Research Proposal_Mridul - Mridul Hasan.pdf

by Sanaul Haque

Submission date: 13-Oct-2025 11:29PM (UTC+0700)
Submission ID: 2779973335
File name: Research_Proposal_Mridul_-_Mridul_Hasan.pdf (685.5K)
Word count: 2145
Character count: 13062

Phishing Awareness and AI Defense Mechanisms in Bangladesh: A Comprehensive Study of User Vulnerabilities and Technological Trust

Scholar Name
Mridul Hasan

Scholar's Affiliation
Dhaka College

Category
Junior

Country
Bangladesh

Research Topic
Cybersecurity

Email Address
heheo1950@gmail.com

Date of Submission
28 September 2025

Abstract

This study addresses the major point of intersection between phishing awareness and AI-based security measures in Bangladesh's environment. Exerting a mixed-method design with quantitative surveys (n=300) and qualitative interviews (n=40-50), we inspect 3 key points: (1) actual vs self-reported phishing detection skills; (2) socioeconomic and cultural factors influencing phishing susceptibility; and (3) actual trust in AI security measures across digital literacy. Theoretically based on Protection Motivation Theory and Digital Capital Approach, this study figures out cybersecurity threat impacts costing Bangladesh a significant loss annually. Outcomes will inform culturally-framed security guidelines and education initiatives, influencing cybersecurity policy and human-computer interaction in emerging economies facing the same difficulties.

1. Introduction

1.1 Problem Specification

Bangladesh has witnessed phenomenal changes in its digital scenario, with internet connectivity increasing from just 3.7% in 2010 to above 44.5% in 2023 [1]. Because of this fast-paced digitization process tens of millions have been exposed to intricate cyber attacks-most notably phishing attacks that made significant financial losses, including a ransomware demand of $5 million to Biman Bangladesh Airlines in 2023 in a single incident [2]. Even though the globally machine learning-based phishing detection has advanced [3], developing nations like Bangladesh face some distinctive challenges stemming from cultural, linguistic, and socioeconomic factors that are understudied in main-stream cybersecurity literature.

According to the reports from the Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT), Bangladesh has seen a significant number of phishing attacks in recent years, reflecting an enlarging threat to its digital infrastructure [2] and identified a strong need for effective countermeasures. But a 2023 study by the BASIS (Bangladesh Association of Software and Information Services) Cybersecurity Awareness Taskforce uncovered a concerning lack of public awareness, with 59% of respondents admitting they were unfamiliar with the term " Phishing" [4] and this shows we have a critical weakness in the country's cyber security.

1.2 Research Aims and Objectives

This work fills three main gaps:

- **The Awareness-Action Gap**: Finding out the gap between self-reported phishing awareness and practical detection capabilities of Bangladeshi internet users
- **Cultural vulnerability factors**: Establish and discuss cultural and behavioral factors that influence vulnerability to region-based phishing attacks.
- **AI Trust Dynamics**: Analyzing trust attitudes in AI-driven security solutions within low-digitally-literate communities.

1.3 Research Questions

1. To what extent Bangladeshi internet users are aware of phishing threats, and how does this awareness make them practice actual security?
2. What cultural, socioeconomic and linguistic factors influence phishing vulnerability in Bangladesh?
3. How the levels of digital literacy directly affect trust in AI-driven phishing detection systems and its adoption?
4. Specifically in Bangladesh what adaption would make AI security solutions more trustworthy and effective?

1.4 Significance of the Study

This research holds significance on multiple levels. Firstly, practical impacts: the results will help to mitigate economic loss and protect vulnerable users by shaping the cybersecurity policies in Bangladesh. Secondly, this study will try to broaden the Protection Motivation Theory [5] and Digital Capital Framework [6] from non western counties to developing country contexts. Thirdly, global relevance: understanding from the Bangladesh context may benefit other fast digitizing countries with similar cybersecurity challenges.

2. Literature Review

2.1 Global Phishing Landscape

Phishing attacks have now intensified from just basic email scams to advanced planned social-engineering assaults that draw on psychological principles [7]. Modern-day phishing operations make greater use of artificial intelligence (AI) for automating message generation as well as personalization of tailored messages [8], with mobile platforms continuing as prime points of entry [9]. AI (ML) detection systems have shown to be effective in identifying phishing websites through identifying typical features of such attacks [10]. Nonetheless, the vulnerability of users towards phishing attempts heavily differs across different cultural contexts [11].

