The role of libraries in preventing cybercrime

Koyel Sengupta
Librarian
Hiralal Mazumdar Memorial College for Women.

Library being a social institution has many social responsibilities to fulfill. Social evil like cybercrime is on the rise and library or library professionals must make it their duty to aware and educate library goers the worst side of cybercrimes and how to prevent them.

Introduction

We are living in an information society where Information and Communication Technology (ICT) is transforming every aspect of cultural, political and social life and which is based on the production and distribution of information. "It is characterized by the (1) pervasive influence of ICT on home, work, and recreational aspects of the individuals daily routine, (2) stratification into new classes those who are information-rich and those who are information-poor, (3) loosening of the nation state's hold on the lives of individuals and the rise of highly sophisticated criminals who can steal identities and vast sums of money through information related (cyber) crime" [(1)].

We need to be information literate to survive in this information society. Information literacy is the ability to understand when and why one need information, where to find it, and how to evaluate, use and communicate it in an ethical manner.

The easiest and fastest way to satisfy one's information need is Internet access. But everything has its own advantages and disadvantages. "The advantages of the Internet are all that people enjoy to access all kinds of information anytime from anywhere; transformation and expansion of trade and business, electronic governance, e-learning and education, research, entertainment, culture, etc. The disadvantages through Internet include hacking, email bombing, unauthorized access to email accounts, data altering, salami attacks (financial crimes), service attack (service blocked)/ trafficking, viruses / worm attacks, trojan attacks / unauthorized programme, fake emails internet time theft, web jacking, blackmailing, violation of privacy, indecent mailing/ dissemination of obscene material, pornography, improper downloading of copyrighted material etc" [(2)].

Internet usage has rapidly changed worldwide in the past few decades. Now-a-days people enjoy high speed mobile internet connection as a result of 4G technology that offers information at one's fingertips anywhere, anytime. The young people is more attracted and addicted to internet. Older people are vulnerable due to a lack of experience online.

What is cybercrime?

Cybercrime can be defined as any illegal activity in which computers or computer network are either a tool for committing crime or a target of crime. Usually the attacker is unkown and difficult to identify. On the other hand, the victims are large in number and easily vulnerable.

What are the most prevalent Cybercrimes?

- Cyberbullying
- Cyberwar
- Cyberstalking
- Cyber terrorism
- Extortion
- Fraud
- Hacking
- Identity theft
- Phishing
- Ransomware
- Spam
- Viruses
- Software piracy
- Computer vandalism
- Obscene or offensive content

Why should we know about Cybercrime?

The reason is simple – survival of the fittest. We are living in an Information Age where everyone uses internet to connect, to gain information and to succeed. Increased use of Watsapp, Facebook, Twitter, E-wallet, E-commerce sites, Net-banking and such other platforms have made modern day life simpler. At the same time, the threats associated with these platforms cannot be overlooked. It should be borne in mind, that there are criminal minded people who uses cyberspace to commit cybercrimes.

According to a draft report titled "*Comprehensive Study on Cybercrime*" (2013) by UNITED NATIONS OFFICE ON DRUGS AND CRIME[(3)], it has been observed that -

- In 2011, more than one third of the world's total population had access to the internet
- Over 60 per cent of all internet users are in developing countries, with 45 per cent of all internet users below the age of 25 years
- It is estimated that mobile broadband subscriptions will approach 70 per cent of the world's total population by 2017
- The number of networked devices (the 'internet of things') are estimated to outnumber people by six to one, transforming current conceptions of the internet
- In the future hyper-connected society, it is hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity

According to a report titled *"Internet in India – 2016"* jointly prepared by IAMAI (Internet and Mobile Association of India) & KANTAR IMRB[(4)] –

- As on December 2016, India had estimated 432 million Internet users.
- It is estimated that by 2017, Internet Users in India are most likely to be in a range of 450-465 million.
- Availability and affordability of smart phones has changed the choice of device and place of access of internet in Urban India, and there is no denying that smart phones have driven internet adoption in rural India to a large extend.

● Internet is perceived predominantly as a requirement for the youth in both rural and urban India, with activities like social networking, entertainment etc being the main purpose for using internet.

