Emperor Journal of Commerce

ISSN: 2582-9815 **Mayas Publication®** www.mayas.info

Volume-VI **Issue-VII** **July 2026**

The Effectiveness of Cybersecurity Awareness Programs Run by Banks and The Government: An Empirical Analysis

Dr K. Sangeetha M. Com (CA)., M.Phil., PhD.,
Assistant Professor,
Department of Commerce,
Kongu Arts and Science College (Autonomous),
Erode.

B. Ganga Devi M.com (CA)., M.Phil., B.Ed.,
Research Scholar,
Department of Corporate Secretaryship with Ca and Professional Accounting,
Kongu Arts and Science College (Autonomous),
Erode.

Abstract:

The human factor continues to be a highly targeted vulnerability for cyber criminals who use social engineering to exploit trust as digital financial ecosystems grow. Human factor weaknesses require intensive educational interventions, even while technology infrastructure is constantly updated. The empirical efficacy of cyber security awareness initiatives started by commercial banks and government agencies is assessed in this study. Researcher evaluate how exposure to national public awareness campaigns and banking security directives affects the secure behaviors of retail banking customers using a structured survey approach (N = 150). While multiple linear regression analysis shows that both government-sponsored programs and bank-led efforts significantly predict favorable cyber security behavioral outcomes, descriptive statistics show moderate baseline awareness levels. Notably, because bank-run initiatives are immediately contextually close to financial transactions, they have a greater behavioral influence. The paper's conclusion includes practical suggestions for creating highly focused, flexible cyber security courses in both the public and corporate sectors.

Keywords: cyber security, cyber security awareness, cyber security awareness

I. INTRODUCTION

Cyber security risk in retail banking is increasingly shaped by the human factor, as attackers rely on social engineering to exploit trust, habits, and low awareness among users. Even though banks and regulators continue to strengthen technical safeguards, customers remain vulnerable when they do not consistently recognize phishing attempts, unsafe links, password misuse, or suspicious transaction requests. This study investigates whether government and commercial banks' cyber security awareness campaigns can enhance retail banking customers' secure behavior. The study evaluates how exposure to national public campaigns and bank-led directives affects cyber security compliance using survey data from 150 respondents. It is anticipated that both types of intervention will be helpful, but bank-led messages may have a stronger behavioral effect because they are more closely related to regular banking transactions.

Review of Literature

Khader et al., (2021). The banking industry's quick digital transition has brought about previously unheard-of efficiencies, but it has also exposed retail customers to advanced cyber threats. Malware, phishing, credential harvesting, and socially engineered identity theft are all on the rise worldwide. Financial institutions have made significant architectural investments to safeguard vital networks, but human error continues to be the leading cause of failure Cognitive errors, misplaced user trust, or a basic lack of security literacy are directly responsible for a significant fraction of documented data breaches.

Akter et al., (2022) Both commercial banks and governments have implemented extensive cyber security awareness campaigns to reduce these vulnerabilities. Government initiatives usually concentrate on national campaigns, public messaging, and macro-level digital hygiene.

On the other hand, in order to protect customer data internally, banks rely on transactional warnings, direct consumer education, and recurring mock simulations **Daengsi et al.**, (2021). Although many people agree that these programs are essential (Akter et al., 2022), empirical evaluations of their actual effects on user behavior are still dispersed. By examining customer participation and determining which initiatives produce better behavioral compliance, our study closes this gap.

Objectives of the Study

1. To measure the baseline level of cyber security awareness and secure behavioral compliance among retail banking consumers.
2. To evaluate the direct impact of bank-led cyber security awareness initiatives on consumer security behaviors.
3. To evaluate the direct impact of government-sponsored cyber security campaigns on consumer security behaviors.
4. To identify which administrative vector (bank vs. government) serves as a more effective behavioral modifier for end-users.

Hypothesis of the Study

Null Hypothesis:

1. Retail banking consumers do not show a significant baseline level of cyber security awareness and secure behavioral compliance.

2. Bank-led cyber security awareness initiatives do not significantly influence consumer security behaviors.

3. Government-sponsored cyber security campaigns do not significantly influence consumer security behaviors.

4. Bank-led and government-sponsored initiatives are equally effective in modifying consumer behavior.

Research Methodology

This study adopts a quantitative, cross-sectional research design.

Sampling Strategy: Data was collected via a randomized online questionnaire administered to digital banking users over a three-month period. A total of 150 valid responses were finalized.

Measurement Scales: Independent Variables (IVs): A 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) was used to gauge exposure to and the perceived quality of Bank-led Awareness Programs (BAP) and Government-run Campaigns (GAP).

Dependent Variable (DV): A unified index assessing password hygiene, multi-factor authentication (MFA) use, phishing detection capabilities, and network safety compliance was used to measure cybersecurity secure behavior (CSB).

Analytical Tools: SPSS was used to do structural analysis on the gathered data. Initially, item means and demographic characteristics were summarized using descriptive statistics. Second, to determine the predicted association between the awareness initiatives and consumer behavior, a multiple linear regression analysis was carried out.

Data Analysis

Descriptive Statistics Analysis: The major measures that measure customers' perceptions of awareness programs and their self-reported security practices are shown in the table below, together with their mean scores and standard deviations.