2.2 Developing Country Contexts

There are certain patterns of vulnerability that studies in developing nations identify. For instance, Indian studies detail how user awareness, financial context, and training impact phishing susceptibility [12]. In Kenya studies have considered trends in fraud in the context of m-payments, highlighting how user interactions are leveraged, as well as suspicion of such systems precipitates fraud attacks [13]. Bangladesh is one of the most interesting examples, now with the fast digitizing of fintech (bKash, Nagad), which offers opportunities together with challenges in terms of strong measures of protection as well as user awareness keeping pace with adoption [14]. Culture plays a huge role in vulnerability. Studies on victimization of phishing in Bangladesh demonstrates how trust and awareness impact user reactions [15], that is consistent with other observations of cultural impacts in security behaviours.

2.3 AI Defense Mechanisms

Today anti-phishing research is dominated by machine learning approaches. If you employ deep learning with architectures such as Convolutional Neural Networks (CNNs) can accurately classify URLs [16], whereas transformer-based email scanners reduce false positives [17]. However, all these approaches tend to stay uniform without considering variations [18] and this aspect needs increased attention from research.

2.4 Theoretical Framework

I base my analysis on two supportive theories:

- **Protection Motivation Theory [5]:** This Consider how threat assessment (vulnerability + severity) and coping assessment (self-efficacy + response efficacy) actually influence protective behaviour.
- **Digital Capital Framework [6]:** This analyzes how the limited or unequal access to certain digital competency creates stratified landscapes for vulnerability.

3. Research Methodology

3.1 Research Design

We will use a mixed-method design described in Figure 1. Here, it initially collects and analyzes quantitative data and later uses qualitative strategies to explain and cite findings.

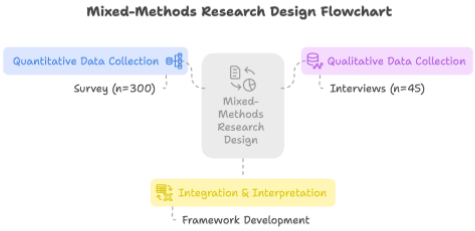

Figure 1. Mixed-Methods Research Design

3.2 Quantitative Phase

3.2.1 Data Collection

I will make a survey form through Google Forms to gather data from over 300 participants. This survey form will be distributed through a variety of leads so that it can guarantee demographic representation. Age groups will be 18-24, 25-34, 25-44, 45+ and geographic locations will be Urban Dhaka, Chittagong and some rural areas.

3.2.2 Questionnaire Design

The questionnaire in the survey will contain four major sections. First there will be demographic information which will ask age, gender, education, occupation and internet usage habits. Secondly, there will be a phishing awareness test with self-reported knowledge (5-points Likert scale) and an actual knowledge test by multiple-choice questions. Thirdly,

security practices evaluation with multiple-response questions about password management and two factor authentication usage. Lastly, I will check the actual phishing detection capabilities by scenarios-based questions presenting mock phishing attempts and trust assessment using semantic differential scales.

3.2.3 Data Analysis

Quantitative analysis will consist of:

- Descriptive statistics to determine awareness levels and security practices
- Inferential statistics (t-tests, ANOVA) to distinguish demographic groups
- Correlation and regression analysis to inspect awareness/practices and detection capabilities relationships
- Factor analysis to determine underlying dimensions of security behaviors

3.3 Qualitative Phase

From the survey respondents I will choose 40-50 individuals to take their consent to participate in in-depth interviews. I will choose to get representation from every perspective of digital literacy levels, demographic groups and phishing history. These structured interviews (20-30 minutes long) will examine personal experience, decision making processes in relation to phishing, attitudes towards security measures.