● Urban India is fast adopting e-commerce, digital payments, online ticketing/cab booking, etc that makes internet and integral part of daily life.

What should be the role of Libraries to combat cybercrime?

A library not only provides internet access but also subscribes e-resources in large number. Users of the university and college libraries are hugely benefitted from the e-resources subscribed by them. Wi-Fi zone inside a library are an attractive target for cybercriminals trying to steal personal information such as passwords and banking details. Libraries are the sensitive place where user may face cyber attacks or might commit Internet crimes. Hence, libraries can play an important role in spreading awareness among library members about cybercrime and how to report it.

"One of the most important weapons we have to combat cybercrime is not only a computer literate public, but also a cyber literate public. So training courses available at libraries offer a valuable service in educating internet users on how stay safe online, how to engage in the digital economy and how to report an incident when it occurs" [(5)].

Libraries must come forward to provide user education in relation with secure access to online information. User education programme must recommend:

● Users to use strong password and never share passwords with strangers. Password would be such that could not be easily guessed by hackers. A combination of letters, numbers and symbols are considered as strong password.

● Be careful about posting information or pictures in social media as these are easy targets of cybercriminals. A person must be careful and selective while uploading personal information or pictures on social networking sites as these can no longer be controlled by the concerned user after posting as status.

- Use secure websites for conducting online transactions. Secure websites refer to those websites whose URL starts with "https" and not "http". It means the site is secured and information will be safe as it passes from one's browser to the website's server.
- Do not click on unknown links as these may contain malware. Unknown links are usually associated with virus threats and clicking them can infect one's computer with virus.
- Do not open emails sent from unknown sources. Email from unknown sources might contain links to harmful and questionable websites. Such mails should be immediately deleted.
- Cautiously use public Wi-Fi networks. Public Wi-Fi networks are available at airports, railway stations, busy crossroads, hotels, educational institutes, cafes and so on. This is the most insecure place of all as personal data can be easily stolen here.
- Uninstall unnecessary software. Removing unwanted software not only helps to get a faster computer but also get rids off irritating pop-ups on computer screen.
- Learn more about internet privacy. Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences.(6)

The library staff also has certain responsibilities to perform to provide the users a safe and secure information environment. These are (7):

- Conduct periodical anti-virus scan. Conducting anti-virus scan at regular intervals gives a virus free working environment. It provides protection from online threats.
- Use firewalls. A firewall is a boundary or a wall to keep intruders from attacking the network. The firewall is network device that is in between a private network and the internet. When a private network is connected to the internet it allows the people to access information from external sources. It also allows external users to enter the private network and steal information from the network. Firewall protects from this unauthorized access.(8)
- Block users from downloading program into public computers. Users might knowingly or unknowingly download software that might invite online threats. Users must be informed and convinced not to do the same.

- The library staff themselves must be aware about cybercrime and how to prevent it. Being updated will not only safe the library staff from not falling to be a victim of cyber crime but also helping the library users in this regard.

Conclusion

Cyber crime is emerging as a serious threat. The governments, police departments and intelligence units have started to adopt strict measures to prevent this crime. Cyber cells have been established. Cyber laws have been formed. Information pertaining to sources of cyber crime and prevention of cyber attacks are being shared with the public by and large, who spent most of the time over the Internet. However, the only way to prevent one from being a victim is to pay attention, be smart, be safe and keep oneself updated.

REFERENCES

1. http://www.businessdictionary.com/definition/information-society.html
2. Kumar, V. D. (2013). Cyber crime prevention and role of libraries. *International Journal of Information Dissemination and Technology*, 3(3), 222-224.
3. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/ CYBERCRIME_STUDY _210213.pdf
4. http://bestmediainfo.com/wp-content/uploads/2017/03/Internet-in-India-2016.pdf
5. https://www.alia.org.au/ideas-campaigns-and-events-your-library/help-stamp-out-cybercrime-acorn
6. https://www.techopedia.com/definition/24954/internet-privacy
7. https://www.slideshare.net/maryrayme/preventing-cybercrime-in-libraries
8. https://www.ukessays.com/essays/computer-science/advantages-and-disadvantages-of-firewalls-computer-science-essay.php