

Review Article

Customers' Perception Towards Victimization Practices In Banking

S.Sathish

Ph.D. Part-Time Research Scholar,
Pg And Research Department Of Commerce,
Kongu College Of Arts And Science,
Affiliated To Bharathidasan University, Tiruchirappalli,
Karur, Tamil Nadu, India.

Dr.Chi.Nanjappa

Assistant Professor And Research Supervisor,
Pg And Research Department Of Commerce,
Kongu College Of Arts And Science,
Karur, Tamil Nadu, India.

Abstract

The Technological Development In The Banking Sector Began With The Use Of Advanced Ledger Posting Machines (Alpm) In The 1980s And Now-A-Days Banks Are Using Core Banking Solution (Cbs) For Providing Better Services To Their Customers. Information Technology And The Communication Networking Systems Have Revolutionized The Functioning Of Banks And Other Financial Institutions All Over The World. Though The Technological Developments Have Taken Place, Still People Are Having Very Limited Access With The Technologies In Bank. This Helps The Fraudsters To Cheat The People By Using So Many Tricks. The Trick Has Been Named As Cyber Crime. As There Is No Physical Evidence To These Crimes, Criminals Are Free To Act. In This Background, The Study Has Been Carried Out To Know The Awareness Level Of Customers About Cyber Crimes And Their Satisfaction Level Towards The Protection Made By Their Banks. This Study Consisted Of 540 Sample Respondents And The Information Collected From Them Were Analysed With Help Of Spss 23.0. The Findings Of The Study Have Been Summarised And Concluded With Suitable Suggestions.

Key Words: Information Technology, Cyber Crime, Awareness And Perception

1. Introduction

Cybercrime Is The Latest And Perhaps The Most Complicated Problem In The World. It Is A Crime Committed On The Internet. A Crime Is An Unlawful Act Which Is Not To Be Measured By The Issue Of Occasions, But With The Lawful Aims And By The Bad Intentions Of Men. Cybercrime Is A Digital Wrong Doing. Digital Criminal Acts Are A Variety Of Wrongdoings, Which Utilize Machines And Network Systems For Criminal Exercises. Cybercrime Is Emerging As A Serious Threat. Cybercrimes Have Affected Different Sectors Among Which Banking Sector Is One Of Them Which Have Witnessed Different Forms Of Cybercrimes Like Atm Frauds, Phishing, Identity Theft, Denial Of Service.

In Today's Globalize World To Narrow Down The World, Banking Sector Provides Many Facilities To Their Clients And Customers Facilities Like Internet Banking, Credit Card Facilities, Debit Card Facilities, Online Transfer, By This All Kind Of Facilities Banks Customer Can Use Bank Facilities 24 Hours And Also They Can Easily Transect And Easily Operate Their Account From Any Place Of The World With The Help Of Net And Mobile. As We All Known That As These Facilities Are Beneficial For The Customer But It Also Have An Evil Side. Today, The Maximum Information Being Online Is Highly Susceptible To Attack By Cyber Criminals. Banks Have Become Many Cyber Fraud Cases Which Caused Huge Loss Of Money To The

Common Customers In Every Year. Cybercrime Can Be Described As A Criminal Activity Done Using Computers And The Internet In Indian Banking Sector.

2. Statement Of The Problem

Cybercrime Is A Growing Threat In The Virtual World Because Individuals And Organizations Are Relying More On Internet At An Increasing Rate. The Use Of Internet And Other Technologies Have Increased The Risk Of Attack From Cyber Criminals Across The Globe. With The Number Of Incidents Of Theft, Phishing, Computer Viruses, Hacking, On The Rise, There Is A Need To Explore The Cybercrime Scenario. Although, With The Advent Of Technologies, The Banking Sector Has Been Able To Reach More Customers However, It Has Also Enhanced The Risk For Customers Who Often Feel Reluctant And Insecure In Opting For Such Services. There Is A Need For The Banks To Evaluate Their Current Operating Practices. And It Also Identified That There Is A Need For Research Work In The Field Of Customers' Awareness Towards Cybercrime In Private Sector Banks With Special Reference To The Following Questions;

1. What Is The Level Of Awareness Of The Customers' Towards Cybercrime In Banks?
2. Are The Customers Perceived About The Victimization Avoidance Practices In Cybercrime?