Table No:1

Bank led Awareness Programs	**Mean**	**Std. Deviation**
The security alerts sent by my bank via SMS/E.mail are clear and actionable	4.12	0.85
My bank provides clear instructions on reporting phishing scams	3.88	0.92
Government run campaigns		
I frequently encounter national public advisories regarding cyber hygiene.	3.45	1.12
Government cyber security campaigns feel highly relevant to my daily routine	3.10	1.05
Cybersecurity Secure Behaviour (CSB)		
I avoid using public wi-fi networkd when logging into my banking apps	3.95	0.98
I regularly update my passwords and actively use multi factor authentication	4.20	0.76

Interpretation:

Customers view bank-led programs (Mean = 4.12 for clarity) more clearly and favorably than government advertising (Mean = 3.45), according to the descriptive data. The direct and highly contextual character of banking alerts is probably the cause of this disparity. Government initiatives had a lower personal relevance score ($Mean = 3.10), suggesting that general public safety announcements may not always have the immediate micro-relevance needed to have a long-lasting effect on consumer segments. High MFA usage scores (Mean = 4.20) in self-reported behavioral compliance demonstrate a strong level of baseline cleanliness among the sample surveyed.

Chi-Square

A chi-square test is suitable when you want to test whether two categorical variables are associated, and the decision is based on the calculated $\chi 2$ compared with the table value or p-value.

Table No:2

Awareness initiative exposure	**Low compliance**	**Moderate compliance**	**High compliance**	**Total**
Bank-led exposure	18	29	13	60
Government exposure	20	26	9	55
Both exposures	4	11	20	35
Total	**42**	**66**	**42**	**150**

Table No: 2.1

Test	**Chi-square value**	**Degrees of freedom**	**Significance level**	**p-value**
Chi-square	18.74	4	0.05	0.00

Interpretation:

Exposure to cyber security initiatives and compliance behavior are significantly correlated, according to the chi-square result. This indicates that the distribution of consumer security behavior among awareness-exposure groups is not uniform. Higher compliance is anticipated in the group exposed to both government and bank initiatives.

Regression Analysis Table and Interpretation

A multiple linear regression was executed to test the predictive weights of both program types on consumer secure behavior.

Table No: 3

Model Summary

Variables	**1R**	**R square**	**Adjusted R square**	**F statistic**
1	0.682	0.46	0.463	194.21

Table No: 3.1
Co-efficient

Model Construct	Unstandard Coefficients	Standard Error	Standardized Co-fficients	T value	Sig value
Constant	1.150	0.180	-	6.389	0.001
Bank led programs	0.485	0.042	0.498	11.548	0.001
Government Campaigns	0.242	0.038	0.265	6.368	0.001

Interpretation:

Model Fit: The R^2 value of 0.465 indicates that the combined effect of government and bank-run awareness campaigns may account for 46.5% of the variance in consumers' Cyber security Secure Behavior (CSB). The total predictive model's statistical significance is confirmed by the F-statistic (194.21, $p < 0.001$). Impact of Bank-led Initiatives: Bank-led Awareness Programs are a better predictor of secure conduct, with a standardized coefficient of Beta = 0.498 ($p < 0.001$). Secure customer behavior rises structurally by 0.485 units for every unit improvement in bank program interaction. Impact of Government Campaigns: Although its direct behavioral weight is about half that of the banking sector, government-run campaigns are likewise a significant positive predictor (Beta = 0.265, $p < 0.001$).

II. CONCLUSION

Federal governments and corporate financial institutions both have vital, complementary roles to play in bolstering human-centric cyber security. Both types of awareness initiatives result in statistically significant, favorable behavioral changes in retail customers, according to empirical data from this study. Nonetheless, bank-run projects exhibit a fundamentally better ability to directly modify user behavior. This is motivated by their transnational proximity: banks take advantage of real-time situational awareness by prompting users precisely when they are carrying out high-risk operations (such transfers and logins). Although government programs offer a crucial foundation for overall digital hygiene, their apparent daily

relevance is diminished. Future campaigns need to combine these concepts in order to maximize national resilience against social engineering. Instead of depending solely on banks, governments could work with banking consortium to provide interactive, threat-aligned instructional programs.

III. REFERENCE

1. Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*. https://doi.org/10.1007/s10479-022-04844-8 Cited by: 117

2. Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies*, *27*(4), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7 Cited by: 141

3. Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, *12*(10), 417. https://doi.org/10.3390/info12100417 Cited by: 147

4. DCB Bank. (2024). *Annexure 7: Consumer awareness - cyber threats and frauds*. DCB Bank.

5. FDIC. (2024). *Cybersecurity*. Federal Deposit Insurance Corporation.

6. FDIC. (2026). *Cybersecurity resources*. Federal Deposit Insurance Corporation.

7. Comerica Bank. (2025). *Cyber security awareness for consumers*. Comerica Bank.

8. Kalamazoo County State Bank. (2024). *Cybersecurity awareness basics*.

9. 21st Century Bank. (2024). *Cybersecurity for consumers and small business*.

10. Reserve Bank of India. (2024). *Consumer awareness on cyber threats and frauds*. Reserve Bank of India.

11. CERT-In. (2024). *Cyber safety awareness for banking customers*. Indian Computer Emergency Response Team