# CYBER CRIME AND MEASURES TO PREVENT IN LIBRARIES

**Dr. Sandeep Bhavsar *** **Dr. Sonia Bhavsar ****

***Librarian**
Welingkar Institute,
Mumbai, Maharashtra,
India.

****Librarian**
MIM,
Ulhasnagar, Maharashtra,
India.

**QR Code**

**ABSTRACT**: - *Libraries have to decide to invest in various measures required to pre-empt / curb cyber crimes and how they perform their respective cost-benefit analysis of such investments. Computer crimes are growing because of the speedy evolution of technology and the laws, including changes, only follow technology. Protection measures such as hardware identification, access controls software and disconnecting critical libraries applications should be devised. It should be noted that technological apparatus do not commit crimes; people do. The perpetrators greatest advantage is the ignorance of the sentinels of the systems. While different countries are passing different legislations relating to computer crime, the awareness of the situation is still lost in our beauracry. In order to effectively tackle this problem, organizations need to make the public aware of the seriousness of the authorities to pre-empt cyber crimes.*

## 1. **Introduction**:

Cyber crime is a new term used in the ICT era. ICT is applicable in every sector of knowledge and service sector. Cyber-crime in plain words can be summarized as crime committed due to use of computers and technologies associated with it. Use of technologies are beneficial but its wrongful use in the society is a crime. There are different nature of cybercrimes like cyber stalking, cyber bullying, cyber warfare, frauds, hacking etc are creating social issues and harms to society in general as well as intellectual activities. Cybercrime halls in detecting theft, phishing, ransom wares, spam and fake messages, etc.

Presently, cybercrime is an ever increasing phenomenon, not only in India but all over the world. The incidence of cybercrime is directly proportional to the level of progress made by a country in computer technology. The report of the United Nations stated that more than 50 % of the websites in the USA, Canada and European countries have experienced breach of security and threats of cyber terrorism which threw a serious challenge before the law enforcement agencies.

Library and Information sector is not escaped from the cyberthefts and crimes. There are some issues in which cyber crimes are playing role like stealing data and information of others or from other sources, passwords, audio video books or literature, pirating literature, altering literature, hacking cites etc. The information and knowledge community as well as information users need the safe environment for information handling and for this purpose library professionals need to have literacy about the cybercrime. If library professionals are fully aware of cyber laws and crime detection measures they also develop literacy among the users and educate them.

## 2. Meaning and Definition of Cyber Crime:

Information Technology Act 2000, though not been statutorily defined any statute or law as yet. IT Act, 2000 does not contained the specific definition of cybercrime. But, cybercrimes is precisely said to be those species of crime in which computer is either an object or a subject of conduct constituting the crime or it may be even both. Thus, any activity that uses computer as an instrumentality, target or a means for perpetrating further crime, falls within the ambit of cybercrime. Prof. S.T. Viswanathan has given 3 possible definitions of cyber crimes and these are :

- Any illegal action in which a computer is the tool or object of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,
- Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,
- Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data.

## 3. Characteristics of Cyber Crime

Cyber crime is result of development and use of technologies and a new variety of crime called the cyber crime has emerged which is radically different from the traditional crimes. This crime has ill-effect of the development of Internet regime. Following are the main characteristics of cybercrime:

1. Low risk high rewarding ventures. The most striking feature of cybercrime is that they are relatively easy to commit, difficult to detect and even harder to prove. The cyber criminals with basic computer knowledge and skill can easily destroy valuable databases and causes huge loss to victims.

2. Lack of awareness among the victims. Many a times, the victim affected by cybercrime is unaware of its occurrence because lack of adequate skill and know-how in handling the computer system.

3. Physical presence is not required in such type of crimes. The cybercrime can be committed even from a far distant and any place without the necessity of its perpetrator's physical presence at the scene of crime.

4. Lack of hi-tech skills among investigating agencies. The detection of cybercrimes requires hi-tech skills, which the investigators generally lack.

5. Victims refrain from reporting cases to the police for the fear of adverse publicity or possibility of the loss of public trust in them.

6. No violence is involved. The cybercrime does not involve any violence, but is rather an outcome of greed, mischief and exploiting the weakness of the victim.

7. No territorial boundaries. The problem of cybercrime becomes more complex because Internet has no territorial boundaries, which enables the criminal to remain out of reach of law in most of the cases.

8. Anonymity and Openness. The computer network used for information dissemination has the feature of anonymity and openness which makes it easy and convenient for the criminal to indulge in crime without being identified or known to the computer user who is a victim of his illegal activity.

