Int.J.HIT.TRANSC:ECCN.Vol.9: Issue 1A (2023) Page 29-44 ISSN: 0973-6875

Available Online at www.hithaldia.in/locate/ECCN
All Rights Reserved

ORIGINAL CONTRIBUTION

Cybersecurity Literacy Programs for Marginalized Communities: Bridging the Gap in Digital Security

[a]Ankita Ghosh, [b]Sudip Diyasi and [c]Dipankar Dey

[a,b]*Department of Computer Application, George College of Management and Science, Kolkata, West Bengal, India*

[c]*Department of Computer Application, Global Institute of Science & Technology, Haldia, West Bengal, India*

ABSTRACT

Marginalized communities, especially in low-income and rural areas, are highly vulnerable to cyberattacks because of low digital literacy, limited economic advantages, and scarce resources for cybersecurity. This paper examines the role of socio-economic factors influencing cybersecurity risks in these populations, as well as investigates the efficiency of digital literacy programs. Using logistic regression analysis, it was established that a lower income level, rural location, and low levels of digital literacy significantly increased the likelihood that a given population group experience cyber incidents. Other analyses of cybersecurity literacy programs such as Cyber Safe for All in Kenya and PMGDISHA in India conclude that culturally relevant and localized approaches are more effective in raising cybersecurity awareness than generic approaches and diluted methodologies. Based on such analyses, we present an integration framework that can better improve security resilience in targeted vulnerable communities. That would require investment in appropriately tailored digital literacy initiatives, both in terms of public-private partnerships and policy design tailored to those needs. The future work should be longitudinal research studies that determine the longer-run effects of such efforts and probe various opportunities available for drawing on emerging technologies to expand access to cybersecurity education. This means empowering these groups in their own efforts to combat unique challenges that their groups face while trying to alleviate and eventually bridge the digital divide.

KEY WORDS: Cybersecurity Literacy; Digital Inclusion; Marginalized Communities; Socio-economic Barriers; Cybersecurity Education Programs.

1. INTRODUCTION

In the early years of the 21st century, when information and communication technologies spread worldwide, people began to contact, communicate, and engage in business in an entirely new way. This opened avenues that were previously inaccessible for economic, educational, and social development, through access to the Internet, bringing about digital inroads with new avenues for economic, educational, and social risks to the very same areas for marginalized communities. These population-increases so often marked by a past of low-income status, low education access, and infrastructure access-even more than often-for lack of awareness and assets to protect against cyber threats. Without the skills required to identify and combat dangers in phishing attacks, malware, identity theft or other forms of cybercrime, the fruits of digital inclusion are lost on targeted groups.

As access continues to narrow the global digital divide, a new kind of inequity appears: the cybersecurity literacy gap. The marginalized communities gain access to digital tools but lack basic knowledge and skills to protect themselves in that environment. Such a gap will have far-reaching consequences, from theft of personal data to financial fraud, and is likely to entrench further social inequalities by discouraging such communities from wholly participating in the digital economy. Cybersecurity education, then, becomes all-important as a crucial part of the type of digital literacy initiatives undertaken to fully empower these populations.

**Corresponding Address:*
Doi: 10.5281/zenodo.14740268

1.1 The Importance of Cybersecurity for Marginalized Communities

Cybersecurity literacy is important for everyone who uses the internet, and assumes a much more critical role for these communities mentioned above:

- Economic Vulnerability: The real economic impact falls on the most open citizens from a lower-income background. For example, a small-scale entrepreneur in a developing community whose access to online business or banking information has been lost due to a cyber-attack will most probably experience financial destruction.

- Limited Access to Support: Generally, members of marginalized groups have little technical support services, legal recourse, or insurance safeguards that can save them from cyber-attacks. Therefore, the impact of this cyber-attack is much more disastrous compared to that of better-off, digitally literate groups that could seek professional help.

- Exploitation by Cybercriminals: Cybercriminals often target low-literacy users through deceptive tactics like phishing, scamming, and spreading misinformation. These attacks target the unsuspecting ones because one has no idea about the best cybersecurity practices.

Toward this end, numerous cybersecurity literacy programs already exist in most countries in the world and aim at empowering marginalized communities with the knowledge and skills they would use to protect themselves online. Programs are usually directed towards poor families, rural inhabitants, senior citizens, and ethnic minorities who are already more excluded from participating in the digital sphere and are less aware of their security concerns.

1.2 The Digital Inclusion Paradox

In depressed areas, the best global efforts have focused on internet access, with no mind to the problems of cybersecurity that this digital inclusion brings. In this sense, it can be termed the paradox of digital inclusion: as the internet becomes the key tool reaching out to more communities, it exposes those communities to risks that it may bring about without the needed tools for defense. This is particularly concerning in developing countries, where efforts for digital inclusion often prioritize connectivity over security education.

Online and mobile internet access has exponentially increased in most areas of rural sub-Saharan Africa where online banking, e-commerce, and education services are available. The primary cause attributing to the rise in cases of mobile money frauds, identity theft, and unauthorized data collection is a deficit in information about cybersecurity in such communities. Similar trends are found in Latin America and South Asia, in which new Internet users are largely ignorant of the most basic principles of safe Internet use, making them easy prey to cybercrooks.