3.4 Unification of Analysis

In this phase I will unify all the data analyzed to develop:

- A Digital Literacy Spectrum arranging participants by security competency
- A Cultural Vulnerability Framework identifying Bangladesh-specific risk factors
- Recommendations for culturally-adapted security interventions and AI Trust Model explaining adoption barriers

4. Project Timeline and Milestones

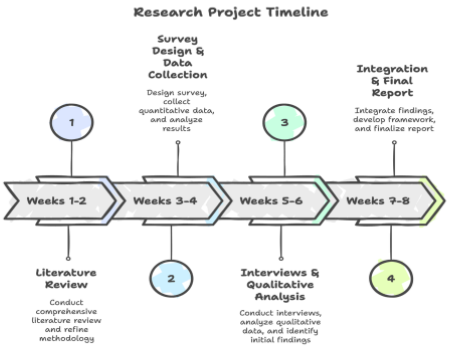

Figure 2. Research Project Timeline (2-Month Duration)

Table 1. Key Project Milestones approximate

Milestone	Deliverable	Timeline
Research Design	Finalized methodology and instruments	End of Week 2
Survey Completion	300+ responses collected and analyzed	End of Week 4
Interviews	40-50 interviews completed	End of Week 6
Data Analysis	Complete quantitative and qualitative analysis	End of Week 6
Framework Development	Cultural vulnerability framework	End of Week 7
Final Report	Complete research report	End of Week 8

5. Expected Implications

5.1 Theoretical Implications

This study will contribute in trying to extend Protection Motivation Theory [5] to non-western contexts and afterall to create a culturally informed Digital Capital Framework [6].

5.2 Practical Applications

The findings will inform:

- Cybersecurity education initiatives in Bangladesh
- Culturally-adapted AI security solution design
- Policy recommendations for digital literacy programs
- Targeted awareness campaigns based on vulnerability profiles

6. Resource Requirements

Google Forms, SPSS For Statistical Analysis, NVivo for qualitative analysis, Equipment to record interviews, Transcription software (paid).

7. Conclusion

This research, in short, fills the critical knowledge gap in phishing awareness and AI defence strategies specially in Bangladesh's digital context. Utilising a mixed-method methodology my research shall construct a holistic framework to improve cybersecurity in this fast-digitizing country. My research will contribute to real-world application of culturally-framed security measures and to theoretical insights into cybersecurity behaviors. My chosen research methodology will allow us to evaluate awareness gaps while examining cultural and behavior factors that are normally neglected by traditional studies. The ultimate framework and policy recommendations will be great inputs to policymakers and educators.

References

[1] World Bank. (2024) Individuals using the internet (% of population) -bangladesh. [Online]. Available: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BD

[2] BGD e-GOV CIRT, "Bangladesh cybersecurity threat report 2023," Bangladesh e-Government Computer Incident Response Team, Dhaka, Bangladesh, Technical Report, 2023, [Online]. Available: https://www.cirt.gov.bd/bangladesh-ct-landscape-2023/.

[3] T. Choudhary, S. Mhapankar, R. Bhddha, A. Kharuk, and R. Patil, "A machine learning approach for phishing attack detection," Journal of artificial intelligence and technology, vol. 3, no. 3, pp. 108–113, 2023.

[4] BASIS Cybersecurity Awareness Taskforce, "Cybersecurity Awareness Survey Report 2023," Bangladesh Association of Software and Information Services, Dhaka, Bangladesh, Aug.2023.[Online].Available:https://basis.org.bd/storage/configuration/basis-cyber-security-awareness-survey-report-2023_1692182015.pdf

[5] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," Journal of Psychology, vol. 91, no. 1, pp. 93-114, 1975.

[6] M. Ragnedda, "Conceptualizing digital capital," Telematics and informatics, vol. 35, no. 8, pp. 2366–2375, 2018.

[7] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," Communications of the ACM, vol. 50, no. 10, pp. 94-100, 2007.

[8] Hoxhunt. Ai phishing attacks: How big is the threat? (+infographic). Hoxhunt. [Online]. Available: https://hoxhunt.com/blog/ai-phishing-attacks. [Accessed: May 5, 2025].

[9] L. Wu, X. Du, and J. Wu, "Effective defense schemes for phishing attacks on mobile computing platforms," IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6678–6691, 2015.

[10] V. Shahrivari, M. M. Darabi, and M. Izadi, "Phishing detection using machine learning techniques," arXiv preprint arXiv:2009.11116, 2020.

