



**An International Multidisciplinary  
Quarterly Research Journal**

Peer Reviewed Referred  
and UGC Listed Journal

Volume - VII, Issue - III, July - September - 2018  
ISSN 2277 - 5730

**AJANTA**

Impact Factor - 5.5 ([www.sjifactor.com](http://www.sjifactor.com))

Is Hereby Awarding This Certificate To

**Asst. Prof. Laxmi Podoli**

As a Recognition of the Publication of the Paper Entitled

**CYBER SPACE: STUDY OF ASSOCIATED RISKS AND  
PRECAUTIONS TO BE UNDERTAKEN**

**Ajanta Prakashan**

Jaisingpura, Near University Gate,  
Aurangabad. (M.S.) 431 004

Mob. No. 9579260877, 9822620877

Tel. No.: (0240) 2400877,

[ajanta1977@gmail.com](mailto:ajanta1977@gmail.com), [www.ajantaprakashan.com](http://www.ajantaprakashan.com)

**Certified as  
TRUE COPY**

**Principal  
Ramviranjai Jhunjhunwala College,  
Ghatkopar (W), Mumbai-400086.**

**Editor: Vinay S. Hatole**

A11 - Laxmi - 2018-19

Peer Reviewed Refereed and  
UGC Listed Journal  
(Journal No. 40776)



ISSN 2277 - 5730  
AN INTERNATIONAL MULTIDISCIPLINARY  
QUARTERLY RESEARCH JOURNAL

# AJANTA

Volume - VII, Issue - III  
July - September - 2018

IMPACT FACTOR / INDEXING  
2018 - 5.5  
[www.sjifactor.com](http://www.sjifactor.com)

**Ajanta Prakashan**


Certified as  
**TRUE COPY**

Principal  
Ramviranjan Jhunjhunwala College,  
Ghatkopar (W), Mumbai-400086.


**CONTENTS**


Sr. No.	Title and Author's Name	Page No.
10	Managing ESG Risk through Regulatory BRR Compliance: A Case of Listed Banks in India CADr. Varsha Ainapure and Vaibhavi Dalvi	68-76
11	Credit Risk Management in Banking Sector in India Poonam Popat	77-85
12	Risk Management in Agricultural Commodity Market Rishita K. Doshi and Krupali A. Vasoya	86-91
13	Psychological Factors in Risk Management of Investments Kavita Shah	92-101
14	Risks of Banking Sector in Indian Economy: A Case Study of State Bank of India and Emerging Paradigm Shift in Risk Management Chintan Vora	102-107
15	Cyber Space: Study of Associated Risks and Precautions to be undertaken Laxmi Podoli	108-113
16	Emotional Connection: A Comparative Study on understanding Banking behaviour of Working and Non-Working Women Kinjal Shethia	114-120
17	A Study on Retail Investors Education with Respect to Stock Market Risk Prasad Dabre	121-127

**Certified as  
TRUE COPY**

  
**Principal**  
 Ramniranjan Jhunjhunwala College,  
 Ghatkopar (W), Mumbai-400086.

## 15. CYBER SPACE: STUDY OF ASSOCIATED RISKS AND PRECAUTIONS TO BE UNDERTAKEN

Asst. Prof. Laxmi Podoli

Ramniranjan Jhunjhunwala College, Mumbai.

### Abstract

Technology is the new driven source in the world and people are evolving with this advancement in technology. With the advancement of technology the risk and crimes throughout the world is increasing due to the use of technology. India is not an exception to the computer generated menace. As per the press release issued by National Crime Records Bureau (NCRB) on 30th November 2017, the number of cyber-crimes has increased from 11,592 cases in 2015 to 12,317 cases in 2016. Uttar Pradesh was ranked first with registration of highest number of cyber crimes that are committed with 2,639 cases in 2016 followed by 2,380 cases registered in Maharashtra. According to the CERT-In, 27,482 cases of cybercrime were reported from January to June 2017. However, as a measure to prevent and control internet crimes, the Parliament enacted the Information Technology Act, 2000 which came into force on October 17, 2000. This paper aims to highlight the provisions of cyber- criminal laws in India relating to cybercrimes and the vulnerability of the cybercrime in present era. This paper also aims at discussing the various precautions that can be undertaken to minimisecyber crime.

**Keywords:** Computer generated menace, CERT-In, cyberspace, encryption, and Cyber- crime.

### Introduction

Intellectual creation and man goes hand in hand. Man always strives to excel in the world as a result tremendous achievement has been made. He is always motivated to keep the pace with existing technologies. One of the most significant inventions of man is internet. However with rapid development in internet technology it has given both advantage and disadvantage to the mankind. This problem is not confined to India only as countries throughout the world are victims of Cyber-crimes and are working to find out the solution for the same as these crimes are invisible crimes as face behind this crimes are very difficult to identify. There is no specific act related to cyber-crime but the laws, rules and penalties for different crimes that are committed in cyberspace are stated under the various provisions of Information Technology Act, 2000.