1.3 Objectives of the Study

This paper will try to shed some light on how such programs may prove instrumental in helping close the continually widening gap in digital security, and how that gap is particularly growing wider yet for marginalized groups [1]. Questions include:

- What are the specific cybersecurity challenges faced by marginalized populations, and how do these challenges differ from those faced by more digitally literate groups?

- What existing cybersecurity literacy programs are in place, and how effective are they in reducing cyber threats in these communities?

- How can scalable, data-driven cybersecurity education programs be developed and implemented globally to ensure both digital inclusion and security?

1.4 Structure of the Paper

Therefore, the paper is divided into: Section 2: this constitutes a literature review of the concepts of digital inclusion, cybersecurity risks, and contemporary cybersecurity literacy programs. Section 3: this briefly describes the

methodology adopted to carry out the study; datasets plus analytical methods used. Results of Quantitative and Qualitative Analyses Since results are presented in Section 4, the analyses embrace the both quantitative and qualitative impacts of cybersecurity literacy on cyber incident rates. In Section 5, implications of the research shall be discussed, complete with recommendations for scaling cybersecurity education efforts. The paper shall end by summarizing key insights and future directions for further research.

2. Literature Review

Research on cybersecurity literacy, digital inclusion, and challenges for marginalized populations spans multiple fields, including education, technology, public policy, and development studies. This paper synthesizes insights from existing studies in three key areas: the state of cybersecurity literacy programs, the impact of digital inclusion on cybersecurity risks, and challenges unique to marginalized communities.

2.1 Digital Inclusion and Cybersecurity Risks

In the last two decades, digital inclusion has been a priority in global development, with initiatives by the United Nations, World Bank, and other organizations working to bridge the digital divide and extend digital benefits to underserved communities [2]. These initiatives aim to promote equitable access to digital resources, the digital economy, and improved quality of life [2]. However, increased digital access also exposes marginalized groups to cybersecurity risks.

Gwagwa et al. (2020) describe this as a "double-edged sword," where communities gain internet access yet face heightened vulnerability to cyber threats [3]. Reports from OECD (2022) and Kaspersky Lab (2021) further highlight phishing, malware, and identity theft as significant risks for these populations, who often lack foundational cybersecurity knowledge [4][5].

Empirical research confirms that low digital literacy contributes to cyber vulnerabilities in marginalized communities. For example, Chen and Wellman (2021) found that low digital literacy in rural Asia increased susceptibility to cyber threats among newly connected users [6]. Lopez (2022) observed similar vulnerabilities among low-income groups in Africa and Latin America due to low digital literacy [7].

Key Insights:

- Correlation between low digital literacy and increased cybersecurity risks: Limited knowledge of cybersecurity best practices among previously excluded groups now gaining digital access often results in higher cyber incident rates.
- Inequitable cyber resilience: Limited access to cybersecurity tools leaves marginalized communities vulnerable, as they lack both resources and awareness.

2.2 Community Informatics and Cybersecurity Literacy

Community informatics (CI) focuses on how ICTs foster social inclusion, equity, and empowerment among marginalized groups [8]. CI has evolved beyond digital access to address digital literacy and, increasingly, cybersecurity education, tackling what Gwagwa et al. (2020) and Chen & Wellman (2021) describe as a "digital safety gap" [3][6]. This gap exposes newly connected users to online risks without adequate cybersecurity knowledge.

Targeted cybersecurity education programs are essential to mitigate cyber risks for vulnerable populations. Initiatives like CyberSafe for All in Kenya and PMGDISHA in India demonstrate the effectiveness of culturally relevant, community-based cybersecurity training. For example, Ngugi et al. (2021) observed a 40% reduction in phishing incidents among CyberSafe participants, highlighting the value of tailored approaches in building cyber resilience [9].

Key Insights:

- Integrating cybersecurity literacy within CI frameworks enables marginalized communities to engage safely online, supporting broader goals of digital equity.

2.3 Challenges Faced by Marginalized Communities in Cybersecurity

Marginalized groups face unique cybersecurity challenges stemming from socio-economic, infrastructural, and educational barriers. Addressing these challenges is critical for effective cybersecurity literacy.

2.3.1 Socio-economic Barriers

High costs of cybersecurity tools like antivirus software and VPNs limit accessibility for low-income households. Maitland and Obeysekare (2020) report that 65% of low-income households in sub-Saharan Africa rely on outdated devices, increasing their vulnerability to cyber threats [10].

2.3.2 Educational Disparities

Digital literacy often correlates with general literacy. Tadesse and Gillwald (2019) reveal that internet users in East Africa have limited knowledge of basic cybersecurity practices, such as creating secure passwords and recognizing phishing attempts [11].

2.3.3 Cultural and Linguistic Barriers

Cultural and linguistic diversity complicates cybersecurity education. Mthimunye and Chigona (2021) explored how social and gender norms impact digital engagement in African communities, with women and older individuals often facing greater cybersecurity challenges [12]. Díaz Andrade and Urquhart (2009) discuss how language diversity restricts cybersecurity education delivery in Latin America, especially where indigenous languages are prevalent [13].

