IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X, p-ISSN: 2319-7668
PP 55-62
www.iosrjournals.org

Cyber Crime: Technological Blight in Digital Banking in India.

Mrs. Vinaya Chaturvedi
Bhavans Vivekananda College, Sainikpuri,chaturvinaya@gmail.com

Abstract: *Internet-banking facilitates various financial institutions, customers of the banks, individuals, businessmen to access their accounts or obtain information on different financial products and services through internet. Technology has created its influence right from corporate governance and state administration, also to small shops which we see in our surroundings. With the popularity of usage of computer in cyber world one can witness expansion the growth of technology which made the term* ***'Cyber'*** *more familiar to the people.*

The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyze etc. Computerization in the billing system has made computers and other electronic devices inseparable in all aspects of the human life as a result common man cannot spend a single day without using computer ,laptops , smart phones or a mobile.

As one can witness increase in the use of technology, electronic banking also emerged in Indian Banking system. Due to increase in the number of persons using internet, misuse of technology in the cyberspace also started which gave initiation to cyber crimes at the domestic as well as in international level .

Keywords : *Cyber crimes ,Computerization, Data Protection, technology*

I. Introduction

In developing economies, cybercrime has increased rapidly due to high usage of the internet and the digitization of economic activities. Need of strict statutory laws to regulate the criminal activities in the cyber world was needed which should also aim to protect technological advancement system as the misuse of technology was increasing at a very high rate. To control these fraudulent practices Indian parliament made "**INFORMATION TECHNOLOGY ACT, 2000**" on 17th Oct 2000 which deals with the laws in the field e-commerce, e-governance, e-banking as well as fines and punishments to be imposed with to control cybercrimes. **Cyber Crime** may be stated as "unlawful acts wherein the computer is either a tool used to perform the crime or it becomes a target of crime or sometimes both."

Cyber Crime is neither defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008. Under the Indian Penal Code, 1860 and a few other legislations meaning of crime or offence has been elaborated which is not done in this act. Hence, to define cybercrime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber crime'.

Certain Acts of Information Technology Act -2000 and the I.T. Amendment Act 2008 were enforced with reference to banking and financial sector transactions. During mid of 90's India saw an improvement in globalization and computerization, growth of computerized governance and growth in E commerce was witnessed during this period .Until then, most of international trade and transactions were done through documents being transmitted through post only. Documentary evidences & records, were mainly paper evidences and paper records or other forms of hard-copies only. As international trade was mostly being done through electronic communication and emails, an urgent need for maintaining and storing electronic records was realized.

II. Need of study

Digital banking is playing unique role in strengthening the banking sector and improving service quality in commercial banks .Majority of commercial banks are also adopting electronic banking services to attract their customers. Although there is a rise in electronic channels of banking in commercial banks but customers still have fear towards their safe n secure electronic banking operations.

This paper tries to present the meaning and definition of cyber crime in the legislation in India which deals with violations relating to the use of or is concerned with the abuse of computers or other electronic gadgets'. This paper attempts to create awareness with respect to various cyber crimes and cyber laws related to banking operations. It also tries to provide an insight towards awareness of cyber laws with reference to banking operations in India.

III. Objectives of study

1. To study the preferences of customers towards internet and digital banking.
2. To ascertain various reasons for not opting digital banking in India.
3. To understand various cyber crimes with respect to digital banking operations.

IV. Review Of Literature

1. - B. Ram Chandra Reddy (2007) in his book "Consumer Awareness towards E-banking" has given an insight about the level of awareness of people towards electronic banking.
2. B. Rama Chandra Reddy 2008 in his book "Emerging challenges in E-banking" by in his book has given an insight towards challenges and problems which are associated with emerging trends in e-banking.
3. CN Reddy 2010 in Electronic & Internet Banking frauds gave the basic idea about the electronic and internet banking adopted by banks presently and about various frauds related to banking.
4. Kamini Dashora, (2011) Cyber Crime in the society: Problems and Preventions, 2011,vol-3,pg 243-244
5. Ajeet Singh Poonia, (2014) has given an insight to understand classification of cybercrime its challengesin International journal of Emerging Trends and Technology in Computer Science (Volume 3,issue 6, Nov- Dec 2014,pg 120)
6.
7. Digpal Singh, H Rathore and Karn Marwah(2014) Cyber Crime in Banking Sector .International journal of law mantra. www.lawmantra.co.in.
8. Cyber Security for financial services: Strategies that empower your business Drive Innovation and Build Customer Trust, Symantec White Paper,2015-P-07