**Certified as  
TRUE COPY**



**Principal**

**Ramniranjan Jhunjhunwala College,  
Ghatkopar (W), Mumbai-400086**

## Review of Literature

1. Nappinai (2010) in his article "Cyber Crime Law in India: Has Law Kept Pace with Engineering Trends-An Empirical Study" states that data protection provision provided in Information Technology Act 2000 and in Amendment Act 2008 is inadequate and does not meet the industry requirement in today's scenario. According to the researcher crimes like data theft; illegally accessing / removal of data; virus attacks etc., could not be prosecuted due to the lack of relevant penal provisions.

2. Kandpal, & Singh (2013) in their article "Latest Face of Cybercrime and Its Prevention in India" the researchers explains the trends in cyber-crimes and comparison with other Asian countries. The researcher provides certain best practices for prevention of cyber-crimes. The researchers also provide information about the various cybercrime cells operating in India.

## Objectives of the study

1. To study the risk associated while dealing in Cyber Space in today's world.
2. To study the various prevention measures to combat cyber crimes.

## Cyber Space

Cyber space is not defined anywhere and it is not restricted to geographical boundaries. It includes everything that relates to computers, internet, software, etc. The Cyber Space is borderless and actions in cyber space are mostly anonymous. Cyberspace has complete **disrespect for jurisdictional boundaries**. Cyber Law is the law governing cyber space. For instance a person residing in one country can manipulate the accounts of any person or bank and transfer or hack the account. All he would need is a laptop computer and a cell phone.

Today's world all are within the ambit of cyberspace and almost all transactions are confined within the cyber world and with our current Prime Minister Shri. Narendra Modi, "Digital India" initiative all those things which were handled manually have come under the purveyance of cyberspace.

For example:

- Dematerialisation of shares is compulsory
- Electronic Data is extensively used by almost all companies
- Income tax filing, GST filling is also done electronically.
- Consumers prefer net-banking, debit cards and credit cards or electronic wallets over cash transactions.

**Certified as  
TRUE COPY**



**Principal**  
**Ramniranjan Jhunjhunwala College,**  
**Ghatkopar (W), Mumbai-400086.**

- Traditional communication method has been replaced by email, mobile phones, video conferencing, etc.
- People prefer online shopping over offline shopping i.e. visiting shops.
- E-contracts which got due recognition in Companies Amendment Act, 2013 are replacing conventional contracts.
- Even government tenders and quotations are placed only electronically.

As today's world is exposed to cyber space 24/7 the exposure to cyber crimes is also 24/7. Some of the crimes that are at increase in India are:

Cyber pornography	Sale of illegal article	Email spoofing
Intellectual Property Crimes	Online Gambling	Cyber Defamation
Salami Attacks	Logic bombs	Cyber stalking
Access to computer systems or networks without permission	Theft of information contained in electronic form	Physically damaging a computer system
Forgery	Email Bombing	Data Diddling

**Cyber Law**

Cyber space is governed by Cyber Law. The Information Technology Act, 2000 is the first cyber law which was passed in India. This act has jurisdiction throughout the country. There is no specific act on cyber crimes yet in India as people in many cases are not even aware about the cyber crimes. Moreover there is a huge gap between the advancement in technology (in terms of crime) while law has its own procedures (in terms of settlement) which are very slow.

**Practices That Can Be Followed by Individual to Reduce Cyber-Crime**

Some practices which are listed below gives an answer to the reasons how and why cyber crimes are committed because we don't follow the precautions while dealing in cyberspace. If we as individual becomes little cautious by following certain practices the cyber crimes against us can be avoided to a greater extent.

**Computer updation at regular interval**

One of the best way to prevent cyber-attacks is to keep a check on operating systems and to keep it updating whenever the software demands. Updated software is difficult to hack and automatically they blocks unnecessary options.

**Certified as TRUE COPY**



**Principal  
 Ramniranjan Jhunjhunwala College,  
 Ghatkopar (W), Mumbai-400086.**

### Selecting correct passwords

The key to your access to your online accounts or computer is your password. Select a password that has different combination of alpha-numeric characters along with special characters like !@#%^&\*.

Its better not to use passwords that can be easily guessed like mobile number, date of birth, personal name, etc. Don't give access to your passwords to your friends or colleagues. Keep changing password in minimum 3 months.

### Security software

Install security software from trusted sources. Security software acts as a protector for the computer from various viruses, spams, Trojan horses, etc. Don't fall into a trap of free security software; try to install paid security software which is more genuine.