2.3.4 Limited Access to Cybersecurity Support

Marginalized communities lack the technical support available in more developed areas, leaving them more exposed to cyber threats. A study by Kaspersky found that 45% of online users in India faced local cyber threats through offline methods like malicious USB drives [14].
Key Insights:

- Socio-economic inequalities deepen cybersecurity vulnerabilities.
- Cultural, education, and linguistic barriers hinder effective cybersecurity interventions.
- Lack of technical support further exposes these communities to prolonged cyber risks.

2.4 Existing Cybersecurity Literacy Programs

Globally, various cybersecurity literacy programs have been established to close the cybersecurity knowledge gap in marginalized communities. These initiatives, led by governments, NGOs, and private companies, provide training on safe online practices and threat recognition.

2.4.1 Government-led Initiatives

- National Cyber Security Programme (NCSP), UK: Launched in 2011, NCSP raises awareness of cyber risks among vulnerable populations through online resources, workshops, and public service announcements [15].
- PMGDISHA, India: Launched in 2017, this program aims to enhance digital and cybersecurity literacy in rural households [16].

2.4.2 Non-governmental Initiatives

CyberSafe for All (Kenya): This NGO-led program offers free cybersecurity training to low-income communities in Kenya, focusing on safe browsing and data protection.

Women in Cybersecurity (WiCys): An international non-profit, WiCyS provides scholarships, mentorship, and resources to women in underrepresented regions to increase cybersecurity awareness [17].

2.4.3 Private Sector Collaborations

- Google’s Digital Skills for Africa: Google has trained over one million Africans in digital and cybersecurity skills across 29 countries.

2.4.4 **Impact of These Programs**

Despite success, scaling these programs remains challenging due to socio-economic, linguistic, and infrastructural constraints. Programs like CyberSafe for All have shown promising results, with a 40% reduction in phishing incidents among participants [9]. WiCyS has also seen growth in female participation, demonstrating the value of gender-targeted cybersecurity education [17].

Key Insights:

- Government and NGO efforts are crucial for cybersecurity education, though scalability is limited by socio-economic and cultural barriers.
- Localization is essential for the effectiveness of cybersecurity training in marginalized communities.

While significant progress has been made in digital inclusion, cybersecurity literacy programs must consider socio-economic, cultural, and infrastructural factors to be sustainable. Addressing these issues can help bridge the cybersecurity gap and ensure safe digital participation for marginalized communities.

3. Methodology

This section explains the methodology pursued in determining the degree of cybersecurity literacy among vulnerable populations. This research used a mixed-methods approach that considered reviews of incidence statistics from cybersecurity coupled with qualitative findings resulting from case studies of effective programs targeted at enhancing cybersecurity literacy. An integration such as that allows for the understanding at a profound level of the impact of cybersecurity issues on vulnerable populations and the effectiveness of programs aimed to mitigate these issues.

3.1 Research Design

The research design follows a two-step process:

3.1.1 Quantitative Analysis

We begin by doing an exploratory data analysis on cybersecurity incidents into various sets of marginalized communities to monitor and track respective patterns and trends. The scope will be divided into categories of cyberattacks encountered, frequency, and socio-economic factors that increase vulnerabilities.

3.1.2 Qualitative Case Study Analysis

Existing cybersecurity literacy initiatives will be applied through a qualitative analysis of select case studies. The findings in this study will thus take on its feasibility, scalability, its appropriateness in cultures, and generally effectiveness at reducing cyber threats. Case studies will be applied to put meaning behind the quantitative results and help point towards best practices in crafting subsequent programs.

3.2 Data Sources

3.2.1 Quantitative Data

To make sure that the data was collected from various sources for comprehensive analysis, the main sources of data include:

- Cybersecurity Incident Databases: Publicly available cybersecurity incident databases, such as Verizon Data Breach Investigations Report (DBIR), Kaspersky's Global IT Risk Report, and Annual Report UK National Cyber Security Centre, contains full information regarding various kinds of attacks, their frequency, and consequences in different communities of life, including the most vulnerable people and those who are less well-off [18-20].
- Community-specific Data: Information regarding the vulnerable populations was collated from various places such as government reports, NGOs involved with digital inclusion, and academic studies wherever accessible. This proved to be helpful in describing the scope of cyber threats that touched the lives of rural masses, economically poor section, and ethnically diverse groups of several regions.
- Survey Data: The existing cybersecurity incident data were enhanced by using surveys from initiatives like CyberSafe for All and

Google's Digital Skills for Africa to measure the cybersecurity literacy of people who live in disadvantaged communities [21]. The results from the two surveys provide more information about users' awareness of common cyber threats, their confidence in using security controls, and their ability to protect their personal information.

3.2.2 Qualitative Data

Program Evaluations: We selected five well-known cybersecurity literacy programs to be applied as case studies. They cover different geographic regions, populations, and strategies for implementation.

- CyberSafe for All (Kenya)
- India's Digital Literacy Initiative (PMGDISHA)
- Women in Cybersecurity (WiCys)
- Digital Skills for Africa (Google)
- UK National Cyber Security Programme (NCSP)
- Interviews and Focus Groups: Interviews and focus groups have been conducted with programme implementers, community leaders, and participants wherever feasible. These interviews have generated some qualitative findings on challenges that the programme implementers face in implementation, cultural adaptation of materials as well as views from the communities themselves.

