud
11) PBX fraud
12) Reading another person's E-mail without permission
13) Sale of proprietary data
14) Software piracy
15) Stolen long-distance calling cards
16) Unauthorized access and entry to system and information
17) Voice mail frauds

IV. TYPES OF CYBER CRIMES AND APPLICABLE LAWS

1) Email Hacking:

Case 1:

1. Victim's password has stolen & obscene emails are sent to his/her friends from address book.
2. Section 43, 66, 67 of IT ACT, 2000 & section 509 of IPC.
3. Person who is hacking email account as well as person who is misusing it is responsible for this crime.

Case 2:

1. Victim's password has stolen & hacker tried to threaten victim to extort money from him
2. Section 43, 66, of IT ACT, 2000 & section 384 of IPC.
3. Person who is hacking email account as well as person who is misusing it is responsible for this crime.

Case 3:

1. Victim's password has stolen & hacker is sending virus, worms or either 419 scam mails from his/her account
2. Section 43, 66, of IT ACT, 2000.
3. Person who is hacking email account as well as

person who is misusing it is responsible for this crime.

2) Virus Dissemination

Viruses are programs which affect available files on the computer & spread over networks using internet.

Case 1:

1. Virus is targeting individual or specific organization which is not detected by antivirus softwares.
2. Section 43, 66 of IT Act, 2000 and section 426 of IPC [6]
3. The virus writer as well as the person who is spreading virus is responsible for this crime.

Case 2:

1. The person pirates softwares & send Pirated CDs
2. Section 43, 66 of IT Act, 2000 & 63 of Copyrighted act.
3. The person who pirates as well as people who buy & use those softwares are responsible.

3) Cyber Pornography Crimes

As per IT act, 2000, publishing, transmitting & causing to be published any porn material in electronic format is considered as cyber crime. There are millions of websites which includes pornography material online.

Case 1:

1. Suspect abuse specific person by publishing his/her nude/naked pictures, clips & sell it online.
2. Section 67 of IT Act, 2000
3. The person who creates & maintain such websites are liable for such crimes.
4. Sometimes cyber café owners are also liable as they are allowing their customers to view such websites.

4) Social Networking (Facebook / Orkut) Fake Profile Impersonation Cases

Case 1:

1. Fake profile of female is created & photograph, phone number & address has been posted on the profile.
2. The profile also describes female as prostitute.
3. Section 67 of IT Act, 2000 & 509 of IPC.

Case 2:

1. Fake Community has been created & wrong information about individual/organization has been posted.
2. Section 153A & 153B of IPC.

5) Web Defacements

1. Crackers/Hackers found loopholes in website. Hacker then replaces the index page with some other page. Hacker can even delete data available of websites.
2. Section 43, 66 of IT Act, 2000 & in some cases 67 also.[7]

6) Email Scams

1. Suspect sends thousands of emails & convinces victim to get out of lot of money. Suspect can also give lucrative offer like job offers, lottery & investment offers.
2. Section 420 of IPC.
3. Sender of an email, sometimes bank account are liable for this crime.

7) Source Code Theft

Program source code is most important asset of any organization. Source code theft is common in software/IT companies.

Case 1:

1. The person theft the code & sell it to the other party after making modification in the source code.
2. Section 43, 65, 66 of IT Act, 2000 & 63 of copyright act.
3. The person who has stolen the code is liable.

Case 2:

1. The person theft the code & sell it to the company competitors.
2. Section 43, 65, 66 of IT Act, 2000 & 63 of copyright act.
3. The person who has stolen the code as well as the person who buys such code is liable.

8) Theft of confidential information

Case 1:

1. Employee steals confidential information of company & mail to competitors & also posts it on to websites & forums.
2. Section 43, 66 of IT Act, 2000 & 426 of IPC.

Case 2:

1. Employee steals confidential information of company & threatens company to make it public unless company pays him money
2. Section 43, 66 of IT Act, 2000 & 384 of IPC.
3. The person who has stolen information as well as

person who threaten victim are liable.

Case 3:

1. Business rivals obtain information using hacking, social engineering & use it for their benefits.
2. Section 43, 66 of IT Act, 2000 & 426 of IPC.
3. The person who has stolen information as well as person who misuse information, both are liable.