9. Paucity of authentic evidence. Since all information is exchanged over a network system in electronic data, no traces remains for once it is erased and the destruction of this sole evidence enables the criminal to remain undetected and escape criminal prosecutions.

10. Have wider ramifications. The range of cybercrime is wider enough to affect the socio-economic as also the legal rights of the people / society

## 4. Need for Cyber Law:

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws is a very technical field and that it does not have any bearing to most activities in Cyberspace. Cyber law is important because it touches almost all aspects of transactions and activities and on involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal angles. Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy.

## 5. Types of cyber laws:

The meaning of cyber crime may be any crime that is committed by means of special knowledge or expert use of computer technology; harmful acts committed from or against a computer or network; an unlawful act wherein the computer is either a tool or a target or both. Hence the types of cyber crimes, in the opinion of scholars are categorized as under:

- Software related crimes.
- Data related crimes.
- Physical crimes.
- Internet and other computer related crimes.

**5.1 Software Related Crimes:** In this type of the crimes are :

A. **Unauthorized Access:** Unauthorized access to computer systems or networks means any person who secures access or attempts to secure access to a protected system.

B. **Salami Attack**: This attack is used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

C. **Logic Bomb**: This is an event dependent program. This implies that this program is created to do something only when a certain event (known as a trigger event) occurs. Examples of some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

D. **VirusAVorm Attack**: Virus is a program that attach themselves to a computer or a file and then circulate it self to other files and to other computer on a network. They usually affect the data on a computer, either by alerting or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

E. **Trojan Attack**: A Trojan, is the program, which is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

F. **Intellectual Property Crime**: This includes software piracy, copyright infringement, trademarks, violations etc.

G. **Trap Door**: Malicious manipulations of security bypass logic used by system developers to save extra key strokes and enter specific programs.

H. **Time Bombs**: Logics inserted into programs to execute understand work when desired.

I. **Super Zapping**: A logic similar to trap door but more devastative wherein programs can be changed and malicious logics can be induced.

J. **Wire-Trapping**: The criminals insert unauthorized signals on a communication line or data channel either to jam the computer system or access desired data for authorized usage.

K. **Software Piracy**: Duplicating computer programs in violation of copyright laws.

**5.2 Data Related Crimes:**

A. **Data Diddling**: This kind of an attack involves alerting the raw data just before it is processed by a computer and then changing it back after the processing is completed.

B. **Data Leakage**: Copying the data on any magnetic or other media for fraudulent or illegal usage or blackmailing.

C. **Data Spying**: Access to big network installations using modems and telecom lines through legitimate password or breaking the password for selling it to a competitor or an enemy country for a price.

D. **Scavenging**: A method of obtaining and re-using information left in or around a computer system after processing. The method ranges from physical examining of 26 dustbins for discarded copies of computer listing to technical search for residual data.

### 5.3 Physical Crimes

A. **Theft**: Taking away the computer, its peripherals, data, software or accessories from the rightful ownership of someone else without the consent and knowledge of the owner.

B. **Breakage:** Sabotaging computer hardware like monitors, keyboards, pouring liquid, powder etc., over keyboard, electronics inserting pins to short circuit the system, cutting cables wires, blocking air flow, arson, bombing or other similar activities.

C. **Destroying Data, Output or Media**: Physically destroying master files by placing magnets near the media like tapes and floppies or scratching the media using a sharp object or physically bending it, misfile or erase active master files.

D. **Inter-Processing Manipulations**: Tampering with master files between normal processing cycles by getting possession of the new master file and altering one or more records for fraudulent purposes etc.

### 5.4 Internet and Other Computer Related Crimes:

A. **E-mail Bombing**: E-mail bombing refers to sending a large amount of e- mails to the victim resulting in the e-mail account (in case of an individual) or mail server (in case of a company or an e-mail service provider) crashing.

B. **Internet Time Theft**: This connotes the usage by an unauthorized person of the internet hours paid for by another person.

C. **Cyber Pornography**: Creating websites that cater nude pictures and literatures. This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the internet (to download and transmit pornographic pictures, photos, writings, etc.)

D**. E-mail Spoofing**: A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source.

E. **Cyber Stalking**: The oxford dictionary defines stalking as ‘pursuing stealthily'. Cyber stalking involves following a person's movements across the internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-room frequently by the victim, constantly bombarding the victim with e-mails etc.

