OPEN ACCESS

ISSN: 3066-0807

Azra H and Zeeshan I
Int J Teach Learn Sci, 2025(11):1863.139
DOI: 10.71010/3066-0807/ijtls-e139

Research Article

International Journal of Teaching and Learning Sciences

Mathematical Modelling of Social Engineering Attacks in Multilingual Digital Communities: An Educational Framework for Cybersecurity Awareness

Haleema Azra* **and Iffath Zeeshan**

Department of Education, American College of Education, Indianapolis, USA

***Corresponding author:** Haleema Azra*

***Citation:** Azra H and Zeeshan I (2025) Mathematical Modelling of Social Engineering Attacks in Multilingual Digital Communities: An Educational Framework for Cybersecurity Awareness. Int J Teach Learn Sci-IJTLS:e139.*

***Received Date:** 10 October, 2025; **Accepted Date:** 25 October, 2025; **Published Date:** 03 November, 2025*

Abstract

Social engineering attacks exploit human psychology rather than technical vulnerabilities, making them particularly effective across diverse digital communities. This mixed-methods research investigates how language barriers and cultural differences affect susceptibility to cyber threats in multilingual populations through mathematical modelling and statistical analysis. Using surveys, controlled experiments, and longitudinal data collection across three diverse metropolitan areas, this study develops predictive models to understand vulnerability patterns and creates culturally responsive educational frameworks for cybersecurity awareness. The research combines probability theory, statistical modelling, and behavioural analysis to quantify risk factors and protective mechanisms within multilingual digital communities. Findings contribute to both cybersecurity defence strategies and mathematics education by demonstrating real-world applications of statistical analysis in protecting vulnerable populations.

Keywords: social engineering, multilingual communities, mathematical modelling, cybersecurity education, cultural responsiveness, statistical analysis.

1. Introduction

Social engineering attacks represent one of the fastest-growing cybersecurity threats, with attackers increasingly targeting multilingual digital communities through sophisticated manipulation techniques that exploit language barriers, cultural misunderstandings, and trust patterns unique to immigrant and diverse populations [1,2]. Unlike technical attacks that target system vulnerabilities, social engineering exploits human psychology, making traditional cybersecurity measures insufficient for protection.

Multilingual communities face unique vulnerabilities due to language processing differences, cultural communication patterns, and varying levels of digital literacy [3]. However, limited research exists on quantifying these vulnerabilities or developing mathematical models that can predict susceptibility patterns across different linguistic and cultural groups. This gap is particularly concerning given the increasing digitization of essential services and the growing prevalence of targeted attacks on immigrant communities.

2. Research Methodology

The following formatting rules must be followed strictly. This (.doc) document may be used as a template for papers prepared using Microsoft Word. Papers not conforming to these requirements may not be published in the conference proceedings.

2.1. Problem Statement

Current cybersecurity education and awareness programs often fail to address the specific vulnerabilities faced by multilingual digital communities. Most educational materials are developed in English with Western cultural assumptions, potentially leaving non-English speakers and individuals from diverse cultural backgrounds more susceptible to social engineering attacks. Furthermore, there is a lack of quantitative research that models how linguistic and cultural factors interact with psychological manipulation techniques used in social engineering.

2.2. Research Objectives

This study aims to:

1. Quantify vulnerability patterns in multilingual communities through statistical analysis of survey data and experimental result
2. Develop mathematical models that predict susceptibility to social engineering attacks based on linguistic, cultural, and demographic factors
3. Create evidence-based educational frameworks that use mathematical concepts to enhance cybersecurity awareness in diverse communities
4. Design culturally responsive interventions informed by statistical analysis and probability theory

2.3. Research Questions

1. How do language proficiency levels, cultural backgrounds, and demographic factors statistically correlate with susceptibility to different types of social engineering attacks?
2. What mathematical models can effectively predict vulnerability patterns in multilingual digital communities?
3. How can statistical analysis and probability theory be integrated into culturally responsive cybersecurity education programs?
4. What cultural communication patterns and trust mechanisms can be quantified to enhance protection against social engineering?
5. How do multilingual individuals process and respond to security warnings in different languages?

6. What mathematical concepts are most effective for teaching risk assessment and threat recognition to diverse populations?

