Education and Society
(शिक्षण आणि समाज)

Special Issue
UGC CARE Listed Journal
ISSN 2278-6864

Education and Society

Since 1977

The Quarterly dedicated to Education through Social Development and Social Development through Education

May 2023

(Special Issue-1/ Volume- II)

INDIAN INSTITUTE OF EDUCATION

128/2, J. P. Naik Path, Kothrud, Pune - 411 038

Content.....

1. Analytical Study of Moonlighting 011
Omkar Suryakant Waghmare and Dr. Sarang Shankar Bhola

2. Information & Technology Laws &Cyber Security in India: Challenges and Solutions 018
Prashant Prabhakar Jarandikar and Sanjeev Kumar Ganpati Sable

3. The Role of Social Media Marketing in the Tourism Industry 021
Soujanya Sachin Nagannawar

4. Evaluation of Performance of Mutual Fund Schemes: A Case Study of LIC Asset Management Company 025
Dr. Mrs. Manisha Vikas Jagtap

5. Compensatory Justice for Rape Victims through the Manodhairya Scheme: Overview 033
Dr. Pooja Prashant Narwadkar

6. Use of Artificial Intelligence in the professional Field of Law in India 039
Dr. Savita R. Rasam

7. Study of Mental Health, Locus of Control and Hopelessness 045
Dr. Vinayak Madhukar Honmore and Miss. Aliya Ismail Nadaf

8. A Study of the SWOT Analysis of Potential Tourist Destinations In Nandurbar District, Maharashtra 052
Mr. Raju Zavrao Yashod

9. Financial Problems: A Study on Brick Making Industries 061
Mr. Rohit Baban Basnaik and Dr. Anil G. Suryawanshi

Information & Technology Laws &Cyber Security In India: Challenges and Solutions

Prashant Prabhakar Jarandikar
Asst.Prop.in Law,
Bharati Vidyapeeth's New Law College, Sangli
Co-Author-Sanjeev Kumar Ganpati Sable
Asst.Prop.in Law,
Bharati Vidyapeeth's New Law College, Sangli

Abstract:

India has emerged as a significant player in the digital economy, with a rapidly growing technology sector and a large population of internet users. However, with the rise of the digital era, the country has also become a prime target for cyber-attacks. This research paper examines the state of cybersecurity in India, exploring the various challenges and opportunities to improve the country's cybersecurity posture. The paper also looks at the current regulatory framework for cybersecurity and recommends strategies for individuals, organizations, and the government to enhance cybersecurity in India.

Introduction:

India has undergone a digital transformation over the past decade, with the proliferation of smartphones, e-commerce, and online transactions. The country has one of the world's largest populations of internet users, and its technology sector is growing at a rapid pace. However, with this growth comes the risk of cyber-attacks, which can cause significant damage to individuals, organizations, and the country's economy. In this research paper, we will examine the state of cybersecurity in India, exploring the challenges and opportunities to enhance cybersecurity and protect critical infrastructure.

Objectives of The Study:

1. To study the meaning, Position of the terms — Cyber Space & Cyber Security.
2. To find out the challenges of the Cyber Security in India & suggest the remedies.

Methodology:

The Present study is Doctrinal Research. The secondary data has been used for the work. The sources for the collection of data are various books, case laws, articles from the journals, newspapers and Internet.

Cyber Laws in India:

Current State of Cybersecurity in India: India has confronted several high-profile cyber-attacks, including the 2016 breach of the Indian banking system, which give rise to in the theft of millions of dollars. The country has also been a victim of state-spon[illegible] cyber-attacks. The reports suggest that China and Pakistan are among the main actors. Despite these challenges, India has taken steps to advance cybersecurity, including the establishment of the **National Cyber Security Policy in 2013** and the

creation of the Indian Computer Emergency Response Team (CERT-In).

What do you mean by Cyber Law?