Scope of study: The purpose of this study is to examine awareness amongst individuals for making use of internet banking. It also attempts to analyze reasons for customers not preferring electronic banking. It further tries to understand various cyber crimes and various cyber legislations made in India with reference to cyber crimes related to internet and digital banking.

Research methodology: Primary data collection through a structured questionnaire consisting of closed ended questions has been done for accomplishment of objectives.. Pilot survey was also done before final survey. Likert scale for checking awareness and level of agreement amongst customers is taken in to consideration. Reliability tests were conducted for checking of genuineness of data. Factor analysis, one- way, two-way ANOVA tests were also conducted. in order to understand variance. Secondary data is collected from various websites, e-journals, news papers, national and international journals etc.

V. Analysis And Interpretation

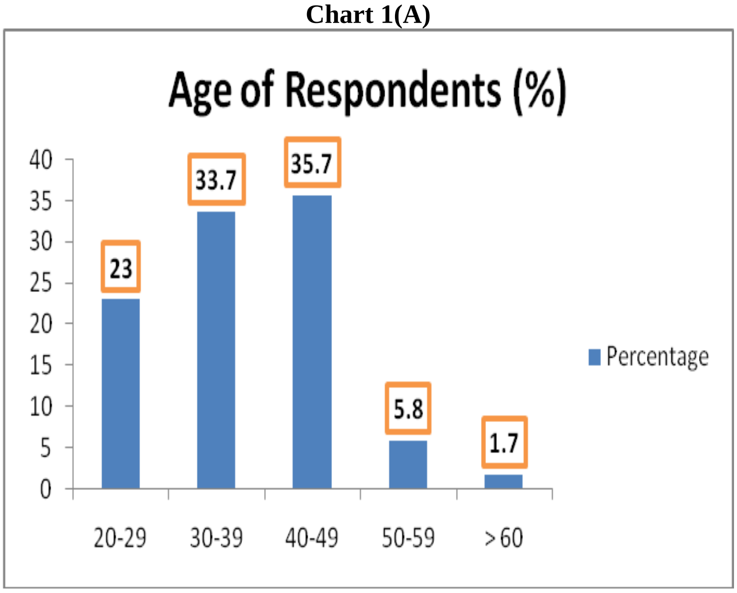
1. To study the preferences of customers towards internet and digital banking.

Primary data collection on individual revealed that married people used more of banking transactions. Study reveals that people of age group of nearly 30-49 years use electronic banking which constitutes of nearly 69.4%of that target population. It also indicated that people of age group 50 years and more consisted of only 7.5% who preferred such internet banking options.

Table 1(a): Age of respondents

Class Interval	Frequency	Percentage
20-29	67	23
30-39	98	33.7
40-49	104	35.7
50-59	17	5.8
> 60	5	1.7
Total	291	100

Chart 1(A)



Further, on the basis of occupation it was analyzed that percentage of retired people and housewives were very less who opted digital services .They were more comfortable with traditional banking culture.

Table 1(b): occupation of respondents

		Frequency	Percent
	student	34	11.7
	employee	151	51.9
	business	38	13.1
	profession	44	15.1
	retired	8	2.7
	housewife	16	5.5
	Total	**291**	**100.0**