2.4. Research Design

This study employs a mixed-methods sequential explanatory design, beginning with quantitative data collection through surveys and controlled experiments, followed by qualitative analysis to provide deeper understanding of the quantitative findings. The research is conducted in three phases over 12 months.

Phase 1: Survey data collection and statistical analysis (Months 1-4)

Phase 2: Controlled experiments measuring social engineering susceptibility (Months 5-8)

Phase 3: Development and testing of educational interventions (Months 9-12)

3. Literature Review

3.1 Social Engineering in Cybersecurity

Social engineering attacks manipulate human psychology to obtain confidential information or gain unauthorized access to systems [4]. These attacks often exploit cognitive biases, emotional manipulation, and social dynamics rather than technical vulnerabilities [5]. Research by Hadnagy (2018) [1] identifies key psychological principles used in social engineering, including reciprocity, commitment, social proof, authority, liking, and scarcity.

The effectiveness of social engineering attacks varies significantly across populations, with factors such as age, education level, cultural background, and technology experience influencing susceptibility [6,7]. However, most existing research focuses on homogeneous, primarily English-speaking populations, leaving significant gaps in understanding how these attacks affect multilingual and multicultural communities.

3.2 Multilingual Communities and Cybersecurity

Limited research exists on cybersecurity challenges specific to multilingual populations. Chen and Zahedi (2016) [3] found that non-native English speakers demonstrated different patterns of email threat detection compared to native speakers, suggesting that language processing affects security decision-making. Similarly, research by Alsharnouby et al. (2015) [8] indicated that cultural factors influence password creation behaviors and security practice adoption.

Multilingual individuals often code-switch between languages depending on context, which may affect their ability to recognize social engineering attempts that exploit linguistic cues [9]. Additionally, cultural differences in authority perception, trust mechanisms, and communication styles may create unique vulnerabilities that are not addressed by mainstream cybersecurity education.

3.3 Mathematical Modelling in Cybersecurity

Mathematical modelling has been increasingly applied to cybersecurity challenges, particularly in areas such as risk assessment, threat prediction, and security investment optimization [10,11]. Statistical models have been used to analyse attack patterns, predict system vulnerabilities, and evaluate the effectiveness of security measures [12].

However, mathematical modelling of human factors in cybersecurity, particularly social engineering susceptibility, remains underdeveloped. Most existing models focus on technical vulnerabilities rather than human psychological and cultural factors that influence security behaviors [13].

3.4 Culturally Responsive Cybersecurity Education

Traditional cybersecurity education often employs one-size-fits-all approaches that may not effectively serve diverse populations [14]. Culturally responsive education principles, originally developed for general education contexts [15], suggest that effective instruction must acknowledge and build upon students' cultural backgrounds and linguistic resources.

Recent research has begun exploring culturally responsive approaches to cybersecurity education, with studies indicating that culturally relevant examples and multilingual materials can enhance learning outcomes [16]. Technology integration has also shown promise in mathematics education, with Zeeshan (2024) [17] demonstrating that incorporating technology and hands-on activities significantly improves student understanding and engagement in algebra. Similarly, Singh and Zeeshan (2025) [18] found that augmented reality (AR) and virtual reality (VR) applications in special education math instruction provide enhanced learning experiences for diverse learners.

The effectiveness of growth mindset strategies in improving mathematical performance has been demonstrated across diverse student populations, with Zeeshan (2025) [19] finding significant improvements in middle school students' mathematics performance in Georgia when growth mindset interventions were implemented. Additionally, Azra (2025) [20] showed that digital visualization tools significantly enhance understanding of non-linear functions in advanced algebra through mixed-methods research in Georgia schools, suggesting that technology-enhanced approaches can improve comprehension of complex mathematical concepts.

However, limited research exists on integrating mathematical concepts into culturally responsive cybersecurity curricula. The intersection of technology, cultural responsiveness, and mathematics education presents opportunities for innovative approaches to cybersecurity awareness, particularly given the demonstrated effectiveness of both mindset interventions and digital tools in mathematics learning.

4. Data Analysis

4.1 Participants and Settings

The study is conducted in one diverse metropolitan area (Atlanta, GA) with data collection at three different community sites within the city. This location was selected for its significant multilingual population and established partnerships with community organizations.

