


# Chapter 1

## Introduction to Cyber Security

**Sudeep Jadey**

 <https://orcid.org/0000-0001-7427-4555>  
NIE Institute of Technology, India


**Girish S. C.**

NIE Institute of Technology, India


**Raghavendra K.**

NIE Institute of Technology, India

**Prasanna Kumar G.**

 <https://orcid.org/0000-0002-8962-8034>  
NIE Institute of Technology, India

**Srinidhi H. R.**

 <https://orcid.org/0000-0002-8727-253X>  
NIE Institute of Technology, India

**Anilkumar K. M.**

JSS Science and Technology University, India

### ABSTRACT

*The rapid growth of the internet and the technological revolution in the information and communication sectors has created a gateway for users to connect online. With digital information being stored, security and privacy has been a major concern around the world to protect vital data. The modern tools and techniques used by cybercriminals perform malicious activities which aim at disrupting, distorting, and stealing sensitive data for self-financial gains. More complexities were added to the cyber world with the emergence of AI and ML algorithms in the smart phones. Cybercriminals take advantage of this barrier and build their network to commit cybercrimes across the globe. This chapter focuses on an audience that includes researchers, professionals, academicians and UG, PG students who are interested to know more about cybersecurity. This chapter aims to provide a brief overview of cybersecurity, cyber laws, cyber-attacks and security tools, objectives of cybersecurity, applications of cybersecurity, and so on. Finally, the future of cybersecurity along with some case studies are discussed.*

DOI: 10.4018/978-1-6684-3991-3.ch001

## INTRODUCTION TO CYBER SECURITY

The Internet has become one of the most important useful source of information for cyber users. The expansion of cyberspace in the digital world has created numerous opportunities and challenges for cyber users to exchange information across the globe. The advent of computers and communication technologies has open the doors for malicious users to weaken security systems of the society. Today, computing devices like laptops, tablets, and smart phones has become a crime instrument for malicious users. Every computing devices is connected to the networks which can access and transmit the data anywhere, making it more vulnerable to cyber-attacks. More complexities were added to the cyber world with the emergence of Artificial Intelligence & machine learning algorithms. Further, Computers with wireless networking creates space for free malicious access. With digital information being stored, security & privacy has been a major concern around the world to protect vital data. The sophisticated modern tools and techniques used by cybercriminals to perform malicious activities aims at disrupting, distorting & stealing sensitive data for self-financial gains. Cybercriminals take advantage of this barrier & build their network to commit cybercrimes across the globe. These cybercriminals create barriers to innovations, financial, economic growth and free flow of information. Thus there is a need to secure these system. The main goal of cyber security is to protect valuable assets. These assets could be hardware, software, network and data (Priyadarshini, I. 2019).

Imagine that you are travelling in a bus having a smart phone with Bluetooth enabled unknowingly in it. A nondescript guy who is sitting away few distance in the same bus might be fiddling with his android phone which syncs with your device through Bluetooth & load the malware into it. All your phone contacts will get an offensive messages which were not sent by you but are from your phone. This is one classic example of security breach through smart devices.

Today, new opportunities are open up for wireless network devices which can be hacked. The airports, restaurants & hotels, libraries, coffee shops & other public places are the prime target sites for cybercriminals to hack assets through wireless networks. Even though these sites are password protected, still it is dangerous because there is slight control who has gained the password. On a wireless network, anyone can listen in on anyone else on the network. A victim in a public place has got no clue who is nearby with respect to wireless network (Waschke, M. 2017, Herrmann, D., & Pridöhl, H. 2020). So let's take a brief overview about cybersecurity

### What is Cybersecurity?

Cybersecurity may be defined as the ability to protect and recuperate from cyberattacks. According to NIST (National Institute of Standards & Technology), it can be defined as the ability to defend cyberspace usage from cyberattacks. Cyberspace could be internet, computer systems, telecom networks, embedded controllers etc. The security of any organization completely relies on three key areas namely confidentiality, availability and integrity.

1. **Confidentiality:** The word confidentiality looks alike privacy. The key idea is to prevent unauthorized users from accessing the sensitive information. Confidentiality makes sure that only authorized users are given permission to access sensitive information. Identity theft, credit card fraud, phishing, wiretapping are some examples of confidentiality attacks

22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/introduction-to-cyber-security/306856](http://www.igi-global.com/chapter/introduction-to-cyber-security/306856)

## Related Content

---

### Unsupervised Keyword Extraction Methods Based on a Word Graph Network

Hongbin Wang, Jingzhen Ye, Zhengtao Yu, Jian Wang and Cunli Mao (2020). *International Journal of Ambient Computing and Intelligence* (pp. 68-79).

[www.irma-international.org/article/unsupervised-keyword-extraction-methods-based-on-a-word-graph-network/250851](http://www.irma-international.org/article/unsupervised-keyword-extraction-methods-based-on-a-word-graph-network/250851)

### Optimization Techniques in Cooperative and Distributed MAC Protocols: A Survey

Radha Subramanyam, S. Rekha, P. Nagabushanam and Sai Krishna Kondoju (2024). *International Journal of Intelligent Information Technologies* (pp. 1-23).

[www.irma-international.org/article/optimization-techniques-in-cooperative-and-distributed-mac-protocols/335523](http://www.irma-international.org/article/optimization-techniques-in-cooperative-and-distributed-mac-protocols/335523)

### Improving Privacy and Security of User Data in Location Based Services

Mohammad Yamin and Adnan Ahmed Abi Sen (2018). *International Journal of Ambient Computing and Intelligence* (pp. 19-42).

[www.irma-international.org/article/improving-privacy-and-security-of-user-data-in-location-based-services/190631](http://www.irma-international.org/article/improving-privacy-and-security-of-user-data-in-location-based-services/190631)

### AI-Powered Language Translation for Multilingual Classrooms

Muhammad Usman Tariq (2024). *Integrating Generative AI in Education to Achieve Sustainable Development Goals* (pp. 29-46).

[www.irma-international.org/chapter/ai-powered-language-translation-for-multilingual-classrooms/348795](http://www.irma-international.org/chapter/ai-powered-language-translation-for-multilingual-classrooms/348795)

### Semiotic Evaluation of Product Ontologies

Joerg Leukeland Vijayan Sugumaran (2011). *Intelligent, Adaptive and Reasoning Technologies: New Developments and Applications* (pp. 64-79).

[www.irma-international.org/chapter/semiotic-evaluation-product-ontologies/54425](http://www.irma-international.org/chapter/semiotic-evaluation-product-ontologies/54425)