Chart 1(B): occupation of respondents

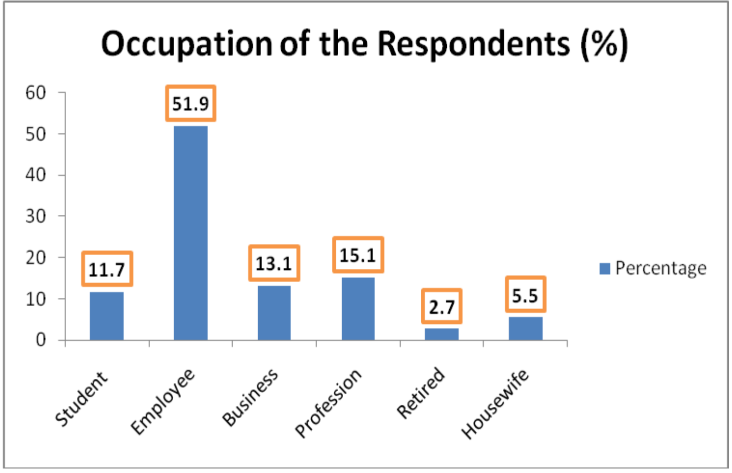
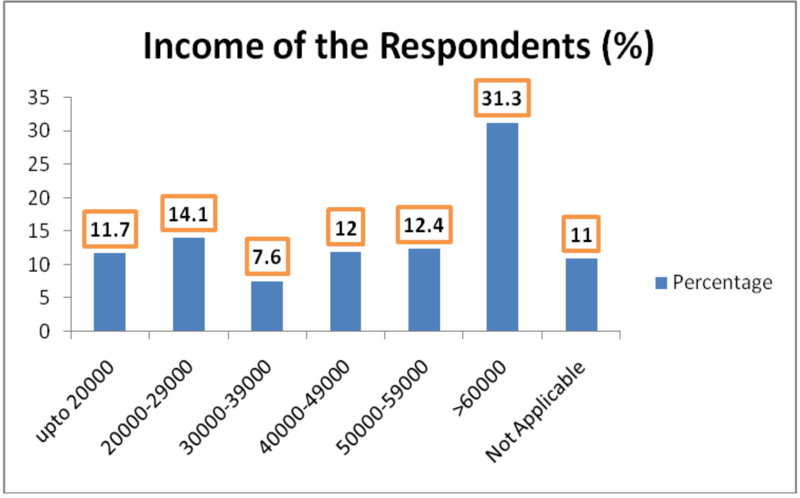


Table 1(c): Monthly income of respondents

Class Interval	**Frequency**	**Percentage**
upto 20000	34	11.7
20000-29000	41	14.1
30000-39000	22	7.6
40000-49000	35	12
50000-59000	36	12.4
>60000	91	31.3
Not Applicable	32	11

Total	**291**	**100**

Chart 1(c): Monthly income of respondents



2.To Ascertain Various Reasons For Not Opting Digital Banking In India.

According to the study conducted the on the respondents revealed that due to lack of awareness of various electronic banking services offered by banks, problems to understand language and problem in understanding and accessing websites, server related issues, security threats and lack of awareness of laws on digital banking for benefit of the customers people are not fully satisfied with the technological advancement in banking area.

Table2(a): Reliability Statistics :