Target Population:

- Adults aged 18-65 residing in multilingual communities in Atlanta, GA
- Minimum 50% non-native English speakers
- Representation from at least 6 different language groups
- Varied socioeconomic and educational backgrounds

Sample Size Calculation: Based on power analysis (α = 0.05, β = 0.20, effect size = 0.3) and resource constraints, the target sample size is:

- **Phase 1 Survey:** 120 participants (40 per location)
- **Phase 2 Experiments:** 60 participants (20 per location)
- **Phase 3 Educational Intervention:** 30 participants (10 per location)

4.2 Phase 1: Survey Data Collection

4.2.1. Survey Development

The Multilingual Cybersecurity Vulnerability Assessment (MCVA) survey is developed through an iterative process involving cybersecurity experts, linguists, and community representatives. The survey is translated into 6 languages (Spanish, Korean, Arabic, Hindi, Mandarin, and Somali) using back-translation methodology to ensure accuracy and cultural appropriateness.

4.2.2. Survey Sections

Section A focuses on demographic and linguistic profiling to establish baseline characteristics of participants. This section captures age, gender, education level, and income range to provide essential demographic context for the mathematical modelling components of the study. The linguistic elements include documentation of primary and secondary languages spoken by participants, along with self-assessed English proficiency across four domains: speaking, reading, writing, and listening. Additionally, this section records years of residence in the current country and incorporates technology usage patterns alongside digital literacy self-assessments, both of which are likely to correlate with cybersecurity vulnerability levels and will be crucial variables in the predictive models.

Section B addresses cultural background assessment, which forms the theoretical foundation for understanding how cultural factors influence social engineering susceptibility. This section documents participants' country or region of origin and attempts to measure cultural values orientation across key dimensions including collectivism versus individualism, power distance, and uncertainty avoidance. The section also explores trust patterns and authority perception, which are expected to correlate strongly with susceptibility to authority-based social engineering attacks. Communication style preferences and community engagement patterns are assessed to understand social network characteristics that may either protect against or increase vulnerability to community-based manipulation tactics.

Section C evaluates cybersecurity knowledge and awareness through multiple assessment approaches. A twenty-question multiple-choice assessment measures general cybersecurity knowledge, though this length may present completion challenges for some participants. The section also assesses familiarity with common attack types, documents any previous cybersecurity training or education participants may have received, and identifies their primary sources of cybersecurity information. Additionally, this section captures participants' perceived cybersecurity threats and concerns, which may reveal cultural or linguistic biases in threat recognition that could inform the educational intervention development.

Section D represents the core vulnerability assessment component, focusing on social engineering susceptibility indicators through multiple measurement approaches. Participants respond to fifteen hypothetical social engineering scenarios distributed across five different attack types, though the reliance on hypothetical scenarios may not perfectly predict real-world behavior. The section includes risk perception assessments for various online activities and measures trust indicators in digital communications. Decision-making processes for suspicious requests are documented alongside help-seeking behaviors when participants encounter uncertainty about digital security, providing insight into cultural patterns of information-seeking and community support utilization.

Section E assesses mathematical and statistical literacy, which is essential for both the research's analytical components and the development of the educational framework. This section includes basic probability and statistics knowledge assessment, though care must be taken to avoid mathematical anxiety that could affect participation rates. The section measures participants' comfort levels with numerical risk information and documents their preferences for different risk communication formats. Previous mathematics education background is also recorded, providing context for understanding participants' capacity to engage with the mathematical modelling concepts that will be integrated into the culturally responsive cybersecurity education interventions.

4.2.3 Survey Administration

Surveys are administered through multiple channels to maximize participation and representativeness:

Online platform (available in 6 languages with audio support)

Community centers with bilingual research assistants

Religious and cultural organizations through partnership agreements

Adult education programs in collaboration with local institutions

4.3 Phase 2: Controlled Experiments

4.3.1 Experimental Design

A series of controlled experiments measure actual susceptibility to social engineering attacks across different linguistic and cultural groups. The experiments use simulated attack scenarios in controlled laboratory settings with full ethical approval and informed consent.

