DLINE JOURNALS

Information Security Education Journal (ISEJ)

Print ISSN: 2349-8161
Online ISSN: 2349-817X
ISEJ 2025:12 (1)
https://doi.org/10.6025/isej/2025/12/1/1-9

Best Practices for Cyber Security in Academic Libraries

Ms. Pooja
DLIS/MIT Central Library
Manipal Academy of Higher Education
Manipal – 576 104, Karnataka. India
pooja.mit@manipal.edu

Rekha D Pai*
MIT Central Library
Manipal Academy of Higher Education
Manipal- 576 104, Karnataka. India
rekha.pai@manipal.edu

ABSTRACT

Information and Communication Technology (ICT) has helped libraries make all their electronic resources accessible to their users. Securing library-subscribed resources from scammers or unauthorised users is a big challenge in the present era. Cyber security is an area that needs to be studied in the present scenario, and the library is no exception. Institutions, including libraries, are one of the targeted areas of ransom ware attacks. Library computers, library patrons' data, and library subscribed resources are the target of cybercriminals. To overcome this, there is a need for cyber security in academic libraries. Manipal Academy of Higher Education (MAHE) has implemented IT policies to secure computer systems, networks, information, and digital assets and control cybercrimes in its various institutions. Librarian plays a significant role in protecting library resources be having cyber security.

Keywords: Academic Libraries, Cybercrimes, Cyber Security, Best Practices for CyberSecurity, MAHE Policies, Librarian Role in CyberSecurity

Received: 18 November 2024, Revised 9 January 2025, Accepted 29 January 2025

1. Introduction

The library is a knowledge hub that includes many resources in print and electronic form. Access to electronic resources became very easy with the advent of Information Technology (IT)/Information Communication

Technology (ICT).Many advantages, like easy access, easy dissemination of information anywhere at any time, saving physical space and time, etc., have made library users more comfortable with e-resources. However, the library or librarian does not have any control over access to e-resources both in the library and off-campus. Securing library-subscribed resources from scammers or unauthorised users is a big challenge in the present era. Cyber security is an area that needs to be studied in the present scenario, and the library is no exception. This paper explains about some of the cybercrimes, cyber security and the best practices to be followed to overcome cybercrime.

2. Literature Review

The world is highly interconnected now with the adoption of new technologies and the internet. The library is also becoming one of the adopters of technology and the internet. Thus, cyber security in libraries has become essential and is a serious issue. Every day, new cyber tools and threats are coming up, and there are many challenges to secure information resources. Finding new platforms to face new threats and actions for cyber security is now common among academic libraries (Ajie, 2019). There is no perfect or permanent solution for cybercrime. However, more and more effort can be put into minimizing cybercrime. Creating a safe and secure cyberspace for the future is important in academic libraries. Establishing an institutional policy, monitoring information security, securing library networks by enforcing property rights laws, increasing awareness about information security, making privacy rights of individual library users, and attending and conducting awareness programmes in the institution or the library for cyber security are the day's needs.

A safe and secure environment is required to access library resources. Library professionals should have literacy about cybercrimes, cyber security measures and cyber law to educate library users. Cybercrime involves low-risk risk, high-res, rewarding ventures, a lack of awareness among the victims, a lack of skills to detect cybercrimes, no territorial boundaries and many more.To control or prevent cybercrime, creating or implementing cyber laws is necessary. Libraries need to implement software-related crime law, data-related crime law, physical crime law, internet and other computer-related crime laws (Bhavsar & Bhavsar, 2017). Acquiring original information from publishers, blocking the downloading of unnecessary information from unauthorised sites, updating the latest version of computer applications, avoiding the opening of suspicious e-mails, and many other measures help control or prevent cybercrime in academic libraries.

Due to the growth and implementation of Information Technologies (IT) handling of library resources has changed from traditional to machine-based systems (computers). Most of the libraries of the 21st century are digital libraries (Anderson, 2003). Securing digital library resources is quite different from traditional libraries. Security awareness of library resources is very important. Security awareness includes four factors: human behaviours, education on information security, knowledge about the use of technologies, and information policy (Fakeh et al., 2012). Education through seminars, awareness programs, training and workshops on cyber awareness helps to avoid cybercrimes in institutions. Knowledge about better use of IT tools in the library can increase information security in the library.