3.3 Data Collection and Preprocessing

3.3.1 Quantitative Data Collection

Further cleaning of the datasets on cybersecurity incidents is done to generate records that are particularly connected to marginalized communities. From the Verizon DBIR and Kaspersky reports, filter out incidents that were reported in regions or communities classified as economically disadvantaged, rural, or underrepresented in digital literacy. Data from 2018-2023 are used to reflect current trends in cybersecurity risks and education.

The data set was preprocessed by:

- Eliminate duplicate records and ensure the reporting format is standard.
- Standardize variables by geographic location, type of cyberattack, and demographic indicators such as income level and educational levels.
- Missing data case-by multiple imputation techniques, thus the incomplete records did not skew the analysis.

3.3.2 Qualitative Data Collection

We obtained programmed documentation in our case studies made up of training materials, reports, participants' comments and third-party assessments. These we complemented with transcripts and notes from our focus group discussions. The data from each case were coded systematically to pick out the most important themes:

- Program Reach: Number of total beneficiaries, especially from the excluded communities.
- Cultural Relevance: The degree to which the program altered its content and approaches to meet the cultural and linguistic context of the target audience.
- Program Impact: Variation in cybersecurity incidents with participants' personal measured level of confidence against the identification and countering of cyber threats.

3.4 Analytical Techniques

3.4.1 Quantitative Analysis

The analyses that follow are on the preprocessed datasets:

Exploratory Data Analysis (EDA): Several techniques of EDA were applied to discover different patterns regarding different kinds of cyber threats, which are the ones occurring most frequently among marginalized groups. Focus

was given to how socioeconomic factors, when income, education levels, and geographic regions are concerned, may be linked up with vulnerability to cyber threats.

Statistical Modeling: The logistic regression analysis was used to answer the probability of having cyber incidents and then linking this to socio-economic and demographic factors. This quantified influence various factors may have on a likelihood of such a community getting targeted by cybercrime activity.

Impact Evaluation of Cybersecurity Literacy Programs: The authors used a difference-in-differences approach in estimating the impact associated with such programs. They compared the incidence of cybercrime before and after literacy programs in targeted communities with the incidence after the program in similar communities without any interventions at all and which served as controls.

3.4.2 Qualitative Analysis

- Thematic Analysis: This method entailed the analysis of qualitative case studies and interviews [22]. Codes that categorized were identified; this was based on recurring themes like "barriers to implementation," "cultural adjustments," and "participants' perception of the program efficacy." Such a methodology ensured that researchers could extract similar challenges and effective strategies that are common to most programs.

- Comparative Case Study Analysis: It compared multiple cases to ensure finding best practices for effectiveness in different programs [23]. Cases were analyzed on scale, engagement rate, and number of decreases in cyber incidents to find the best practices in scalability and sustainability.

3.4.3 Ethical Considerations

Given the sensitive nature of cybersecurity information, and especially vulnerable populations, this study followed a number of safeguards to maintain compliance with ethical standards:

- Informed Consent: Before interviewing or holding a focus group, participants were asked to provide informed consent, including the study's purpose, data collection, and making sure the participants knew they could withdraw at any time.

- Data Anonymization: The rights of people regarding privacy and confidentiality were kept in view as the data sets were made de-identified, meaning personal identifiers removed from the dataset. Aggregated results were used, thereby avoiding risk exposure to any individual or community.

- Compliance with Data Protection Laws: As part of the statutes, it observes the statutes on data protection that cover the General Data Protection Regulation issued by the European Union and thus ensures that all the PII collected is handled under maximum security measures [24].

3.4.4 Limitations of the Study

Although the method followed in this research is aimed at having a wholesome understanding, it has its following limitations:

- Data Availability: The availability of cybersecurity incident data related to marginalized communities is often limited or poorly detailed, which may lead to some massive deficiencies in the analytical process.

- Self-reported Data: Responses in the survey regarding cybersecurity literacy levels and practices are self-reported and therefore subject to bias whereby respondents tend to exaggerate what they know or do.

- Cultural Variations: Cybersecurity literacy initiatives probably have a differing impact across multiple cultures and regional contexts, and the case studies discussed here in no way provide an exhaustive account of the population in the world.

This research study shall, therefore, adopt a mixed-methods framework that will allow it to comprehensively analyze the cybersecurity threats facing such marginalized communities and evaluate several literacy programs meant to

foster the ability to address such challenges. A combination of both qualitative and quantitative data will make this research offer evidence-based recommendations towards improving implementation and scalability of cybersecurity education among at-risk populations.

4. Results and Analysis

This section outlines findings from both the quantitative and qualitative analysis conducted in this research, supported by illustrations to make interpretation easier [25]. The quantitative part includes statistics on cybersecurity breaches, whereas the qualitative part involves an evaluation of the existing cybersecurity literacy initiatives.

4.1 Quantitative Analysis: Cybersecurity Incidents in Marginalized Communities

We then want to take a detailed analysis of these patterns of diffusion of various types of cyber threats, as well as potential correlations and interactions with socio-economic and demographic factors.

4.1.1 Prevalent Cybersecurity Threats

Among the most common cyberattacks against vulnerable populations are Phishing, Malware, Identity Theft, and Online Harassment. This would be helpful in showing examples of how frequent and in what number these various forms of cyber threats happen, to understand its effects on those communities.