F. **Password Attacks**: Attempts to obtain or identify a user account or password using different methods like Trojan horse, IP spoofing, packet sniffers etc.

G. **Brute-Force Attack**: A method of implementing a password attack using a program that runs across the network and logs into a shared resources such as a server.

H. **Main-in-the-middle**: Access to network packets through network packet sniffers, routing and transport protocols.

I. **Hacking:** Unauthorized access to programs, systems etc., with an intention to commit further offences. There are various kinds of hackers like Crackers, Code Hackers, Cyber punks, Phreakers etc.

J. **Blackmailing:** The old crime of blackmailing on the new medium of internet.

K**. Frauds**: Committing frauds through online investment newsletters, bulletin boards, e-mail online spasm etc.

These are generally observed cyber crimes and due to advancements new crimes are emerging.

### 6. Measures to Prevent Cybercrime :

**1. Strong Passwords**

It is absolutely essential to have passwords that cannot be easily guessed or captured by cyber criminals. Use different user ID / password combinations for different accounts and avoid writing them down. One way of making the passwords more complicated is by combining letters, numbers, special characters ( minimum 10 characters in total) and changing them on a regular basis. For instance, use S*&99#m@9991 as password.

**2. Securing computer**

Activate firewall. Firewalls are the first line of cyber defense; they block connections to unknown or fraudulent websites and prevent some types of viruses and hackers.

**3. Use anti-virus/malware software**.

Viruses can be prevented from infecting computers by installing and regularly updating a legal version of anti-virus software. In today’s world, no computer should be accessing the internet without anti-virus software protection.

**4. Block spyware attacks**

A part of anti-virus software is also blocks spywares, which could otherwise infiltrate device. This is essential because spyware can stay in computer system for a long time and pass on vital information from PC to remote sources.

**5. Be Savvy about social media**

With increased exposure to social media for every individual, it has become vital to make sure that social networking profiles (e.g. Facebook, Twitter,etc) are set to private. Check security settings, and be careful about the information post online. Be careful to operate under a gravatar or online alias when you are part of public forum or chat room conversation.

### 6. Secure Mobile Devices

Mobile phones today carry all manner of personal and secret information. Be aware that mobile phone is also vulnerable to viruses and hackers. Never leave your smartphone unattended. Take regular backups of mobile data. If possible, keep phone under lock and key when it is not likely to be in use for a long time.

### 7. Make sure that system is installed with latest operating system updates

Keep the applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates, as the companies always engaged in bringing the protection of system up to date against the latest viruses. Turn on automatic updates to prevent potential attacks on older software.

### 8. Programme to protect Data

One can use the benefits of technology to protect data. Use different encryption methods to encrypt most sensitive files such as Income tax returns or your investments, make regular backups of all important data, and see to it that store the information at another location as well.

### 9. Wireless network must be password protected

Due to increase terrorism worldwide, unsecured wi-fi networks may actually become enabling networks for those planning attacks. Such networks at home are vulnerable to intrusion if they are not properly secured with password keys. Review and modify default settings. Public wi-fi, “Hot Spots “ are susceptible to intrusive cyber criminals. Avoid conducting financial or corporate transactions on such networks.

### 10. Do not reveal your e-identity to unknown people

While Facebook and Linkedin have made everyone’s identity a matter or public knowledge, it is up to you to keep the settings your accounts private, and be cautious when giving out personal information such as your name, address, mobile number or financial information online. Make sure of the security of websites on which you are making online purchases and the privacy settings on your social networking site accounts.

### 11. Avoid opening links on files which could be scamming you

Opening links in mails from unknown sources can lead to vicious virus attacks. Always think before you click on a link or file from an unknown source. Don’t feel pressured by any emails. Check the source of the message and do verify the source if any doubt. Never reply to emails that ask you to verify your information or confirm your user ID or password.

### 12. Call the right authority for help

Cyber crime cells have now opened across India. There is thus no need to panic. If you find that you are a victim of illegal content on the net, or if you suspect an identity theft, computer crime or a commercial scam, approach the police. If you need help with maintenance or installation of a software firewall or anti-virus software on your computer, consult a certified computer technicial. Take care, and stay protected.

## 7. Cyber Crimes in Libraries:

To detect the threats and possible counter measures and control of cyber crime with adherence of cyber law is an essential instrument.

a. determination of type of computer crimes already experienced by some libraries

b. identify the factors contributing to the continued recurrence of such crimes and

c. evolve appropriate measures to control, curb and preferably pre-empt cyber crimes.