Scale: All Variables

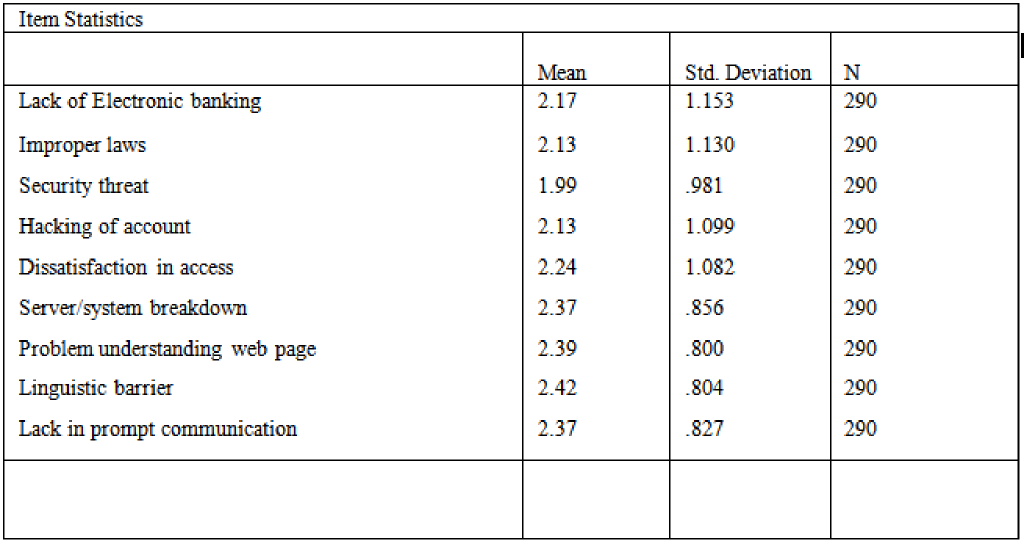
Case Processing Summary

		N	%
Cases	Valid	290	100.0
	Exclud Eda	0	.0
	Total	290	100.0

Reliability Statistics

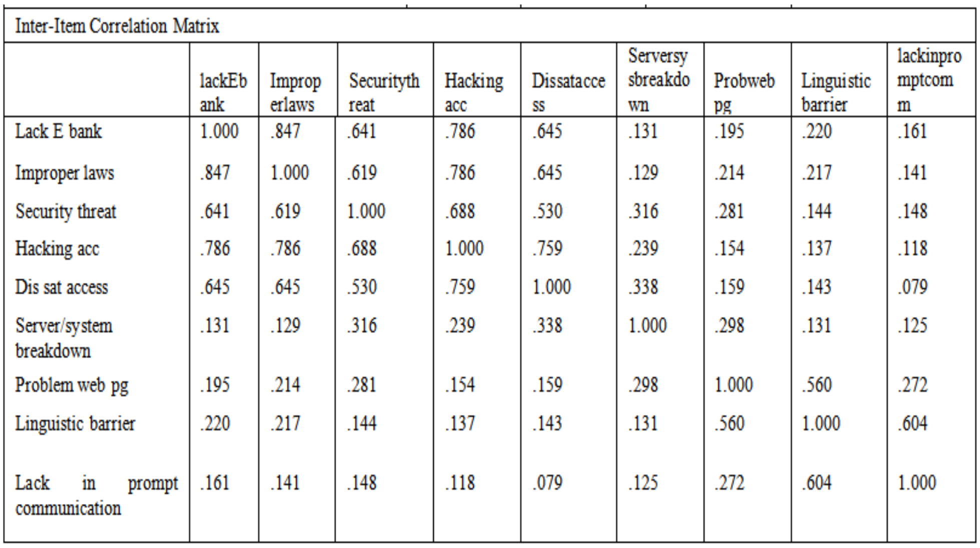
Cronbach's Alpha	Cronbach's Alpha Based On Standardized Items	N Of Items
.842	.829	9

Cronbach's Alpha Is 0.842, Which Indicates A High Level Of Internal Consistency For 0ur Scale With This Specific Sample.



Item Statistics

	Mean	Std. Deviation	N
Lack of Electronic banking	2.17	1.153	290
Improper laws	2.13	1.130	290
Security threat	1.99	.981	290
Hacking of account	2.13	1.099	290
Dissatisfaction in access	2.24	1.082	290
Server/system breakdown	2.37	.856	290
Problem understanding web page	2.39	.800	290
Linguistic barrier	2.42	.804	290
Lack in prompt communication	2.37	.827	290



Inter-Item Correlation Matrix

	lackEbank	Improperlaws	Securitythreat	Hacking acc	Dissataccess	Serversysbreakdown	Probwebpg	Linguistic barrier	lackinpromptcomm
Lack E bank	1.000	.847	.641	.786	.645	.131	.195	.220	.161
Improper laws	.847	1.000	.619	.786	.645	.129	.214	.217	.141
Security threat	.641	.619	1.000	.688	.530	.316	.281	.144	.148
Hacking acc	.786	.786	.688	1.000	.759	.239	.154	.137	.118
Dis sat access	.645	.645	.530	.759	1.000	.338	.159	.143	.079
Server/system breakdown	.131	.129	.316	.239	.338	1.000	.298	.131	.125
Problem web pg	.195	.214	.281	.154	.159	.298	1.000	.560	.272
Linguistic barrier	.220	.217	.144	.137	.143	.131	.560	1.000	.604
Lack in prompt communication	.161	.141	.148	.118	.079	.125	.272	.604	1.000