4.3.2 Experimental Conditions

Language Condition Variables encompass three distinct approaches to examining how linguistic factors influence social engineering susceptibility. The comparison between native language and English communication provides a fundamental baseline for understanding language processing effects on threat recognition, though implementation requires authentic translation that preserves cultural nuances rather than literal conversions that may distort meaning. High proficiency versus low proficiency English scenarios attempt to isolate the role of language competency, but this distinction may oversimplify the complex relationship between proficiency levels and cognitive load during threat assessment, particularly since proficiency can vary significantly across different domains such as technical vocabulary, conversational fluency, and written comprehension. Code-switching scenarios represent an innovative approach that acknowledges authentic multilingual communication patterns, but they introduce substantial complexity in terms of experimental control and interpretation, as code-switching behaviors are highly individualized and culturally specific, meaning that some participants may find mixed-language communications natural while others experience them as confusing or artificial.

Cultural Context Variables attempt to operationalize theoretical frameworks about how cultural background influences vulnerability to different manipulation strategies. Authority-based appeals that vary cultural authority figures require extensive cultural knowledge and community consultation to avoid stereotyping while ensuring that the selected figures are genuinely recognized and respected within specific cultural contexts, though the diversity within cultural groups may make universal authority figures difficult to identify. Community-based appeals that distinguish between in-group and out-group sources assume participants have clear, stable cultural identities, but many individuals in multilingual communities navigate multiple, overlapping group affiliations that complicate simple binary categorizations of insider versus outsider status. Urgency and scarcity appeals adapted for different cultural contexts present significant risks of reinforcing cultural stereotypes if not developed through extensive community engagement and cultural competency, while the adaptation process itself may introduce confounding variables that obscure the cultural factors being investigated.

Attack Type Variables reflect realistic threat scenarios but present substantial methodological and ethical challenges for experimental implementation. Phishing emails with cultural and linguistic targeting require careful balance between experimental authenticity and ethical considerations, as overly specific cultural references could perpetuate harmful stereotypes or cause genuine distress to participants who may recognize realistic elements from their own community experiences. Voice-based social engineering in multiple languages demands significant resources for authentic implementation and raises complex questions about speaker selection, accent authenticity, cultural appropriateness, and standardization across different phonetic and prosodic systems, while ensuring that voice actors can deliver convincing performances without inadvertently introducing cultural biases. Text message attacks incorporating cultural references need extensive development to maintain experimental validity while avoiding the reinforcement of cultural assumptions or biases that could compromise both the research integrity and participant wellbeing. Social media manipulation across platforms popular in different communities introduces technological variables that may overshadow the cultural and linguistic factors central to your research, particularly given the rapid evolution of social media platforms and their varying adoption patterns across demographic and cultural groups, potentially creating confounding effects that complicate data interpretation and limit the generalizability of your findings.

4.3.3 Experimental Measures

The Primary Measures present a structured approach to quantifying social engineering susceptibility, but several methodological concerns warrant consideration. The binary classification of responses as high risk versus low risk may oversimplify the complexity of threat assessment behaviors, particularly when participants from different cultural backgrounds may demonstrate varying risk tolerance levels that don't align neatly with binary categorizations. Time to recognition of threat as a continuous measure provides valuable data about cognitive processing speed, but this metric assumes that faster recognition necessarily indicates better threat detection, which may not hold true across all cultural contexts where deliberate, careful consideration might be culturally valued over rapid decision-making. The confidence assessment using a five-point Likert scale may suffer from cultural response bias, as some cultures discourage expressions of high confidence while others may demonstrate confidence even when uncertain, potentially confounding the relationship between actual threat recognition ability and reported confidence levels. Information disclosure level as an ordinal measure from none to partial to complete provides useful data about behavioral outcomes, but the distinction between partial and complete disclosure may be difficult to standardize across different types of social engineering scenarios and cultural contexts where information sharing norms vary significantly.

Secondary Measures involving verbal reasoning patterns during think-aloud protocols and decision-making processes influenced by cultural factors offer rich qualitative data but introduce substantial analytical complexity. Think-aloud protocols may be culturally biased toward participants comfortable with verbal self-reflection and may disadvantage those from cultures where internal processing is preferred over external verbalization, potentially skewing results toward certain cultural groups. The documentation of decision-making processes and cultural influences requires trained researchers capable of recognizing subtle cultural cues and patterns, which may be challenging to achieve consistently across different cultural backgrounds represented in your study. Additionally, the language in which participants conduct their think-aloud protocols may influence their reasoning patterns, creating confounding effects between linguistic and cultural variables that could complicate interpretation of your findings and limit the validity of cross-cultural comparisons within your experimental design.