Organisational, physical, and technological security are very important in the present scenario. For information security use of technology, policies and awareness activities are required which helps to run the library smoothly (Singh & Margam, 2018).

Identification, authentication, authorisation, integrity, confidentiality or secrecy, no repudiation and availability are the basic safety requirements (Lima et al., 2016). Librarians should be prepared to manage library resources securely by maintaining computers, monitoring the functioning of e-resources accesses, etc. Constructing and implementing security policies is a big challenge for academic libraries. Institutional support is needed for the successful implementation of the security policy.

3. Cybercrime

Digital devices can be used in library for giving library services, promoting library resources, developing library services. At the same time, digital devices can be used for criminal activities using the internet. Mainly, cybercrime involves identity theft, technology fraud, computer viruses, data breaches, scams, etc. Generally, cybercrime has 5 types:

- Hacking
- Malware
- Identity Theft
- Social Engineering
- Software Piracy

4. CyberCrime in Academic Libraries

Health, finance, military, social media, public institutions, and many others are the most common sectors targeted by cybercrime. Institutions, including libraries, are one of the targeted areas of ransomware attacks. In this attack, cybercriminals target library computers, library patron personal data, and library subscribed resources.

The following cybercrime can affect library users and library resources in academic libraries

4.1 Stealing of Library Subscribed Resources

The library is investing huge amounts in subscriptions to e-books, e-journals, and e-databases. It also invests large amounts of budget in research support services like anti-plagiarism software, Grammar checking software, Remote access software, Discovery services, and many others. Hence, cybercrimes like stealing passwords, audio video books, literature of subscribed resources, hacking sites, piracy of library resources, etc., must be avoided.

4.2 Misuse of Library Subscribed Resources

Most of the libraries used to provide usernames and passwords to access e-resources from its subscribed platforms. Since many library users misused that system, now the libraries have implemented remote access software. E-mail addresses provided by the organization are enabled to access electronic resources. Sharing e-mail IDs and passwords with friends and family to access library e-resources who are not part of the institutions and sending downloaded articles to others is now at risk for users.

4.3 Social Media Frauds

The library has started using social media platforms to give current awareness services, and new arrivals

notifications, update its users about library activities, promote library services and many more. This platform allows cybercriminals to share and receive information from library users. Social engineering attacks may increase by using social media. Displaying students' contact details or personal information leads to phishing attacks, credential theft, data theft, and other crimes. Sharing of links to library resources or articles is a loss for the library.

4.4 Software Crimes

Digital library usage can be done with the help of software. The library subscribes to many software to provide adequate services to its users. Unauthorised access, Virus attacks, Intellectual property crime, Software piracy, Wire-trapping and many other crimes come under software crimes. Librarians should be aware and trained to protect library software from such crimes.

4.5 Data Crimes

Data is an essential part of the digital library. In digital libraries, user information and content of library resources are considered as data. Data diddling, data leakage, data spying, and scavenging are some of the most important data crimes.

4.6 Physical Crimes

To access the digital content of the digital library, computers, the internet, smart devices, and many physical equipment are necessary. Almost all libraries in the country have separate computer labs or information centres that help users access e-resources from the library. Theft of physical library resources, breaking of library equipment, and destroying data manually by deleting the contents become physical crimes. Monitoring users' activity in the library is very important to overcome this crime.

4.7 Internet and Computer Crimes

The Internet has become part of our life. Everywork is dependent on the Internet. Digital libraries are meaningless without the Internet and computers. E-mail bombing, e-mail spoofing, internet time theft, password attacks, hacking, fraud, and many others come under internet and computer crimes. Using some security software helps to overcome the effects of these types of crimes.

5. Cyber Security

Cyber security means protecting individuals, institutions or organizations from cyber-attacks or cybercriminals. It mainly defends internet-connected devices and services from various cybercrimes. Cyber security's role is to protect networks, devices, and data from cyber criminals and unauthorized access. Cyber security is needed to protect data from criminals.

6. Importance of Cyber Security

- To protect personal data from criminals.
- To preserve the reputation of government or private organizations.
- To increase the betterment of data management in organizations.

- To maintain trust and credibility among organizations.

- To provide streamlined access to the data.

- To educate or train people to get secure from cybercrime.

7. Cyber Security in Academic Libraries

The following are some of the commonly used cyber security

7.1 Network Security Network security secures library networks from unauthorised access, misuse, and modification of academic library computer networks. Firewall, E-mail security, Remote access security, Data loss prevention, etc., are a few types of network security aspects of the library.