9) Online Sale of illegal articles

Sale & Purchase through net. There are web sites which offer sale and shipment of contrabands drugs. They may use the techniques of stenography for hiding the messages. Depending upon illegal items, provisions of narcotic drugs, psychotropic substance act, and arms act, wild life related laws can also be applied.

10) Credit Card Frauds

Case 1:

1. Victim's Credit cards have been misused on airline websites, online gambling websites, and pornography websites.
2. Section 43, 66 of IT Act, 2000 & 420 of IPC.
3. All persons who have stolen information to who have misused information online are liable.

11) Mobile Crimes

Mobile Phones have become popular means of communications. SMS forging is method to spoof identity of SMS. Call Forging is method to spoof caller ID of Call.

Case 1:

1. Suspect has misused victim's number to send SMS or make call to other person/ competitors.
2. Section 65, 66 of IT Act, 2000.
3. The person who is misusing the victim's number as well as company who allows user to change identity of SMS or Call are liable.

V. ADVANTAGE OF CYBER LAW

Following are the advantages of cyber laws

1) .Secured E-commerce for Setting Online Business.
2) Digital Certificate for securing site.
3) Blocking unwanted content from Internet.
4) Proper monitoring of traffic.
5) Security Against common frauds.
6) Born of new Security Agencies like Cyber Cell.
7) Software as well as Hardware security.

VI. PROTECTION FROM FRAUD WITH INTERNET SECURITY TIPS

Following are some security tips

1) Do not use your full or partial Social Security number as a Personal Identification Number (PIN), user ID or password [5].

2) Make sure that your password is 8 or more characters and combines letters, numerals, and symbols. Do not use the same user ID and password for your financial accounts as you do for other sites.

3) Consider a screen lock on your mobile device. Many mobile phones offer this option, as well as other customizable security settings, which can help keep your phone and information secure.

4) Do not use your mobile device to store sensitive personal information or bank account numbers.

5) Never respond to urgent email claiming to be from a bank or any company that requests your account information or personal details [9].

6) Limit the amount of personal information you provide on social networking sites. The more information you post, the easier it may be for a criminal to use that information to steal your identity, access your data, or commit other crimes.

7) Be cautious about messages you receive on social networking sites that contain links. Even links that look like they come from friends can sometimes be harmful or fraudulent – attempting to gain control of your computer or steal your personal information. If you are suspicious, don't click the link. Contact your friend or the business directly to verify the validity.

8) Keep your computer operating system and browser up to date with the latest software and security downloads. These may be called "patches" or "service packs" and should be installed as soon as possible.

9) Don't open attachments or install free software from unknown sources; this may expose your computer and the information on it to unauthorized sources.

10) Install a comprehensive Firewall/Antivirus/Anti-spyware software package on your computer. These software suites help detect and remove viruses and spyware, which can steal vital information.

VII. CONCLUSION

One of the most significant findings to emerge from this research is that Internet is the playground of Hackers and Malicious programs. To be safe on the internet we have to remember to never respond to any email advertisement, and only visit sites we know or have book marked, and verify the

address before browsing further. Always Use Genuine Operating System Regularly Updated with Internet. Set a strong password with a mix of alphabets, numbers and special characters. Never click on any links sent through mail or chat. It may be a link which can steal your cookie or inject any viruses.

REFERENCES

[1] RD. Hartley, "Ethical Hacking: Teaching Students to Hack", EastCarolina University, http://www.techspot.com/news/21942-universityoffers-ethical-hacking-course.html, , 2002.

[2] T. Wulf, "Teaching ethics in undergraduate network"Consortium forComputing Sciences in College, Vol 19 Issue 1, 2003.

[3] I. See http://www.cs.ruu.nl/cert-uu/satan.html.

[4] N.B. Sukhai, "Hacking And Cybercrime", AT&T, 2005.

[5] www.facebook.com/i3indyatechnologies.

[6] http://www.cyberlawsindia.net/

[7] http://security.tipcentral.net/

[8] C.C. Palmer, Ethical hacking , IBM systems journal, http://www.research.ibm.com/journal/sj/403/palmer.html , 2001.

[9] www.facebook.com/mrooppss.