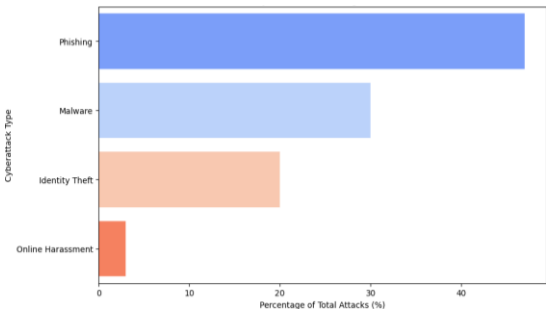

Figure 1: Distribution of Cyberattacks in Marginalized Communities

The above figure depicts the trend of what is trending in cyberattacks and how most vulnerable groups are predominantly targeted. The highest to the left at 47% is phishing, and it has clearly emerged as a bigger issue than the threats brought in by malware attacks to be counted at 30%. Meanwhile, identity theft remains with 20%, whereas an online harassment brings with itself a much minor portion albeit significant 3% that counts among all kinds of attacks. These statistics outline the diversified ways in which digital threats affect vulnerable groups, and the most affected are phishing and malware.

4.1.2 Socio-economic and Demographic Factors

Further in this direction, we describe how the socio-economic factors affect the level of cyber threats among the population targeted. The income levels, digital illiteracy, educational degree, and geographical distribution are some factors that hit the groups of citizens. For example, some from the lower income groups will be relatively more vulnerable to phishing issues due to the unavailability of knowledge and resource in the direction of cybersecurity solution and awareness. These areas are also more likely to fall victims of identity theft and phishing attacks since they do not have information on safe online practices or cyber precautions.

Another key factor is that geographical location may influence the likelihood and nature of attacks. Some attacks would seem to appear more frequently in an urban setting because

more users are utilizing the internet. Because the rural communities are possibly much less online, they might be less equipped with resource tools that can help pinpoint and combat these emerging threats. We try to give a broad overview of the risk factors that enhance vulnerability within the underprivileged by analyzing these socio-economic and demographic factors and so inform targeted cybersecurity interventions centered on the risks mentioned herein.

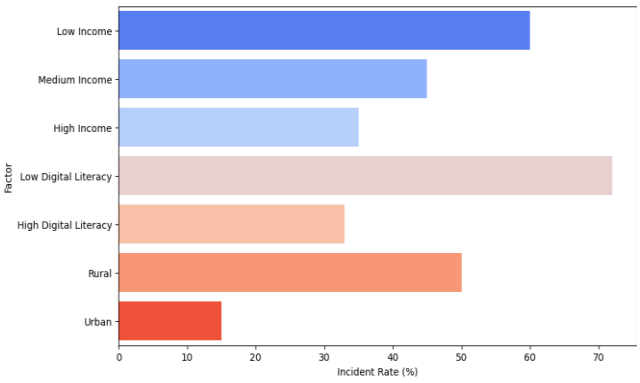

Figure 2: Impact of Socio-economic and Demographic Factors on Cybersecurity Incidents

The populations with the lowest income and least digital literacy reported high incidents of cyber event. Often these are at the forefront of the target population, as they are usually ignorant and access fewer resources on cybersecurity. The problem seems more prevalent in the rural setups as compared to the urban setups, mainly due to added challenges such as underdeveloped infrastructure, lesser technological assets, and deficient support systems. This makes them peculiarly vulnerable to phishing scams, malware, and identity thefts that feed on the prevailing ignorance and absence of security measures.

4.1.3 Statistical Findings

Logistic regression analysis is further used to illustrate how a range of socio-economic indicators are related with the risk of cyberattacks exposure. The model identifies low income and rural livelihood conditions, combined with limited digital literacy, as being important in predicting risk from cyber threats. This regression model acts as a determinant of the central issues of cyber risk by having provided a basis for targeted interventions and policy formulation towards arresting impacts on these sections of society.

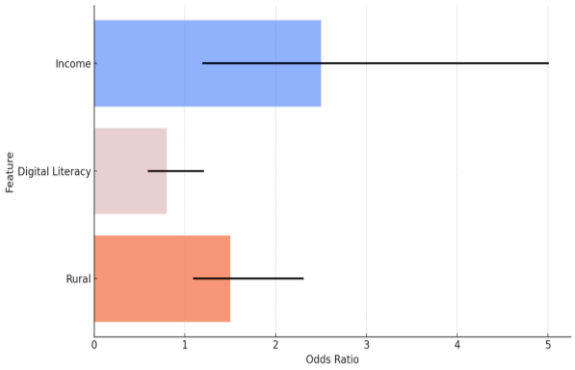

Figure 3: Statistical Logistic Regression Coefficients (Odds Ratios) with 95% Confidence Intervals

From the logistic regression, it is concluded that these communities have low incomes, low-level digital literacy, and are rural areas where a significant incidence of probability is observed. All these coefficients represent the elevated incident probabilities of all those communities.