Internet laws and regulation are collectively referred to as "cyber laws" in this context. Cyber laws cover anything that has to do with, is connected to, or results from legal matters or any citizen activity **in cyberspace.**

The sector of the legal system that is related to legal informatics and that controls the electronic exchange of information, e-commerce, software, and information security is known as cyber law. It is also known as Internet law or cyber law. It is associated to legal informatics and electronic components like computers, software, hardware, and information systems. It shelters a wide range of themes, including online privacy and freedom of expression, as well as access to and use of the Internet, which includes numerous subtopics.

Definition of Cyber Security -Sec.2(1) Information & Technology Act, 2000: -

"Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Cyber Laws in India:

In the advancement of society and globalisation India has also framed laws against cybercrime. By different cyber laws the Indian Citizens as will as persons residing in Inda are prevented from sharing private information with strangers online. One of the major cyber laws in India is **The Information and Technology Act 2000.** The Act was passed and revised in 2008 to cover many types of offenses under Indian cyber law. It has been in effect since the establishment of cyber laws in India.

Legal issues relating to the usage of network information technology and devices' distributive, transactional, and communicative features are covered by cyber law. it covers all of the laws, regulations, and constitutional clauses that apply to networks and computers. The Act defines the various types of cybercrime and the penalties associated with them.

Challenges to Cybersecurity in India:

India faces several challenges to enhancing cybersecurity, including a lack of awareness among the general public, inadequate infrastructure, and a shortage of skilled cybersecurity professionals. The country's regulatory framework for cybersecurity is also fragmented, with multiple agencies responsible for different aspects of cybersecurity. This fragmentation has resulted in a lack of coordination and information-sharing, making it challenging to address cybersecurity threats effectively.

Major Cyber Attacks in India:

1. Union Bank of India Heist 2016

Through a phishing email sent to an employee, hackers accessed the credentials to execute a fund transfer, swindling Union Bank of India of $171 million, Prompt action helped the bank recover almost the entire money.

2. Wannacry Ransomware May 2017

The global ransomware attack took its toll in India with several thousand computers getting locked down by ransom-seeking hackers. The attack also impacted systems belonging to the Andhra Pradesh police and state utilities of West Bengal.

A. **Ransomware Data Theft at Zomato May 2017**

The food tech company discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an 'ethical' hacker-who demanded the company must acknowledge its security vulnerabilities-and put up for sale on the Dark Web.

B. Petya Ransomware: June-2017

The ransomware attack made its impact felt across the world, including India, where container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port Trust got affected.

Opportunities to Enhance Cybersecurity in India:

India has several opportunities to improve its cybersecurity posture, including the promotion of cybersecurity awareness among the general public, the development of a comprehensive regulatory framework, and the establishment of partnerships between the government and private sector. The country can also force its growing technology sector to develop innovative cybersecurity solutions and create a skilled workforce of cybersecurity professionals.

Recommendations for Improving Cybersecurity in India:

To enhance cybersecurity in India, stakeholders must take proactive steps to address the challenges and leverage the opportunities. Some recommendations include:

1. Promoting cybersecurity awareness among the general public through campaigns and education programs.
2. Developing a comprehensive regulatory framework for cybersecurity that promotes information-sharing and coordination among agencies.
3. Establishing partnerships between the government and private sector to enhance cybersecurity in critical infrastructure.
4. Investing in infrastructure to support the growth of the technology sector, including the development of data centers and cybersecurity research centers.
5. Developing a skilled workforce of cybersecurity professionals through training programs and incentives.

Conclusion:

India has made significant progress in enhancing its cybersecurity attitude, but there is still much work to be done. The country faces several challenges, including a lack of awareness, inadequate infrastructure, and a fragmented regulatory framework. However, India also has several opportunities to improve cybersecurity, including promoting cybersecurity awareness, developing a comprehensive regulatory framework, and leveraging its growing technology sector. By taking proactive steps to address the challenges and leverage the opportunities, India can enhance its cybersecurity posture and protect its critical infrastructure and economy from cyber-attacks.