4.4 Phase 3: Educational Intervention Development and Testing

The intervention design, informed by findings from Phase 1 and Phase 2, focuses on creating culturally responsive educational strategies that merge mathematical modelling concepts with cybersecurity awareness through community based participatory design principles. Key mathematical components include probability and risk assessment techniques such as basic probability, Bayes' theorem, and decision trees; statistical analysis and pattern recognition using descriptive statistics, correlation analysis, and regression modelling; and data visualization to create and interpret graphs reflecting cybersecurity trends. To enhance cultural responsiveness, the interventions will feature language integration through materials available in participants' primary languages, culturally relevant examples, and community specific communication patterns. Furthermore, they will incorporate cultural context by utilizing examples from participants' experiences, embedding cultural values, and recognizing diverse approaches to authority. Community engagement will be fostered through peer education models with local instructors, collaboration with existing community organizations, and development of tailored threat awareness campaigns.

4.5 Data Analysis Plan

The quantitative analysis component encompasses both descriptive and inferential statistics to gain insights into the demographic and linguistic characteristics of the sample, the distribution of cybersecurity knowledge, and vulnerability scores. Descriptive statistics will include cross tabulation of cultural factors with security behaviors, while inferential statistics will employ multiple regression analysis to identify predictors of social engineering susceptibility, ANOVA to compare vulnerability levels across different linguistic and cultural groups, and chi-square tests to explore categorical relationships between variables. Additionally, mathematical modelling techniques such as logistic regression will be developed to predict social engineering susceptibility, along with hierarchical linear modelling to account for community level effects. Advanced machine learning approaches, including random forest and neural networks, will be utilized for identifying complex patterns. Model validation efforts will include cross-validation techniques to assess generalizability, ROC curve analysis for examining model discrimination ability, and calibration plots to evaluate the accuracy of predictions.

Complementing the quantitative analysis, qualitative analysis will utilize thematic analysis to code open-ended survey responses and interview data, leading to the development of themes that elucidate cultural factors impacting cybersecurity behaviors. This will integrate qualitative findings with quantitative models for a comprehensive understanding. Additionally, content analysis will examine think aloud protocols during experimental tasks, revealing reasoning patterns across various linguistic groups and identifying cultural scripts that influence threat assessment. This dual approach of quantitative and qualitative analyses will provide a robust framework for understanding the complexities of cybersecurity behaviors within diverse cultural contexts.

5. Ethical Considerations

This research involves potential deception through simulated social engineering attacks and collection of sensitive information about vulnerability to cyber threats, necessitating comprehensive ethical protocols to protect participants and communities. Informed consent procedures include full disclosure of research purposes and procedures, clear explanation of simulated attack scenarios and their educational purpose, and explicit acknowledgment of participants' right to withdraw at any time without penalty. Privacy protection measures encompass de-identification of all survey and experimental data, secure storage of data with encryption and access controls, and destruction of identifying information after analysis completion to prevent any potential harm from data breaches or misuse. Risk mitigation strategies involve conducting debriefing sessions after all experimental procedures to address any concerns or psychological impacts, providing cybersecurity education materials to all participants to ensure they benefit from their involvement, and connecting participants with community resources for ongoing cybersecurity support beyond the study period. Cultural sensitivity considerations include collaboration with community advisory boards to ensure research approaches are appropriate and respectful, training of research staff in cultural competency to facilitate meaningful engagement with diverse participants, and ongoing consultation with community representatives throughout the study to address emerging concerns and maintain community trust and support.

6. Expected Results and Mathematical Models

6.1 Anticipated Survey Findings

Based on preliminary literature review and pilot testing, we expect the following patterns to emerge from survey data:

Language Proficiency Effects:
Lower English proficiency correlates with higher susceptibility to English language social engineering attempts.
Native language attacks may show different vulnerability patterns.
Code switching scenarios may create unique vulnerability windows.