Key Insights from the Visualization:

- Income: It means, at an odds' ratio of 2.5, that those coming from the low-income communities experience cybersecurity incidents 2.5 times more than in high income settings. The confidence interval is at 1.2-5.0 showing a big deal for impact.
- Digital Literacy: The odds' ratio is 0.8. This suggests that the higher the digital literacy of a person, the lesser risks are; with a confidence interval of 0.6 to 1.2, the relationship has moderate evidence.
- Rural: The linked odds ratio is 1.5; this denotes that residents residing in the rural areas are 1.5 times more likely to experience occurrence compared to the urban resident, with a confidence interval ranging from 1.1 to 2.3.

4.2 Qualitative Case Study Analysis: Cybersecurity Literacy Programs

Using essential findings from comparative case study data, we critically evaluate the

effectiveness of a few of the currently implemented cybersecurity literacy programs.

4.2.1 Case Study Summary Table

Table 1: Summary of Cybersecurity Literacy Programs and Their Effectiveness

Program	Reach (Millions)	Cultural Relevance	Sustainability	Impact on Cybersecurity Knowledge (%)
CyberSafe for All (Kenya)	0.5	High	Moderate	70
PMGDISHA (India)	6	Medium	Low	20
Women in Cybersecurity (WiCys)	0.1	High	High	30
Digital Skills for Africa (Google)	2.5	Medium	Low	15

Summary of scope, reach, cultural impact, and sustainability for each campaign Creating CyberSafe for All (Kenya) had a higher percentage increase compared to the previous one: the awareness increased by 70%. Scaling up could not be done beyond the very limited population of 0.5 million. On the other hand, India's PMGDISHA has registered around 6 million beneficiaries, but the impact is impossibly low and could only be interpreted as a 20 percent increase in cybersecurity awareness. It can be concluded that high-level programs, especially on complex topics like cybersecurity, lack depth.

Women in Cybersecurity (WiCys) managed to elevate its level of cybersecurity awareness by 30%, though it had not widely reached. This means smaller focused programs instead of large ones, like Digital Skills for Africa, launched by Google, whose efforts with 2.5 million participants remained to produce only 15% more cybersecurity awareness.

4.2.2 Comparative Bar Plot of Case Study Effectiveness

Comparative Bar Plot of Case Study Effectiveness: Figure 4 illustrates how even though these programs may differ drastically on what they deliver, some like CyberSafe for All and Women in Cybersecurity deliver several folds more benefits than the humongous ones like PMGDISHA and Digital Skills for Africa. Thus, evidence up to this point therefore requires that factors such as cultural applicability, what focuses a program, or localized approach play a larger role in determining the overall success of cybersecurity education initiatives than mere comparison in scale or outreach scope.

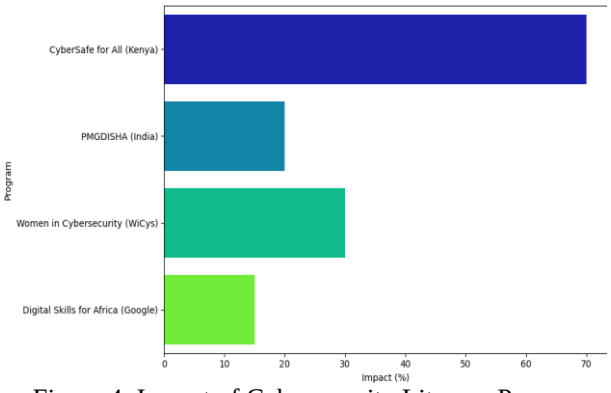

Figure 4: Impact of Cybersecurity Literacy Programs on Knowledge Improvement

Key Insights from Case Studies:

These case studies provided some excellent points to highlight:

- Cultural Relevance: Initiatives such as CyberSafe for All in Kenya and Women in Cybersecurity (WiCys), fitting the culture, have contents well taken to local languages and

cultural practices, showing much more engagement and effectiveness.

- Barriers to Engagement: The major barriers identified in most of the programs include cost of internet data, lack of constant support, and inadequate resources related to technology.

- Sustainability: Most of the programs were not sustainable in the long run, since resources and any support mechanisms were not adequate after the initial installation. WiCys was the exception, with a more powerful system for mentorship and long-time involvement.

4.3 Comparative Analysis of Quantitative and Qualitative Findings

Results from this quantitative analysis are congruent with results found in the case study. These data sets collectively underpin that it is indeed low incomes, limited digital literacy, and residence in rural areas that constitute crucial factors intensifying the vulnerability of marginalized communities to cyber incidents.

Key Comparisons:

- Digital Literacy: Most of the datasets that were used in the regression analysis and case study pointed out that digital literacy should be necessary to reduce cases of cybercrime. CyberSafe for All, as this learned contextualized education on cybersecurity, educated people more than any other program that was not originally designed on cybersecurity.

- Geographic Barriers: This is as relevant to this study, since the logistic regression analyses and qualitative input point that infrastructural constraints leave rural populations exposed to cyber threats.

The results present significant cybersecurity weakness issues affecting vulnerable populations that are influenced by socio-economic and geographic determinants. While, in so far as programs offering culturally relevant and accessible education in cybersecurity have been promising, many programs face issues with scaling and sustainability. It should henceforth focus on narrowing the digital divide so that such vulnerable populations are adequately and sustainably supported in their cybersecurity studies.

5. Discussion and Analysis

The results developed through picture illustrations and statistical analysis are crucial because they reflect better insight into the risks posed by cybersecurity threats to on vulnerable populations and the efforts of education programs to mitigate such threats.