7.2 Application Security Application security is the process of developing, adding, and testing security features in an application. The library subscribes to many applications to access e-resources. Securing applications from unauthorised users is very important for academic libraries.

7.3 Information Security This security in libraries involves library resources security, policy security, computer security, Internet security, cloud security, database security, and many others.

7.4 Hardware Security Hardware security involves protecting hardware systems like computers, CD-ROMs, network cables, and many others. Digital libraries mainly run on computers and their components. Protecting them from criminals is very important.

7.5 Software Security A digital library has a bundle of software collections. Virus attacks, malware attacks, and corruption of library software are basic software crimes in an academic library. Securing software from cyber criminals through other software or communication with other systems over networks is helpful to over come this.

7.6 Data Security A library is a collection of data, including library user data, library resources data, library hardware or software data, and many others. Data security safeguards library data from corruption, theft, or unauthorised access.

8. Academic Library Challenges in Cyber Security

Academic libraries face many challenges in protecting library resources from cyber crimes. Some are listed below

8.1 Lack of Awareness The primary challenge is the lack of awareness among users and library staff members about cybercrime. This leads to a big problem: the loss of library resources.

8.2 Insufficient Infrastructure To avoid or control cyber crimes in the academic library, cyber security tools/infrastructure, such as software and technologies, are needed.

8.3 Lack of Training about Cyber crimes To safeguard library resources from cyber criminals, training about cyber crimes and cyber security measures is needed.

8.4 No Library Policies Academic libraries need to have library policies regarding cyber-crimes and cyber security. These policies help prevent cyber-attacks or cyber-crimes by giving clear instructions or guidelines to library users and library staff members.

9. Best Practices for Cyber Security in Academic Libraries

To overcome cybercrimes, libraries need to take some precautions or measures. Some of the best practices for cyber security in academic libraries are:

- Subscribing original data from authorised publishers.

- Keep an eye on systematic download or sharing of library information.

- Creating strong passwords can avoid most of the e-mail crimes, unauthorised access, and fraud cases. The Password should include a combination of special characters, capital letters, small letters, and numbers instead of the date of birth or name.

- Avoiding phishing emails from unknown persons/unknown sites.

- Usage of anti-virus software/updating software regularly to prevent software attacks. Librarians should monitor library software frequently.

- Avoiding illegal software installation in the library computer systems.

- Blocking unwanted websites, non-educational internet sites, and some social media sites and avoiding unauthorised links helps not to become the victims of cybercrime.

- Avoiding the use of public Wi-Fi and securing mobile devices.

- Installing and updating the latest version of operating systems in the library.

- Protecting wireless networks by using strong passwords in the library.

- Regularly monitor library-subscribed software and maintain usage reports of e-resources.

- Strictly prohibit sharing library and library user personal data with anyone.

10. Information Technology Policies Adopted in Manipal Academy of Higher Education (MAHE)

MAHE implemented IT policies to secure computer systems, networks, information and digital assets. The MAHE IT policies help faculty, staff, students, and others who are working across all MAHE institutions understand the policies and understand the effect of violating the formed policies. The Digital and IT Department of MAHE maintains all the policies. MAHE IT policies are mainly divided into three types are:

10.1 Acceptable Usage Policy This policy applies to all IT assets and services MAHE provides. The guidelines given by this policy include proper care and maintenance of assets, access to removable media like flash drives, storage cards, and many others, and not sharing users' accounts and passwords for systems or services. The policy covers a clear desk and screen policy, guidelines for workstation usage, printer usage, internet usage, e-mail usage, mobile devices, physical document protection, and Office 365.

10.2 Information Security Policy Malware Information Sharing Platform (MISP) provides management direction for information security and some security controls need to be adopted to maintain and manage the information security in MAHE by establishing an information security program including policy documents, by supporting procedures, risk management frameworks, by establishing documents with detailed instructions about information and information assets, by monitoring reviewing, reporting and investigating document violations and many aspects are included to secure information in this policy. In this policy, there is a provision for review from time to time, and it can change and add to the existing rules depending on the existing environment.

10.3 Communications Security Policy This policy provides some general guidelines about MAHE networks and their components. It also explains in detail the remote access policy, wireless guidelines, firewall policy, network security, instant and social messaging, and clock synchronization.