3. Objectives Of The Study

The Present Study Is Undertaken With The Following Specific Objectives:

1. To Study The Awareness Level Of Customers Towards Cybercrime In Banks.
2. To Understand The Perception Level Of Level Of Customers Towards Victimization Avoidance Practices.

4. Methodology

4.1 Period Of This Study

The Required Primary Data Have Been Collected From The Sample Respondents During The Period From April 2019 To August 2019. The Analysis Of Data And Research Report Writing Were Made During The Period From December 2019 To February 2021.

4.2 Sampling Design And Methodology

The Present Study Intends To Examine The Issues Framed In The Objectives And Hypotheses Relating To The Study. This Study Is An Empirical Research Based On Survey Method. The Data Collected For The Study Include Both Primary Data And Secondary Data. The Present Study Is Confined To Erode District. Hence, The Samples For The Present Study Have Been Taken From Branches Of The Banks In Erode District. For The Purpose Of Selecting Samples, Non-Probability Purposive Sampling Method Has Been Adopted. By Using This Method, 540 Customers Those Who Are Having Bank Account Has Been Taken As The Sample For This Study. The Primary Data Has Been Collected Through Structured Questionnaire Method. The Secondary Data Were Collected From Various Journals, Books, Newspaper And Websites Related To The Study. In The Present Study, The Data Collected From The Primary Sources Are Analyzed With References To Each Of The Objectives With The Help Of The Statistical Tools Such As Percentage Analysis, Chi-Square Test And Analysis Of Variance (Anova).

5. Review Of Literature

Susheel Chandra Bhatt Anddurgesh Pant (2011) Found That All The Banks Use The Latest Technology For The Online Security Feature But Still They Have Small Loopholes In This Feature. All Bank Users Do Not Use Online Facilities Because They Have No Proper Information And The Reason Behind All This Is The Same Lack Of Awareness. **Atulbammara Et Al (2012)** Their Research Paper Attempts To Study The Assurance And Responsiveness Of Public And Private Sector Banks With Respect To Their Customers Exclusively Cyber-Crime Victims. Their Paper Presents The Preliminary Findings Of A Research Study To Identify The Essential Ingredients Of Successful Bcm Implementation Based On Experiences Of Banks In India. **F.Wada And G.O. Odulaja (2012)** Made A Study To Assess Cybercrime And Its Impact On The Banking Institutions In Nigeria. It Also Examined The Existing Policy Framework And Assessed The Success Of The Institutional Counter Measures In Combating Cybercrime In The Banking Industry. **R.R. Soni And Sonineena(2013)** Their Study Is An Effort To Review And Analyze The Subject In Indian Context With A Comparative Touch Between Private And Public Sector Banks In The Country. Frauds With Online Payments, Atm Machines, Electronic Cards And Net Banking Transactions Have Become A Serious Issue. **R.Judithpriya Et Al (2018)** Advocated *That* The Use Of Modern Gadgets Have Greatly Increased The Number Of

Cybercrimes. It Was Also Stated That No One Could Exist In This World Without The Use Of Modern Electronics Such As Mobile Phones, Computers, Laptops, Etc. The Usages Of These Gadgets Are Now Most Commonly Seen In College Students. The Three Forth Of The Part Of Education Has Become Internet. They Are Exposed More To These Gadgets. The Result Revealed That The Technical Advancement Has Paved The Way For Cybercrime.

6. Limitations Of The Study

In The Entire Course Of The Study, Data Was Collected And Interpreted With Utmost Care And Consistency. But, The Present Study Has Some Limitation. The Study Has Been Made By Adopting Purposive Sampling. The Study Is Restricted Only To The Erode District. Hence, The Results May Not Be Applicable To Other Areas.

7. Data Analysis And Interpretation

Table 1
Distribution Of Sample Respondents According To Their Level Of Awareness

Socio Economic Variables	Calculated Value Of Chi-Square	Degrees Of Freedom	Level Of Significance
Place Of Domicile	12.085	2	Significant At 1 Per Cent Level
Age	14.285	1	Significant At 1 Per Cent Level
Gender	6.041	1	Insignificant At 5 Per Cent Level
Marital Status	2.559	1	Insignificant At 1 Per Cent Level
Education	7.006	2	Significant At 5 Per Cent Level
Occupation	8.157	3	Significant At 5 Per Cent Level
Type Of Family	2.552	1	Insignificant At 5 Per Cent Level
Family Size	7.063	2	Significant At 5 Per Cent Level
No. Of Earning Members	14.799	2	Significant At 1 Per Cent Level

Source: Primary Data

Sources Of Awareness

The Following Table Displays The Distribution Of Respondents Based On The Sources Of Their Awareness About Cybercrimes In Banking.