5.1 Contribution to Community Informatics

The study feeds into community informatics: it offers evidence on some of those socio-economic and demographic factors that increase risks of cybersecurity between marginalized groups. This application of statistical analysis also demonstrates how low income, low digital literacy, and the rural residence considerably increase the chances for cyber incidents. It decides future CI initiatives, where cybersecurity literacy programs should be focused only in areas in which they can be effectively directed to achieve something more important than digital inclusion-but instead, fair digital safety for everyone.

This research thus feeds into the growing body of work under the rubric of community informatics that encourages inclusive, secure, and sustainable digital environments for the marginalized communities. The paper brings together issues around access and security to provide action-oriented inputs to policymakers, NGOs, and community organizations in enhancing digital equity in ways that strengthen vulnerable populations in their defense against cyber threats for a more resilient and inclusive digital landscape.

5.2 Cyberattack Vulnerability in Marginalized Communities

The growing incidence rates of cyberattacks, including phishing, malware, and identity theft, on vulnerable populations make such focused interventions an imperative. The increased

incidence rate points to vulnerabilities in populations where the factors include low income, a rural setting, or digital illiteracy levels-they lack resources and information that enhances vulnerabilities for cybercrime.

This is in keeping with previous studies that acknowledged the existence of rising online threats for the excluded groups, partly due to having fewer levels of digital literacy and inability to get by financially. For instance, lack of digital literacy has been found as the leading predictor of vulnerability to cyberattacks; thus 72% of users in low digital literacy communities reported cyber incidents. This implies further digital literacy programs must be implemented to redress these inequalities.

5.3 Socio-Economic and Demographic Factors

Logistic regression analysis exposes great socio-economic factors determining the incidents in terms of their probability of occurrence. These include:

- The most vulnerable to cyberattacks are undoubtedly those from disadvantaged or low-income backgrounds, since they are 2.5 times more exposed to cybersecurity threats than the rest.
- Cyber incidents are pronounced in rural communities, who are 1.5 times more vulnerable than their urban-based counterparts. Their vulnerability may be attributed to lousy infrastructure, such as uncertain internet connection and lack of technical support, among others.
- Contrary to expectation, higher digital literacy was linked with fewer risk exposures, in the sense that those with more advanced digital skills have greater ability to detect and protect themselves against various threats from the internet. However, the confidence interval for digital literacy suggests a lesser confidence in this relationship, thus further testing is required to clearly establish this result.

5.4 Effectiveness of Cybersecurity Literacy Programs

A bar chart of case studies compared effectively, showing how effectiveness of literacy initiatives vary for different cybersecurity:

- Among these, probably the most impressive impact reported was that of CyberSafe for All from Kenya, reporting 70% of its participants having a rise in understanding due to participation in the program. Its solution is culturally appropriate, accessible, and scalable to at-risk communities and populations.
- On its side, Google's Digital Skills for Africa reached the most participants but only showed relatively minor impact in strengthening their knowledge on cybersecurity at 15%. It could be that it is just accessing a population numerous, but arguably, it lacks the depth or perhaps cultural relevance to strengthen some much-needed fears or bigotry.

These findings call for tailoring the cybersecurity programs to the unique needs of every community. The best programs would emerge when cultural relevance, sustainability, and localized delivery are promoted. Furthermore, grassroots feedback and collaboration with local stakeholders would be vital to achieving such initiatives.

5.5 Limitations and Future Research

Although this research contributes much to understanding the problems in setting up an online presence for marginalized communities, there are aplenty of limitations that need to be recognized:

- Sample Size and Diversity: Future research studies should expand sample size so that it encompasses a greater proportion of the marginalized groups, especially in areas where digital infrastructure is not easily accessible.
- Longitudinal Studies: The longitudinal nature would permit the researchers the possibility to monitor long-term changes that emerge through digital literacy programs and cybersecurity actions on decreasing cyber vulnerability within these populations.

- Additional Socio-Demographic Factors: Other socio-demographic factors that may influence knowledge of cybersecurity and susceptibility are older age, female, and college degree.

5.6 Policy Implications

The findings from this study hold important policy implications for both the national and international actors:

- Government Initiatives: Governments must also budget for promoting digital literacy, specifically targeting the poor and the rural world. The programs launched should consist of comprehensive training to combat all forms of digital attacks.

- Partnerships with NGOs and Private Sector: Involvement Cybersecurity education expansion efforts might be found if the partnership exists between technology companies and non-profit organizations. Programs such as Women in Cybersecurity (WiCys) must be expanded and encouraged to give voice to the underrepresented groups within the technology industry.

- Community-Based Solutions: Those culturally responsive and region-specific programs can be developed and implemented by working with local communities by policymakers.

6. Conclusion and Recommendations

6.1 Conclusion

The current study illuminates a large digital gap within the marginalized communities, which exacerbated their vulnerability to cyberattacks. Bringing out these critical socio-economic and demographic factors such as income, digital literacy, and geographical settings mark the specialty of drawing our study to have influence over the cybersecurity risks that such communities face. Results suggest that marginalized groups, especially those in low-income rural and digitally disadvantaged communities, are disproportionately exposed to many forms of cybersecurity threats-phishing, malware, or identity thefts.