Cultural Factors:
High power distance cultures may show greater susceptibility to authority based attacks
Collectivist cultures may be more vulnerable to social proof manipulation
Community trust patterns may both protect against and increase vulnerability to certain attack types

6.2 Proposed Mathematical Models

6.2.1 Primary Vulnerability Prediction Model

Logistic Regression Model:
$\log(p/(1-p)) = \beta_0 + \beta_1(\text{Language Proficiency}) + \beta_2(\text{Cultural Orientation}) + \beta_3(\text{Digital Literacy}) + \beta_4(\text{Education Level}) + \beta_5(\text{Age}) + \beta_6(\text{Time in Country}) + \beta_7(\text{Community Integration}) + \varepsilon$
Where:
p = probability of falling for social engineering attack
Language Proficiency = standardized English proficiency score
Cultural Orientation = composite score of cultural values assessment
Digital Literacy = technology skills and knowledge score
Education Level = years of formal education
Age = participant age
Time in Country = years residing in current country
Community Integration = social network and community engagement score

6.2.2 Attack-Specific Models

Authority-Based Attack Model:
$P\ (\text{Authority Attack Success}) = 1/(1 + e\text{^}(-(\alpha + \beta_1{*}\text{Power Distance} + \beta_2{*}\text{English Prof} + \beta_3{*}\text{Authority Experience})))$
Community-Based Attack Model:
$P\ (\text{Community Attack Success}) = 1/(1 + e\text{^}(-(\alpha + \beta_1{*}\text{Collectivism Score} + \beta_2{*}\text{Community Trust} + \beta_3{*}\text{Social Network Size})))$

6.2.3 Risk Assessment Framework

Individual Risk Score:
Risk Score = Σ(Attack Type Probability × Attack Type Impact × Exposure Frequency)
Community Vulnerability Index:
CVI = (Σ Individual Risk Scores / N) × Community Cohesion Factor × Resource Availability Factor

6.3 Expected Model Performance

Based on pilot data and similar research in related fields, with our focused sample size, we anticipate:
Overall model accuracy: 70-80% for primary vulnerability prediction
Sensitivity: 75-85% for identifying high-risk individuals
Specificity: 65-75% for correctly identifying low-risk individuals
Area under ROC curve: 0.75-0.85 indicating good to excellent discrimination

6.4 Educational Framework Development

The educational framework integrates essential mathematical concepts that emerged as most relevant from the research findings, focusing on probability and risk assessment alongside statistical analysis and pattern recognition. In probability and risk assessment, learning objectives include understanding basic probability concepts as applied to cybersecurity threats, calculating and interpreting risk levels for different online activities, and using conditional probability to update threat assessments through culturally responsive activities such as calculating probability of scams targeting specific cultural communities, analyzing statistical patterns in attacks on multilingual populations, and using community specific data to understand local threat landscapes. Statistical analysis and pattern recognition components emphasize learning objectives that help participants recognize patterns in cybersecurity data and personal digital behavior, interpret statistical representations of cybersecurity threats, and use descriptive statistics to analyze personal risk factors through activities including analyzing cybersecurity survey data from participants' own communities, creating visualizations showing threat trends affecting multilingual populations, and comparing statistical patterns across different cultural groups.

The instructional design principles emphasize culturally sustaining pedagogy through language integration that teaches mathematical concepts in participants' primary languages initially with gradual transition to technical English terms while maintaining native language support and providing peer translation opportunities, cultural relevance that draws mathematical examples from participants' cultural experiences while integrating traditional mathematical practices and recognizing diverse approaches to numerical reasoning, and community connection through local data usage, integration with existing networks, and peer educator model development. Active learning strategies incorporate hands-on mathematical modelling where participants create vulnerability assessment models and work in small groups on statistical analysis, combined with real world applications including analysis of actual cybersecurity incidents and development of personal risk assessment tools. Assessment and evaluation frameworks measure learning outcomes through mathematical knowledge assessments of probability and statistics concepts, cybersecurity awareness improvements in threat recognition and risk assessment decision-making, and cultural integration maintenance while gaining security knowledge. Program effectiveness evaluation employs quantitative measures such as reduced experimental social engineering susceptibility scores and improved cybersecurity knowledge assessments, alongside qualitative measures including participant feedback on cultural responsiveness, community member reports of behavior change, and instructor observations of engagement and learning.