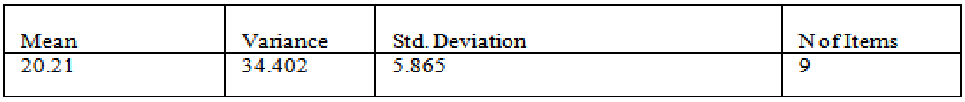
This column presents the value that Cronbach's alpha would be if that particular item was deleted from the scale. We can see that removal of any question would result in a little higher Cronbach's alpha. Therefore, we would not want to remove these questions.

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Max/ Min	Variance	Nof Items
Item Means	2.246	1.993	2.421	.428	1.215	.022	9
Item Variances	.961	.641	1.329	.688	2.074	.084	9

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Lack Ebank	18.04	24.486	.753	.767	.801
Improperl aws	18.08	24.724	.748	.762	.802
Security threat	18.22	26.572	.679	.554	.812
Hacking acc	18.08	24.786	.768	.778	.800
Dissat access	17.97	25.819	.674	.619	.812
Serversysbreakdown	17.84	30.791	.303	.249	.849
Probwebpg	17.82	30.537	.364	.407	.843
Linguisticbarrier	17.79	30.533	.363	.554	.843
lackinpromptcomm	17.84	31.214	.271	.386	.851



Mean	Variance	Std. Deviation	N of Items
20.21	34.402	5.865	9

2. **To Understand Various Cyber Crimes With Respect To Digital Banking Operations.**

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes various cyber crimes related to electronic/internet/digital banking.

1. Cracking: It is one of the most alarming cyber crimes . In this case offender can damage inside our computer systems without our knowledge and permission and can make unauthorized alterations in precious confidential data and information.

2. E-Mail Spoofing: A spoofed e-mail is the one which misrepresents its origin. It shows different origin not from where actually it has originated.

3. SMS Spoofing: Spoofing is a blocking through spam ("spam" means the unwanted and uninvited messages). In this case offender steals identity of another person in the form of mobile phone number and sends SMS via internet and receiver gets the SMS from the mobile phone number of the victim. SMS spoofing is a serious cyber crime against any person.

4. Carding: It means making false ATM cards (i.e. Debit and Credit cards)which are used by criminals for their monetary benefits for the purpose of withdrawing money from the victim's bank account without his knowledge and faith. More of the unauthorized use of ATM cards is seen this type of cyber crimes.

5. Cheating & Fraud: Person who tries to steal password and data storage does it with a negative mind which leads to fraud and cheating.

6. Assault by Threat: This category refers to threatening a person with for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

7. Intellectual Property Crimes: Intellectual property consists of a bundle of rights. Any unlawful act by which owner is deprived completely or partially of his rights is an offence. The general forms of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

8. Online Gambling: Online fraud and cheating has now become money making business which is growing presently in the cyber world. There are many cases which reveal credit card crimes, fake job offerings, etc.

9. Financial Crimes: Users of networking sites and phone networking try to attack the victim by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

10. Forgery: To cheat and deceive large number of persons by sending threatening mails as online business transactions and troubling the victims is increasing at a large speed.

11. URL hijacking or squatting: Using the domain name in bad faith. the squatters neglect the existence of a trademark to profit from others .Same Domain name claimed by two parties either by claiming that they had registered the name first or by right of using it before the other. Typo squatters will buy a domain with a typo in them. For example two similar names i.e. www.yahoo.com and www.yaahoo.com. or www.linkdin.com or www.linkedin.com.

12. Cyber Vandalism: Vandalism means purposefully or intentionally destroying or damaging property of another. Cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.

13. Hacking Computer System: Hacking refers to unauthorized access/control over the computer which results in loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and are done to damage the reputation of particular person or company.

14. Virus transmission: Viruses are programs that attach themselves to a computer or a file and then circulate and infect other files and other computers on a network. The data on a computer is affected by them either by altering or deleting the data from the system.

