A Study on Customers Awareness of E-Banking Cyber Security

A.S. Aravindh[1], Dr. K. Rajesh Kumar[2]

[1]*Research Scholar, Department of Business Administration, Annamalai University, Annamalai Nagar-608002, India*
[2]*Professor, Department of Business Administration, Annamalai University, Annamalai Nagar-608002, India*

This study describes and finds out the customers awareness of E-Banking Cyber Security. Here Awareness of E-Banking Cyber Security belongs to the dimensions of Malware, Social Engineering Attack, Identify Theft, Key loggers, and Man-in-the-Middle. In the study to find out through the Path Regression Analysis, which awareness has the most impact an E-Banking Cyber Security? In this study Descriptive research design and convenience sampling technique are applied.

Keywords: Cyber Security, E-Banking, Customers Awareness.

1. Introduction

Customer Awareness of E-Banking Cybersecurity refers to the level of perception and understanding that customers acquire regarding the possible cyber threats and security risks related to using online banking services. This awareness consists of familiarity with various types of cyber attacks (such as Malware, Social Engineering Attack, Identify Theft, Key loggers, and Man-in-the-Middle) perceptive of secure online behavior (like using tough passwords, enabling two-factor confirmation, and avoiding distrustful links), and the recognition of cyber security best practices that care for personal and financial information while accessing banking platforms.

The study aimed to investigate the influence of e-banking security awareness on Malware, Social Engineering Attack, Identify Theft, Key loggers, Man-in-the-middle threats; Here E-banking security awareness is the independent variable, and e-banking cyber security awareness is the dependent variables of this study. The study is undertaken in Chennai city through a pretested and well-designed mail survey. Hence, the researcher intended to study the cyber security awareness among the public sector bank customers.

2. Review of Related Literature:

Over the past 15 years, numerous studies have highlighted the importance of security across all Internet-based services and channels, focusing on various cyber security issues (Adholiya and Adholiya, 2019). They assessed users' awareness of cyber security tips during e-banking and analyzed how socio-economic factors influenced this awareness, based on a sample of 200 bank customers. Findings revealed that many customers were aware of cyber threats and cybercrime, while socio-economic status significantly impacted their awareness of such threats. According to 2021 statistics, 98% of cyber attacks employed social engineering tactics, affecting 43% of IT professionals within the prior year. Additionally, a study by Vimala (2016) explored customer perceptions and awareness regarding e-banking security. Using data from 50 customers in one area, it found that only 32% recognized security issues in e-banking, with 50% experiencing attacks like hacking and phishing. The study also pointed to gaps in knowledge among cybercrime victims and emphasized the importance of local government and banks conducting awareness initiatives about cyber security risks. Olalere et al. (2014) examined the influence of educational background on respondents' awareness of phishing attacks and their experiences with information breaches during e-banking, along with their understanding of malware threats. Their survey on five common cyber security issues showed that most individuals believed e-banking was secure, downplaying associated risks; they suggested advertising through television and radio and hosting quarterly seminars to enhance customer awareness of these risks. Tabiaa et al. (2017) concluded that fostering customer knowledge and awareness is crucial to mitigate e-banking security risks, advocating for collaboration between government and private sectors to achieve this goal.

3. Objective:

To measure the customers awareness level of E-Banking Cyber Security

4. Research Design and Sample:

In the present study descriptive research design will be adopted. Descriptive research studies are those studies which are concerned with describing the characteristics and attitude of a particular individual, or a group. Here the study describing the customers awareness level of E-Banking Cyber Security. Descriptive research is a widely accepted method in fact-finding, and the study includes adequate and accurate interpretation of results. The convenience sampling technique is applied to this study to measure customers awareness level E-Banking Cyber Security. 640 sample data is collected from various demography segment banking customers.

5. Analysis and Interpretation:

The study takes Path Regression Analysis of Customers Awareness of E-Banking Cyber Security

Table- 1: Model Fit Summary

Model	R	R-Square	Adjusted R-Square	Std. Error of the Estimate	Durbin-Watson
Customers awareness of E-Banking Cyber Security	0.990	0.980	0.980	0.16769	1.596

Dependent Variable: Customers awareness of E-Banking Cyber Security

The model reveals that the R- (Multiple Correlation Coefficients) value is 0.990. It is measuring the degree of relationship between the Customers awareness of E-Banking Cyber Security and the predicted values like Malware, Social Engineering Attack, Identify Theft, Key loggers, and Man-in-the-Middle. R-Square (Coefficient of Determination) value is 0.980. It is more than about 98% of the variation in customers awareness of E-Banking Cyber Security is explained by the variation in the independent variables. Adjusted R-squared value is 0.980. It adjusts the statistic based on the number of independent variables in the model. That is the desired property of goodness-of- fit statistic.

Furthermore, Durbin-Watson (DW) value exists 0 à 4 is good correction, (0 à2 is positive auto correction, 2 à 4 negative auto correction) Here statistics show 1.596, indicating positive auto correction, i.e., good correction.