MAHE policies give users an idea of some do's and don'ts, which helps secure University data from threats. Rules can be added, updated, modified, and deleted in all policies as per the requirements.

11. Librarian's Role in Cyber Security

Librarians play a major role as managers who manage the entire library, which includes resources management, service management, enquiries management, and many others, with the help of other team members. Librarians can play several roles in academic libraries' cyber security. Some are listed below:

11.1 Librarian as an Educator/Trainer The Librarian is called the teacher of teachers. He/she can educate the library user in many ways. The Librarian of an academic library can educate his/her library users, such as students, faculty, and research scholars, about library e-resources, library policies, library services, and the do's and don'ts of the library. In controlling cybercrime, the librarian should educate the users by conducting awareness programs for the users.

11.2 Librarian as Policy Developer Policy provides detailed information. Librarians can develop cybercrime or cyber security policies to avoid cybercrimes in the academic library. A set of guidelines helps library users minimise cybercrime.

11.3 Librarian as Learner Learning is a lifelong process. Librarians should explore new technologies, new updates about the software, cybercrimes and security measures which help them to control cybercrimes in the library.

12. Conclusion

The Internet has its own advantages and drawbacks. The development in technology has led a few people to

become cybercriminals. Higher educational institutions such as engineering college libraries, medical college libraries, university libraries, etc., are investing huge amounts of money in e-resources. The institution needs to take some measures to protect its subscribed resources with the support of a library/librarian. Making institutional level policies, giving awareness about cybercrimes and cyber security, and organizing certificate courses for the students and staff of the institution can help to control cybercrimes. Librarians should be flexible in learning new technology and should be aware of the latest trends in the cyber world. Then only library resources can be saved from cybercrime.

References

[1] Ajie, I. (2019). A review of trends and issues of cybersecurity in academic libraries. *Library Philosophy and Practice*, 2019.

[2] Singh, V., Margam, M. (2018). Information security measures of libraries of central universities of Delhi: A study. *DESIDOC Journal of Library and Information Technology*, *38*(2), 102–109. https://doi.org/10.14429/djlit.38.2.11879

[3] Anderson, J. M. (2003). Why we need a new definition of information security. *Computer & Security*. *IEEE Security & Privacy*, *1*(2), 72–76.

[4] Lima, J. S., Rafaela, A., Araújo, S. De, Edvander, F., Santos, P. (2016). Information Security in Academic Libraries: the Role of the Librarian in Planning and Introducing New Institutional Policies, 389–419.

[5] Singh, B. P., Kumar, A., Kumar, A. (2017). Internet Security and its Best Practices in Educational Libraries. *January*, 267–274.

[6] Ngwum, N., Raina, S., Aguon, S., Taylor, B., Kaza, S. (2020). A Model for Security Evaluation of Digital Libraries. *Journal of The Colloquium for Information Systems Security Education*, *7*(1), 1–12. https://cisse.info/journal/index.php/cisse/article/view/115

[7] Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 1–27. https://doi.org/10.3390/s23167273

[8] Aregbesola, A., Nwaolise, E. L. (2023). Securing Digital Collections: Cyber Security Best Practices for Academic Libraries in Developing Countries. 1–12. https://digitalcommons.unl.edu/libphilprac

[9] Mishra, A., Alzoubi, Y. I., Gill, A. Q., Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2), 1–35. https://doi.org/10.3390/s22020538

[10] Ramsay, J., Renaud, K. (2012). Using insights from email users to inform organisational email management policy. *Behav. Inf. Technol.*, *31*, 587–603.

[11] Zissis, D., Lekkas, D. (2012). Addressing cloud computing security issues. *Future Gener. Comput. Syst.*, *28*, 583–592.

[12] Tsesis, A. (2019). Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure. *Univ. Colo. Law Rev.*, *90*, 593–629.

[13] Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *J. Comput. Commun.*, *9*, 80–102.

[14] Saha, R. (2024). Data Privacy and Cyber Security in Digital Library Perspective: Safe Guarding Data Privacy and Cyber Security in Digital Library Perspective: Safe Guarding User Information. *International Journal of Scientific Research in Engineering and Management (IJSREM)*, *8*(4), 1–6. https://doi.org/10.55041/IJSREM30761

[15] MAHE IT policies. Retrieved from https://www.manipal.edu/mu/policies/it-policy.html