Chapter 14
Information Security Awareness Among Postgraduate Students: A Study of Mangalore University

Dayanandappa Kori
Mangalore University, India

Renuka Naik
Mangalore University, India

ABSTRACT

Information security prevents unauthorized access to using, disclosing, altering, inspecting, recording, or destroying information. Information security programs are designed to achieve three main goals: confidentiality, integrity, and availability of information. The study highlights awareness and perceptions of information security among postgraduate students. To make everyone aware of the opportunities and difficulties that exist in today's threat landscape, modify risk behaviour, and develop or strengthen a secure corporate culture, information security awareness training is required to be effective. This paper aims to assess information security awareness among Postgraduates of Mangalore University. A survey was conducted, and appropriate tools and technologies were used to collect and interpret the data. Based on the results, suggestions for information security among postgraduate students were made.

INTRODUCTION

In today's world, the Internet is considered a necessary part of our daily lives, and the number of people who use it is increasing at an alarming rate. As information and communication technology has advanced and the proliferation of low-cost and simple-to-use devices, more data has been produced, and more information has been used. Information security is required to protect confidential information. Information Security (IS)-related events continue to occur even though security logs have been established. Because of this, it is critical to increasing students' understanding of ethical and unethical perceptions of information technology in today's society, particularly in the classroom. Information security refers

DOI: 10.4018/978-1-6684-4755-0.ch014

to keeping information secret to prevent it from being used or read by someone with malicious intent and extorting information from sources without authorization. Traditionally, the difficulty that arises from the inability to transfer data to those who have received formal education has been viewed as the opposite. They safeguard the community's interests and the fundamental amenities that society requires and possesses in such areas. When a society expands, the exchange of information becomes increasingly necessary. Information security was initially intended to protect only written and oral communication, but it became necessary to keep the general public away from readily available information as time went on. As a result, information was kept confidential to protect the community from harm.

INFORMATION SECURITY

Over the past few years, technological advancements in information technology (IT) have heightened concerns about the risks to data that can result from a lack of IT security. These dangers include, among other things, being exposed to viruses and malware as well as attacks on network systems and services. Furthermore, insufficient IT security can jeopardize data confidentiality, integrity, and availability by allowing unauthorized access to sensitive information, leading to severe consequences. For this reason, it is critical to ensure that personal information about individuals is protected and secured at all times in a secure environment. When discussing processes and methods that have been established and implemented to protect confidential information from being altered, disrupted, or destroyed and from being subjected to an investigation, it is customary to bring up the subject of information security. It contains information, particularly electronic data that can be used or consulted without the owner's permission. Therefore, it is a type of intellectual property. Even though it is solely concerned with the processes used to protect data, information security is an essential component of cyber security. In information security, the term refers to a subset of cyber security, a more important concept. Information security is at the heart of all our activities regarding information technology security. Protecting the confidentiality, integrity, and availability of information is important to ensure information is not compromised when critical concerns arise. It is not only natural disasters that are a cause for concern, but also computer/server failures and similar problems. As a result, there has been significant growth and development in information security. People, Software, and services interact in a complex environment known as cyberspace. This is made possible by the widespread availability of information and communication technology (ICT) devices and networks worldwide. As a result of India's rapid growth in the information technology sector, ambitious plans for rapid social change and inclusive growth, as well as the country's prominent position in the global information technology market, it ensures that proper attention is paid to creating a secure computing environment and confidence in electronic transactions, Software, services, devices, and networks have emerged as one of the country's most compelling priorities. This kind of concentration makes it possible to develop an excellent cyber security ecosystem in the country that is compatible with the globally connected environment. However, the cyberspace environment is prone to various intentional or unintentional disasters, artificial or natural. Therefore, as cyber-attacks increase in volume and sophistication, there is a greater need to protect personal information, sensitive corporate information, national security, and critical infrastructure. Because of the plethora of devices available today, it is now impossible to imagine a time when you did not have access to relevant information. However, information access security has surpassed the accessibility of information itself. The first thing we do is check our phones from the moment we wake up. Then, we connect to the internet,