Table 2
Sources Of Awareness About Cybercrime In Banking

Sources	No. Of Respondents	Percentage
Television	62	11.48
Radio	137	25.36
Newspapers And Magazines	88	16.30
Own Accord	92	17.04
Friends And Relatives	104	19.26

Bank/ Rbi Advice	57	10.56
Total	540	100

Source: Primary Data

It Is Observed From The Table 2 That Most (25.36 Per Cent) Of The Respondents Have Come To Know About Cybercrimes Through Radio, 19.26 Per Cent Are Aware About Cybercrimes Through Friends And Relatives, 17.04 Per Cent Of The Respondents Get The Awareness Through Own Accord, 16.30 Per Cent Of The Respondents Aware Through Newspapers And Magazines, 11.48 Per Cent Of The Respondents Aware Through Television And 10.56 Per Cent Get Awareness Through Bank And Rbi Advice.

Relationship Between Personal And Socio Economic Variables And The Perception Level Of Samplerspondents In Respect Of Protection Against Victimization Through Cybercrime

In Order To Analyze The Perception Of The Respondents About The Victimization Avoidance Practices From The Cybercrime, There Are 30 Statements Have Been Used. To Test The Reliability Of The Data, Cronbah's Alpha Has Been Applied. Further, The Respondents Have Been Segmented By Using Cluster Analysis Based On Their Life Style.

Table 2

Distribution Of Sample Respondents According To Their Level Of Satisfaction: 'F' Test

Socio Economic Variables	Calculated Value Of 'F' (Anova)	Level Of Significance
Place Of Domicile	15.231	Significant At 1% Level
Age	16.568	Significant At 1% Level
Education	8.112	Significant At 1% Level
Occupation	9.720	Significant At 1% Level
Family Size	1.743	Insignificant At 5 % Level
No. Of Earning Members	8.600	Significant At 1% Level

Source: Primary Data

Table 3

Distribution Of Sample Respondents According To Their Level Of Satisfaction: 'Z' Test

Socio Economic Variables	Calculated Value Of 'Z'	Level Of Significance
Gender	1.735	Insignificant At 5 % Level
Marital Status	3.933	Significant At 1% Level
Nature Of Family	2.196	Significant At 5 % Level

Source: Primary Data

8. Findings Of The Study Based On Awareness Level

- ❖ It Is Found That Majority (52.3 Per Cent) Of The Respondent Belong To Urban Area Have High Level Of Awareness About Cybercrimes In Banking.
- ❖ It Is Found That Majority (58.2 Per Cent) Of The Respondents Belong To The Age Category Of Up To 25 Yearshave High Level Of Awareness About Cybercrimes In Banking.
- ❖ It Is Found That Majority (51.3 Per Cent) Of Male Respondents Have High Level Of Awareness About Cybercrimes In Banking.
- ❖ It Is Found That Majority(51.3 Per Cent) Of The Unmarried Respondents Have High Level Of Awareness About Cybercrimes In Banking.

- ❖ It Is Found That Majority (56.3 Per Cent) Of The Respondents Belong To The Educational Category Of Post Graduate/Profession Have High Level Of Awareness About Cybercrimes In Banking.
- ❖ It Is Found That Majority (51.7 Per Cent) Of The Respondents Belong To Others Group Have High Level Of Awareness About Cybercrimes In Banking.
- ❖ It Is Found That Most (49.2 Per Cent) Of The Respondents Belong To Nuclear Family Have High Level Of Awareness About Cybercrimes In Banking.
- ❖ It Is Found That Majority (55.5 Per Cent) Of The Respondents Belong To The Category Of Up To Three Member Family Have High Level Of Awareness About Cybercrimes In Banking.
- ❖ It Is Found That Majority (68.3 Per Cent) Of The Respondents Belongs To Three And Above Earning Member Family Group Have High Level Of Awareness About Cybercrimes In Banking.
- ❖ It Is Found That Most (25.36 Per Cent) Of The Respondents Have Come To Know About Cybercrimes Through Radio Out Of Six Sources About Cybercrime In Banking.