By using the internet to commit a crime

i. Electronic Banking
ii. Intellectual Property in as much as it applies to cyberspace
iii. Data protection and privacy
iv. Identity Theft, Hacking and Viruses.

Facilitation of Traditional Criminal Activity :

i. Stalking
ii. Stealing Information
iii. Child Pronography

Factors Contributing to Computer Crimes :

i. Lack of network control.
ii. Poor security culture in organization
iii. Lack of security technologies
iv. Inadequate HR for system handling
v. Inadequate staff training and education in security practice and procedures.
vi. Exploitation of insider knowledge or access.

Computer Crimes detected mostly in Libraries

i. Abuse of Internet access
ii. Unauthorized access to information by insider
iii. System penetration by outsider.
iv. Theft of laptop, computer hardware or devices.
v. Virus, worm or Trojan Infection.
vi. Web site defacement
vii. Theft or breach of confidential information.
viii. Hacking
ix. Information forgery and counterfeiting

Governance of Indian Cyber Laws :

i. Information Technology Act, 2000
ii. Information Technology (Amendment ) At, 2008
iii. Cyber Crime Investigation Cell.
iv. Communications Convergence Bill, 2001.
v. Cyber Security Forum-Joint Collaboration between India & U.S.
vi. E-Governance and E-Policy
vii. Punishments.

## 8. Measures and tips to avoid cyber crimes in information environment:

There are few measures which library and information professionals can manage and few of them are:

- Acquiring original information sources from the authorized publishers
- Block users to download information on the library computers
- Librarians have to check at regular intervals working of anti-virus software's and regular renewals of the software's
- Protect the servers from virus attack using firewalls
- Update the latest versions of the tools used for security maintenance
- Protection of passwords and modify them are regular intervals, and use of additional layer of security to password by verification code etc.
- Not to open the suspicious e-mails or open links which are unknown or unfamiliar, it might be leading to malware issues.
- Do not use public wi-fi for financial transactions or information handling, turn off sharing facilities while using public wi-fi. Use Virtual Private Network
- User education program sessions amy cover security of data and information handling in ICT usage

**References**:

- Aggarwal, R. (2013). Dispute Settlement for Cyber Crimes in India: An Analysis. Interdisciplinary Perspectives on Business Convergence, Computing, and Legality. doi:10.4018/978-1-4666-4209-6.ch015
- Cyber Crime Prevention.(n.d.). Retrieved October 28, 2018, from http://darjeelingpolice.org/Cyber_Crime_&_Prevention.pdf
- Cyber Crime. (n.d.). Retrieved October 05, 2018, from http://shodhganga.inflibnet.ac.in/bitstream/10603/7829/12/12_chapter 3.pdf
- Cyber stalking, Cyber Harassment and Cyber Bullying. (n.d.). Retrieved November 18, 2018, from https://astrealegal.com/telecommunication-cybercrime-crime/
- Hazra, A. (2015, November 08). MANAGEMENT OF TECHNOLOGY & INNOVATION_2. Retrieved November 3, 2018, from https://vdocuments.mx/documents/management-of-technology-innovation2.html
- Kidd, M and Rayme, M92013) Cybercrime!. Accessesd at https://www.slideshare.net/maryrayme/preventing-cybercrime-in-libraries.
- Leave, A. (2014, March 16). Top Ten Cyber Crime Prevention Tips. Retrieved November 14, 2018, from

http://scamoftheday.com/wordpress/2014/03/16/top-10-cyber-crime-prevention-tips/

- Shikarpur, D., & Bhagwat, V. (2015, January 31). 'Cybercrimes – Technology's Menace of the 21st century'. Retrieved March 03, 2016, from https://nrinews24x7.com/news_reg_cyber2015013105.html
- Shivhare, S. (2011, May 11). Cyber Crime And Its Implications. Retrieved October 20, 2018, from http://pioneerjournal.in/conferences/tech-knowledge/12th-national-conference/3621-cyber-crime-and-its-implications.html
- Siddique, M. (20177). Impact of Electronic crime in Indian Banking Sector – An Overview. International Journal of Business & Information Technology,1(2). Retrieved October 30, 2018, from www.ojs.excelingtech.co.uk
- Singh.Pramod Kumar; "Law on Cyber Crimes" (P.4-11, 14-16 & 40-63) Book Enclaves; New Delhi. (2007)