### Protect your personal identity

For most of the services, users will have to provide personal information in order to handle billing and shipping of purchased goods, if important then only provide. Ignore email messages that ask for personal details. Genuine companies generally don't send spam emails and neither asks for personal details. Don't follow the link provided in email or in any message directly. It is always advisable to type or copy the URL directly on the website.

### Keep a tab on your banking transactions at regular intervals

Keep a regular check on your banking transactions. Be careful while using net banking or mobile banking. Don't keep your birthdates or mobile number as your password. Don't keep your details open. Remember to sign out or logout from your personal laptop as well after your transactions.

### Be cautious with your mobile phones

People generally use mobile phone with least care and with the ever increasing trap of social media, specially girls are more prone to cyber crimes. Don't carry your cell phone to the bathroom. Make sure that phone camera is not on in changing room.

### Socio savvy

Studies shows that most of time people fall prey to cybercrimes because of their extensive use and information sharing on social media. Make sure that your personal details are secured and keep a tab on people who access your portfolio very often. Be careful with information that you share and be more vigilant.

**Certified as  
TRUE COPY**



**Principal**

### **Don't hesitate to take help**

If any cyber-crime is committed and you comes to know about it don't wait for the next crime to happen report immediately about the same with the police station. Don't try to be expert if you are not an expert consult a technician for computer related issues.

### **How to File a Cyber Crime Complaint**

The Information Technology Act of India clearly states that when a cyber-crime is committed a complaint can be filed at any cyber cell as cyber-crime has global jurisdiction. There are two ways of filling a cyber-crime complaint.

#### **A] Offline Method (Visiting a Cyber Cell or a nearby police station)**

Step 1- A person has to submit an application to the Head of Cyber Crime Investigation Cell about the offence that has been committed.

Step 2- Along-with application documents and information regarding the crime has to be submitted.

#### **B] Online Method**

Step 1- Visit website: [www.cybercrimecomplaints.com](http://www.cybercrimecomplaints.com) or [www.cybercrime.gov.in](http://www.cybercrime.gov.in)

Step 2 – Register by providing your email id and user id of your choice. For [cybercrime.gov.in](http://cybercrime.gov.in), complain can be filled anonymously.

Step 3- User id and password will be sent to the registered email and complaint can be filled by filling the required information

**OR**

An email can be sent to the cyber cell in your area.

Documents to be submitted while registering a complaint:

In case of vulgar emails or abusive emails soft and hard copy of the offending e-mail/ image/ text, source of origin (if possible), email address of the offending sender etc.

In case of hacking- server logs, soft copy and hard copy of compromised data, suspects, impact of the hacking etc.

### **Conclusions**

Cybercrimes are increasing day by day due to less conviction as general people lacks awareness regarding computer crimes. Most of the times people even do not know that they have become a victim to the illegal activities of perpetrators of cybercrime.

**Certified as  
TRUE COPY**

**Principal**

**Ramuiranjan Jhunjhunwala College,  
Ghatkopar (W), Mumbai-400086.**



As a result, most of the crime remain unreported, and a few which are reported, result in acquittal due to ignorance of the police and investigating officials about the technicalities of these crimes and lack of sufficient evidence against the accused. Most of cyber-crimes are bailable acts which provide ample scope for the offenders to delete or destroy the evidences.


Introduction of several provisions in the IT Act by the IT (Amendment) Act, 2008, relating to data protection, are extremely essential in today's business environment.

The government has also created task force to combat cyber crime which includes: 1) Indian Computer Emergency Response Team (CERT-In) - functional organisation of MeitY, which provides guidelines for securing Indian cyber space, 2) Cyber Swachhata Kendra- This centre provides detection of malicious programs and free tools to remove the same for common users 3) Cyber Surakshit Bharat Programme – aims at training Chief Information Security Officer (CISO) and other Information Technology Officers of Central govt., State govt., Banks, PSU etc. to address Cyber security challenges.

### Bibliography

- <http://ncrb.gov.in>
- <https://cybercrime.gov.in/cybercitizen/home.htm>
- <http://meity.gov.in/cyber-surakshit-bharat-programme>
- <https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms> retrieved on 28th July 2018.
- Bhatt, S. C., & Pant, D. (2011). Cyber-crime in India. International Journal of Advanced Research in Computer Science, 2(5).
- Nappinai, N. S. (2010). Cyber Crime Law in India: Has Law Kept Pace with Engineering Trends-An Empirical Study. J. Int'l Com. L. & Tech., 5, 22.
- Kandpal, V., & Singh, R. K. (2013). Latest Face of Cybercrime and Its Prevention in India. International Journal of Basic and Applied Sciences, 2(4), 150-156.

**Certified as  
TRUE COPY**

  
**Principal**  
Ramniranjan Jhunjhunwala College,  
Ghatkopar (W), Mumbai-400086.