6.5 Implications and Applications

This research makes significant theoretical contributions across multiple disciplines by providing the first comprehensive mathematical modelling of social engineering vulnerability in multilingual populations and developing culturally responsive frameworks for understanding cyber threats through the integration of linguistic and cultural factors into quantitative security models. In mathematics education, the study demonstrates real-world applications of statistical analysis and probability theory while developing culturally sustaining approaches to applied mathematics education and providing evidence for the effectiveness of community based mathematical learning. For cultural and linguistic studies, the research offers quantitative analysis of how language and culture affect digital security behaviors, mathematical modelling of cultural communication patterns and trust mechanisms, and evidence-based approaches to serving multilingual communities in technical education. The practical applications span multiple sectors, beginning with the cybersecurity industry where the research provides improved understanding of human factors affecting diverse populations, development of more effective security awareness programs, and enhanced threat intelligence considering linguistic and cultural factors. In the education sector, contributions include culturally responsive curricula for cybersecurity and mathematics education, professional development frameworks for educators serving multilingual communities, and integration of real-world applications into mathematics instruction. Community organizations benefit from evidence-based approaches to cybersecurity awareness in multilingual communities, mathematical tools for assessing and communicating community vulnerability, and frameworks for developing culturally appropriate security education programs. Policy implications extend to national security through better understanding of vulnerabilities in multilingual populations and evidence based approaches to community level cybersecurity resilience, immigration and integration services that incorporate cybersecurity support as a component of immigrant integration, and digital equity initiatives that integrate cybersecurity considerations into digital inclusion efforts while recognizing language and cultural barriers to effective cybersecurity and developing multilingual and multicultural cybersecurity resources.

7. Limitations and Future Research

7.1 Study Limitations

This study acknowledges several important limitations that may affect the interpretation and application of findings. Generalizability concerns include the potential that findings may not apply to all multilingual communities or geographic regions outside Atlanta, as the smaller sample size limits statistical power for detecting small effect sizes and the single city focus may not reflect the diversity of multilingual community experiences nationwide. Methodological limitations present additional challenges, as self reported data may include bias and social desirability effects, experimental scenarios may not fully capture the complexity of real world social engineering attacks, and the cross-sectional design limits understanding of long-term vulnerability changes over time. Cultural and linguistic constraints further impact the research scope, since translation and cultural adaptation processes may not capture all cultural nuances, research team cultural competency levels may affect data interpretation accuracy, and community engagement levels may vary significantly across different cultural groups, potentially influencing participation rates and response quality across the study population.

7.2 Future Research Directions

Future research directions encompass four key areas that build upon current cybersecurity education foundations. Longitudinal studies will focus on long term tracking of cybersecurity behavior changes following educational interventions, analysis of how vulnerability patterns evolve with increased time in host countries, and examination of intergenerational differences in cybersecurity knowledge and behavior among diverse populations. Expanded population studies will broaden the research scope through investigation of additional language groups and cultural communities, comparative analysis of urban versus rural multilingual community vulnerabilities, and focused investigation of age specific patterns in multilingual cybersecurity education effectiveness. Advanced modelling approaches will leverage cutting edge methodologies including machine learning and artificial intelligence applications for vulnerability prediction, network analysis of social engineering spread through multilingual communities, and development of real time risk assessment tools specifically designed for diverse populations. Finally, technology integration initiatives will drive innovation through mobile application development for culturally responsive cybersecurity education, implementation of virtual reality and simulation-based training programs tailored for multilingual populations, and integration of natural language processing technologies for enhanced multilingual threat detection capabilities.

8. Conclusions

This research addresses a critical gap in cybersecurity protection for increasingly diverse digital communities while advancing mathematics education through real world application of statistical analysis and modelling. By quantifying vulnerability patterns in multilingual populations and developing culturally responsive educational frameworks, this study contributes to both academic understanding and practical protection of vulnerable communities.

The integration of mathematical modelling with cultural responsiveness represents an innovative approach that recognizes diversity as both a challenge requiring protection and an asset contributing to more robust cybersecurity understanding. The expected outcomes include not only improved protection for multilingual communities but also enhanced mathematics education that demonstrates the relevance and power of statistical thinking in addressing contemporary social challenges.

As our digital world becomes increasingly interconnected and our communities become more diverse, research that bridges cultural understanding with technical protection becomes essential. This study provides a foundation for developing more inclusive, effective, and mathematically grounded approaches to cybersecurity education and protection.

The findings will inform cybersecurity professionals, educators, policymakers, and community organizations working to create more secure and equitable digital experiences for all populations. Through careful mathematical analysis and culturally responsive design, this research contributes to building stronger, more inclusive defenses against the human centered threats that increasingly define our cybersecurity landscape.