Perception Level Of Sample Respondents In Respect Of Protection Against Victimization Through Cybercrime

- ❖ From The Total Of 540 Sample Respondents In The Study, Majority (63.3 Per Cent) Of The Sample Respondents Belong To The Urban Category, Majority (52.4 Per Cent) Of The Sample Respondents Belong To The Age Category Of 26 To 50 Years, Majority (56.3 Per Cent) Of The Sample Respondents Are Male, Majority (64.4 Per Cent) Of The Sample Respondents Are Married, Majority (60.0 Per Cent) Of The Sample Respondents Belong To The Category Of Under Graduates, In Terms Of Occupation 32.6 Per Cent Of The Sample Respondents Belong To The Category Of Others, Majority (65.6 Per Cent) Of The Sample Respondents Belong To The Nuclear Family, Majority (56.7 Per Cent) Of The Sample Respondents Belong To The Category Of 4 To 6 Members In The Family Size, 36.1 Per Cent Of The Sample Respondents Belong To The Category Of Only One Earning Members In The Family And Majority (60.7 Per Cent) Of The Sample Respondents Belong To The Income Category Of Below Rs.25,000.
- ❖ The 'Z' Test Applied Has Revealed That There Is A Significant Relationship Between The Perception About Victimization Avoidance Practices In Banking And Marital Status, And Family Type Of The Respondents.
- ❖ The 'F' Test Applied Has Revealed That There Exists Significant Relationship Between The Perception About Victimization Avoidance Practices In Banking And The Different Groups Of Respondents, That Is, Place Of Domicile, Age, Education, Occupation, Number Of Earning Members In The Family And Monthly Income Of The Respondents.
- ❖ The Variables Such As Gender And Family Size Of The Respondents Are Not Having Significant Relationship With The Perception About Victimization Avoidance Practices In Banking.

9. Suggestion And Conclusion

This Research Report Is Based On Primary Data. It Is Useful To Know The Consumer Awareness Towards Cyber-Crime. The Awareness Level Of Customers About Cybercrime Is Low In All The Demographic Categories. Hence, It Is Suggested That Workshops And Seminars Should Be Conducted By Banks From Schools And Colleges And General Public To Create Awareness On Cybercrime Victimization. Further, Short Duration Courses Could Be Conducted With A Subsidized Fee By Public And Private Sectors To Train The Public About Security Measures Needed To Be Adopted While Online Banking Services. A Strong Education System Should Be Followed In The Society To Deliver Education At Every Stage With A Special Stress On Information Technology Which Should Be Secure And Free From Cybercrime And In Reach To A Common Man. The Banks Should Also Increase The Dependability Of Their Security Mechanism Among The Mind Of Their Customers In Order To Increase The Perception Level Of Customers About The Victimization Avoidance Practices.

10. References

1. Atulbamrara, Gajendra Singh, Mamta Bhatt (2012), "An Explorative Study Of Satisfaction Level Of Cyber-Crime Victims With Respect To E-Services Of Banks", Journal Of Internet Banking And Commerce, Vol. 17, No.3,Pp 1-15
2. Azeeznureniayofe And Osunadeoluwaseyifunmitan (2009), "Towards Ameliorating Cybercrime And Cybersecurity",International Journal Of Computer Science And Information Security,Vol. 3, No. 1,Pp 1-11
3. Judith Priya, R, Sreerithanyaa, R.S., Preethisri, T.J. (2018), "Awareness Of Cybercrime Among College Students - An Analytical Study", International Journal Of Management And Social Sciences, Vol. 8, No.13, Pp.87-90
4. Raghavam A.R. And Lathaparthiban (2014), "The Effect Of Cybercrime On A Bank's Finances", International Journal Of Current Research, Volume-2, Pp-173-178.
5. Soni.R.R. And Sonineena (2013), "An Investigative Study Of Banking Cyber Frauds With Special Reference To Private And Public Sector Banks", Research Journal Of Management Sciences, Volume No. 2(7), Pp.22-27
6. Susheel Chandra Bhatt And Durgesh Pant (2011), "Study Of Indian Banks Websites For Cyber Crime Safety Mechanism" International Journal Of Advanced Computer Science And Applications, Volume. 2(10),Pp 87-90
7. Wada F And Odulaja G.O (2012), "Electronic Banking And Cyber Crime In Nigeria - A Theoretical Policy Perspective On Causation",African Journal Of Computing & Ict Reference Format, Vol.5. No.1, Pp. 69-82.