15. Unauthorized access or Trespass: Accessing someone's computer without the right authorization of the owner without disturbing , altering , misusing, or damaging data or system by using wireless internet connection.

16. Internet Time Thefts: Internet time theft comes under hacking. An unauthorized person uses the internet for his own usage and number of the Internet hours is paid by another person. Victim's ISP user ID and password is accessed by unauthorized persons, either by hacking or by gaining access to it by illegal means and he uses it to access the Internet without the other person's knowledge. One can identify time theft if internet time (hour) has to be recharged often, despite infrequent usage.

17. Cyber Terrorism: Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

18. Cyber Warfare: Cyber warfare involves the battle space use and targeting of computers and networks in warfare. It involves both offensive and defensive operations pertaining to the threat of cyberattacks, damages, disruptions and sabotage.

19. Distribution of pirated software: It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
20. Possession of Unauthorized Information: It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

Cyber Crimes affects the companies at large as almost all the companies gain an online presence and take advantage of the rapid gains in the technology but greater attention to be given to its security threats and risks. In the modern cyber world cyber crimes is the major issue which is harming an individual as well as society at large .

I.T. legislation in India:

Government of India enacted its Information Technology Act 2000 with its objectives stated in Act itself "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the deserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto." The Information Technology Act, 2000, was thus passed as the ctNo.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000.The Act mainly deals with certain issues like legal recognition of electronic documents, legal recognition of digital signatures, offenses and contraventions, justice dispensation, systems for cyber crimes.

Amendment Act 2008:

The previous Act was the subject of certain debates, reviews and few criticisms. Due to some omissions in the act it resulted the investigators to rely more and more on the provisions of Indian Penal Code even in technology based cases with the I.T. Act ITACT was referred but reliance was more on IPC rather on the ITA. The need for an amendment was felt for the I.T. Act from the year 2003-04. Major industrial bodies were consulted and advisory groups were formed to suggest recommendations for the need of Information Technology Amendment Act 2008. This Amendment Act got the President assent on 5th Feb 2009 and was made effective from 27 Oct 2009. ITAA considers main issues like data privacy, information security, defining cybercrime, making digital signature technology neutral, defining reasonable security practices to be followed by corporate, redefining the role of intermediaries, recognizing the role of Indian Computer Emergency Response Team, inclusion of some additional cyber crimes like child pornography and cyber terrorism, authorizing an Inspector to investigate cyber offences (as against the DSP earlier).

Penalty For Damage To Computer System: According to the Section: 43 of 'Information Technology Act, 2000' whoever does any act of destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine up to 1crore to the person so affected by way of remedy. According to the Section:43A which is inserted by 'Information Technology(Amendment) Act, 2008' where a body corporate is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. And Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

Suggestions and Preventive Measures for Cyber Crimes:

Certain measures are taken by users while using the internet to perform digital banking transaction which will help them to combat the Cyber Crime are not to reveal their account details via e-mails and while chatting. Updated Anti-virus software protection against virus attacks should be used by all those who are using internet. One should never reveal credit card number to any unsecured site to guard against frauds. Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day. It is better to use a security programmes by the body corporate to control information on sites.Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of customers. Justice must be provided to the victims of cyber crimes. They should be provided compensation and offenders are also to be punished.

VI. Conclusion

With the increasing use of internet services worldwide, it is becoming easy to access any information easily. Internet which is the medium for huge information and a large base of communications but using it can be beneficial if certain precautionary measures are also taken by users while using the internet which will help them to combat the Cyber Crime.

Bibliography

[1]. Ajeet Singh Poonia, cybercrime,challenges and its classification, International journal of Emerging Trends and Technology in Computer Science (Volume 3,issue 6, Nov- Dec 2014,pg 120)

[2]. Kamini Dashora, Cyber Crime in the society: Problems and Preventions, 2011,vol-3,pg 243-244.

[3]. Digpal Singh, H Rathore and Karn Marwah: Cyber Crime in Banking Sector .International journal of law mantra. www.lawmantra.co.in.www.cyberlawsindia.net,

[4]. www.meity.gov.in/content/cyber-laws, https://www.legalindia.com/cyber-crimes-and-the-law/