Acknowledgements

The authors would like to thank everyone, just everyone!

References

1. C. Hadnagy, *Social engineering: The science of human hacking*. Wiley, 2018.
2. F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Comput. Secur.*, vol. 59, pp. 186–209, 2016, doi: 10.1016/j.cose.2016.02.008.
3. Y. Chen and F. M. Zahedi, "Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China," *MIS Q.*, vol. 40, no. 1, pp. 205–222, 2016, doi: 10.25300/MISQ/2016/40.1.09.
4. K. D. Mitnick and W. L. Simon, *the art of deception: Controlling the human element of security*. Wiley, 2002.
5. R. B. Cialdini, *Influence: The psychology of persuasion*. Harper Business, 2006.
6. S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2010, pp. 373–382, doi: 10.1145/1753326.1753383.
7. P. Kumaraguru et al., "Protecting people from phishing: The design and evaluation of an embedded training email system," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2007, pp. 905–914, doi: 10.1145/1240624.1240760.
8. M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing emails," *Int. J. Hum.-Comput. Stud.*, vol. 82, pp. 69–82, 2015, doi: 10.1016/j.ijhcs.2015.05.005.
9. O. García and L. Wei, *Translanguaging: Language, bilingualism and education*. Palgrave Macmillan, 2014.
10. L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002, doi: 10.1145/581271.581274.
11. K. Hausken, "Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability," *Inf. Syst. Front.*, vol. 8, no. 5, pp. 338–349, 2006, doi: 10.1007/s10796-006-9003-4.
12. T. Alpcan and T. Başar, *Network security: A decision and game-theoretic approach*. Cambridge University Press, 2010.
13. A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: Managing security behaviour in organisations," in *Proc. 2008 New Secur. Paradigms Workshop*, 2008, pp. 47–58, doi: 10.1145/1595676.1595684.
14. V. Zimmermann and K. Renaud, "Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset," *Int. J. Hum.-Comput. Stud.*, vol. 131, pp. 169–187, 2019, doi: 10.1016/j.ijhcs.2019.05.005.
15. G. Gay, *Culturally responsive teaching: Theory, research, and practice*, 3rd ed. Teachers College Press, 2018.
16. M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" in *Int. Conf. Cyber Secur. Sustain. Soc.*, 2019, pp. 118–131.
17. I. Zeeshan, "The impact of integrating technology and hands-on activities on student understanding and engagement in algebra," *Int. J. Soc. Sci. Manag. Stud.*, vol. 10, no. 11, 2024.
18. S. Singh and I. Zeeshan, "The impact of augmented reality (AR) and virtual reality (VR) in special education math instruction: A systematic review," *Int. J. Sci. Res. Arch.*, vol. 14, no. 3, 2025, doi: 10.30574/ijsra.2025.14.3.0744.
19. I. Zeeshan, "The effect of digital visualization tools on understanding of non-linear functions in advanced algebra: A mixed methods study in Georgia schools, USA," *Eur. J. Educ. Pedagogy*, 2025, doi: 10.24018/ejedu.2025.6.5.991.
20. H. Azra, "The effect of digital visualization tools on understanding of non-linear functions in advanced algebra: A mixed methods study in Georgia schools, USA," *Eur. J. Educ. Pedagogy*, 2025, doi: 10.24018/ejedu.2025.6.5.991.
21. A. Bandura, *Social foundations of thought and action: A social cognitive theory*. Prentice Hall, 1986.
22. P. Slovic, "Perception of risk," *Science*, vol. 236, no. 4799, pp. 280–285, 1987, doi: 10.1126/science.3563507.

23. H. Azra and I. Zeeshan, "Harnessing big data analytics in education: Balancing student success with privacy concerns and ethical considerations in Greenfield University in USA (pseudonym)," *Comput. Sci. Inf. Technol.*, vol. 15, no. 6, art. 09, 2025, doi: 10.5121/csit.2025.150609.
24. L. S. Vygotsky, *Mind in society: The development of higher psychological processes*. Harvard University Press, 1978.
25. I. Zeeshan, "Examining the effects of growth mindset strategies on middle school students' performance in mathematics in Georgia, USA," *Eur. J. Educ. Pedagogy*, 2025, doi: 10.24018/ejedu.2025.6.5.990.