[11] R. M. Rodriguez, E. Golob, and S. Xu, "Human cognition through the lens of social engineering cyberattacks," Frontiers in Psychology, vol. 11, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusId:220425567

[12] S. Goel, K. Williams, and E. Dincelli, "Got phished? internet security and human vulnerability," Journal of the Association for Information Systems, vol. 18, no. 1, p. 2, 2017.

[13] S. O. Owiti, P. S. Ogara, and P. A. Rodrigues, "A fraud management framework for mobile financial services within Kenya," EPRA International Journal of Economics, Business

and Management Studies, 2022. [Online]. Available: https://api.semanticsholars.org/CorpusId:255298466

[14] K. Mahmud, M. M. A. Joarder, and K. Muheymin-Us-Sakib, "Adoption factors of fintech: Evidence from an emerging economy country-wide representative sample," International Journal of Financial Studies, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusId:255320837

[15] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, "Don't click: towards an effective anti-phishing training. a comparative literature review," Human- centric Computing and Information Sciences, vol. 10, pp. 1–41, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusId:221084452

[16] H. Le, Q. Pham, D. Sahoo, and S. C. Hoi, "Urlnet: Learning a url representation with deep learning for malicious url detection," arXiv preprint arXiv:1802.03162, 2018.

[17] R. Meléndez, M. Ptaszynski, and F. Masui, "Comparative investigation of traditional machine-learning models and transformer models for phishing email detection," Electronics, 2024. [Online]. Available: https://doi.org/10.3390/electronics13244877

[18] T. Sutter, A. S. Bozkir, B. Gehring, and P. Berlich, "Avoiding the hook: Influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception," IEEE Access, vol. 10, pp. 100 540–100 565, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusId:252339152

Research Proposal_Mridul - Mridul Hasan.pdf

ORIGINALITY REPORT

15%	14%	13%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	arxiv.org Internet Source	2%
2	internationalpubls.com Internet Source	1%
3	par.nsf.gov Internet Source	1%
4	www-emerald-com-443.webvpn.sxu.edu.cn Internet Source	1%
5	thesai.org Internet Source	1%
6	www.hindawi.com Internet Source	1%
7	www.utupub.fi Internet Source	1%
8	Yuxin Zhang, Xingyu Fu, Rong Yang, Yangxi Li. "DRSDetector: Detecting Gambling Websites by Multi-level Feature Fusion", 2023 IEEE Symposium on Computers and Communications (ISCC), 2023 Publication	1%
9	Mohammad Mahmudul Hasan, Fowjia Tajnin Muna. "Technology Trends and Cyber Security in Bangladesh", International Journal of Technology Diffusion, 2022 Publication	1%

10	Mahmuda Khatun, MD Akib Ikbal Mozumder, Md. Nazmul Hasan Polash, Md. Rakib Hasan, Khalil Ahammad, MD. Shibly Shaiham. "An Approach to Detect Phishing Websites with Features Selection Method and Ensemble Learning", International Journal of Advanced Computer Science and Applications, 2022 Publication	1 %
11	Md Mohan Uddin, Khandker Md Nahin Mamun, Abdul Hannan Chowdhury. "Understanding pragmatic meanings of fintech among vulnerable consumers in Bangladesh for enhanced customer experience management", Journal of Financial Services Marketing, 2025 Publication	1 %
12	www.researchgate.net Internet Source	1 %
13	mau.diva-portal.org Internet Source	<1 %
14	wikimili.com Internet Source	<1 %
15	www.semanticscholar.org Internet Source	<1 %
16	Alexandros Kavvadias, Theodore Kotsilieris. "Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review", Applied Sciences, 2025 Publication	<1 %
17	samwell-prod.s3.amazonaws.com Internet Source	<1 %

18	www.oic-cert.org Internet Source	<1%
19	Daniel Aldam. "AI-Powered Phishing: The Current Landscape and Future Projections", XRDS: Crossroads, The ACM Magazine for Students, 2025 Publication	<1%
20	Md. Robiul Islam, Ayesha Siddika, Nahida Shaulin. "chapter 2 AI Readiness and Trust in Government", IGI Global, 2025 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	Off		