Table- 2 Regression Weights for Customers Awareness of E-Banking Cyber Security

Regression Weights	Estimate	S.E.	C.R.	P
Customers Awareness of E-Banking Cyber Security <--- Malware	0.210	0.009	23.022	0.000
Customers Awareness of E-Banking Cyber Security <--- Social Engineering Attack	0.225	0.008	28.731	0.000
Customers Awareness of E-Banking Cyber Security <--- Identify Theft	0.178	0.009	19.832	0.000
Customers Awareness of E-Banking Cyber Security <--- Key loggers	0.233	0.009	24.940	0.000
Customers Awareness of E-Banking Cyber Security <--- Man-in-the-Middle	0.150	0.010	15.721	0.000

Note: .000 is 1% α -significant level

The Path diagram represents the independent variables of the Customers Awareness of E-Banking Cyber Security like Malware, Social Engineering Attack, Identify Theft, Key loggers, and Man-in-the-Middle. Here Path Regression analysis employed on all five variables; among them, all variables are highly significant at 1% α -significant level.
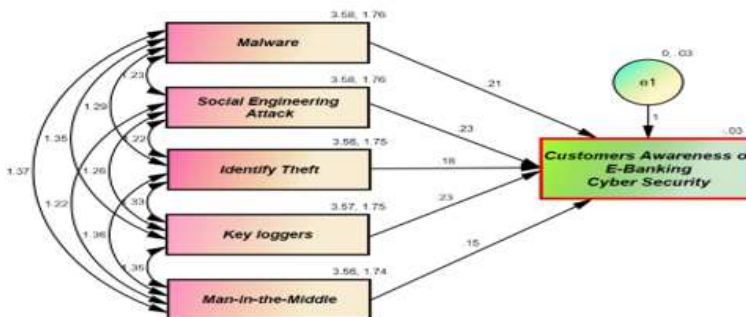

Fig-1 Path Regression Analysis of Customers Awareness of E-Banking Cyber Security

Table-3 Covariance for Customers Awareness of E-Banking Cyber Security Dimensions

Covariance	Estimate	S.E.	C.R.	P
Malware <--> Man-in-the-Middle	1.372	0.088	15.588	0.000
Man-in-the-Middle <--> Social Engineering Attack	1.217	0.084	14.418	0.000
Man-in-the-Middle <--> Identify Theft	1.358	0.088	15.509	0.000
Man-in-the-Middle <--> Key loggers	1.345	0.087	15.428	0.000
Malware <--> Key loggers	1.350	0.088	15.419	0.000
Social Engineering Attack <--> Key loggers	1.261	0.086	14.748	0.000
Identify Theft <--> Key loggers	1.332	0.087	15.305	0.000
Social Engineering Attack <--> Identify Theft	1.216	0.085	14.384	0.000
Malware <--> Identify Theft	1.290	0.086	14.963	0.000
Malware <--> Social Engineering Attack	1.226	0.085	14.448	0.000

The above table interprets covariance relationship of Customers Awareness of E-Banking Cyber Security Dimensions all relationships are significant. The probability of getting a critical ratio as large as 15.588 in absolute value is significant at less than 0.001. In other words, the covariance between Malware <--> Man-in-the-Middle, Man-in-the-Middle <--> Identify Theft, and Man-in-the-Middle <--> Key loggers relationships are highly significant at 1% level. The estimate values are 15.588, 15.509 and 15.428 is highly significantly different from at the 0.05 level (two-tailed).

Table-4 Correlations for Customers Awareness of E-Banking Cyber Security Dimensions

Correlations	Estimate
Malware <--> Man-in-the-Middle	0.783
Man-in-the-Middle <--> Social Engineering Attack	0.694
Man-in-the-Middle <--> Identify Theft	0.777
Man-in-the-Middle <--> Key loggers	0.770
Malware <--> Key loggers	0.770
Social Engineering Attack <--> Key loggers	0.718
Identify Theft <--> Key loggers	0.761
Social Engineering Attack <--> Identify Theft	0.692
Malware <--> Identify Theft	0.734
Malware <--> Social Engineering Attack	0.697

The above table interprets Correlation's relationship of Customers Awareness of E-Banking Cyber Security Dimensions, all variables' relationships are positive correlated. Among the relationship the high correlated Dimensions are Malware <--> Man-in-the-Middle, Man-in-the-Middle <--> Identify Theft, Man-in-the-Middle <--> Key loggers, and Malware <--> Key loggers the correlation values are 0.783, 0.777, 0.770, and0.770 respectively.

6. Findings

The significant variables are compared with estimated values, which resulted in the first influencing Customers Awareness of E-Banking Cyber Security dimension is 'Key loggers', and the estimate value is 0.233. The second influenced dimension is 'Social Engineering Attack' and the estimate value is 0.225. The third influenced dimension is 'Malware', and the estimate value is 0.210.

7. Suggestions

Successful cyber security awareness entails customers being positive in safeguarding their information and recognizing common caution signs of scheme. It also means that customers are informed about the protection features provided by their banks, such as encrypted communications, fraud protection, and security alerts measures. High awareness helps customers moderate risks, reduce vulnerability to cyber threats, and eventually protect both their own and the bank's data reliability in the digital banking environment.

References

1. Adholiya.A and S. Adholiya, "A Study on Cyber Security Practices and Tips Awareness among E- Banking A Study on Cyber Security Practices and Tips Awareness among EBanking Services Users of Udaipur 2019
2. Oliveira, Martins, C. T. and Popovič, A., 2014. Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. International Journal of Information Management, 34(1), pp.1-13.
3. Tabiaa,M, A. Madani, and N. El Kamoun, "EBanking: Security risks, previsions and recommendations," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 11, pp. 189–196, 2017.
4. Vimala,V "An Evaluative Study on Internet Banking Security among Selected Indian Bank Customers," Amity J. Manag. Res., vol. 1, no. 1, pp. 63–79, 2016.