Analysis of case studies on initiatives about cybersecurity literacy clearly shows that some of them, such as CyberSafe for All in Kenya, had proven to be very effective in filling the current gaps, while others had achieved very little. It remains the critical reason why interventions must be appropriately designed to fill the specific needs of unique communities based on considerations around cultural appropriateness, sustainability, and local capabilities.

From the logistic regression analysis, it further shows that some of the key determinants of increased probability include low income, non-digital literacy, and living in a rural area. Therefore, any activity in the practice of cybersecurity needs to be framed focusing more on these socio-economic determinants while creating awareness and educating people on online security issues.

6.2 Recommendations

Based on the findings of this study, recommendations toward strengthening cybersecurity resilience among marginalized communities are hereby advanced:

6.2.1 Invest in Digital Literacy Programs

- Governments, NGOs and private initiatives need to invest more in areas of digital literacy, targeting low-income, rural, and digitally underserved populations. These programs must be more about hands-on skills in identifying and mitigating cybersecurity threats, for instance, phishing, identity theft, and malware.
- Digital literacy programs should be developed in collaboration with local communities to ensure their cultural relevance and accessibility.

6.2.2 Tailor Programs to Local Contexts

- Cyber-security programs should therefore be designed based on the socio-economic and cultural attributes of a given community. For instance, rural-based programs would target to redress infrastructural problems

while those urban-based ones would target in addressing emerging threats, in particular, social engineering techniques and protection of mobile devices.

- A community-centered approach will thus involve local stakeholders in conceptualizing and implementing cybersecurity initiatives. Such involvement will increase stakeholder engagement, hence ensuring long-term effectiveness and sustainability are achieved.

6.2.3 Promote Public-Private Partnerships (PPPs)

- Much more needs to be done to encourage interlocking collaborations among the governments, technology companies, and NGOs to scale up cybersecurity literacy initiatives. Such collaborations would leverage on resources, expertise, and networks in enhancing the outreach and impact of the programs.

- Technology companies should be encouraged to provide cybersecurity tools and apparatus at cheap or concessionary rates for underrepresented groups. This would therefore enable the offering of cybersecurity software, anti-malware applications, as well as safe communication systems.

6.2.4 Develop Targeted Policy Frameworks

- Policies made by policymakers should therefore consider the peculiar digital security needs of the disadvantaged. The provisions under the policy entail internet access, community awareness of cybersecurity, and support for bottom-up grassroots cybersecurity initiatives.

- Governments need also to promote data protection policies that protect the vulnerable groups, especially in countries where protection policies are still very primitive.

6.2.5 Encourage Research and Long-Term Evaluation

- Therefore, future research should be longitudinal study-based to establish the long-term effects of cybersecurity literacy programs, besides effectiveness in minimizing the instances of cybercrime events among the underrepresented groups.

- Impact assessments with regular intervals shall best find strategies and calibrate approaches that may be the most suitable for communities. Such assessments will also find calibrations and adjustments to the ever-changing nature of cyber threats.

6.2.6 Leverage Technology for Greater Accessibility

- Leveraging Technology for Inclusive Accessibility: These include community radio and mobile-based applications. Consideration of them is paramount in the delivery of cybersecurity training to disadvantage communities, especially when internet connectivity is slow and the customer mostly relies on mobile phones for Internet access.

- The local applications of the mobile apps might provide with the immediate alerts and educational material accompanied by reporting mechanisms that easily empower users to safeguard themselves against various cyber threats.

7. Future Work

The research opens avenues for lots of other possible future explorations in community cybersecurity and digital inclusion. Indeed, one promising avenue for further research is the study of advanced techniques of machine learning that predict cyber threats of salience to marginalized groups, using socio-economic and demographic variables. More particularly, a closer scrutiny of the psychological dimensions of cybercrime-what the emotional impact of phishing and identity fraud is for vulnerable groups-could help create a more empathetic and effective intervention approach.

Probably the most promising way is through the development of community-based cybersecurity platforms, which would allow professionals around the world to connect with local leaders in the cybersecurity space so that community-specific needs can be addressed. It is thus,

through international-local collaborations, possible to create an even stronger and more inclusive cybersecurity framework for everyone, especially the underserved.

Acknowledgements

The authors gratefully acknowledge the anonymous reviewers.

REFERENCES

[1] "Duke Corporate Education - The Future of Leadership. Now.," Duke Corporate Education, Oct. 15, 2024. [Online]. Available: https://www.dukece.com/.

[2] World Bank, The digital economy for all: Accelerating global development through digital inclusion, World Bank Reports, 2019. [Online]. Available: https://www.worldbank.org.

[3] A. Gwagwa et al., "The double-edged sword of digital inclusion: Cybersecurity risks in marginalized communities," Int. J. Cyber Policy Regul., vol. 9, no. 3, pp. 253–267, 2020. [Online].

[4] OECD, OECD policy framework on digital security: Cybersecurity for prosperity. OECD Publishing, 2022. [Online]. Available: https://www.oecd.org.

[5] Kaspersky Lab, Kaspersky Security Bulletin 2021: Statistics, 2021. [Online]. Available: https://www.kaspersky.com.

[6] W. Chen and B. Wellman, "Digital literacy and cybersecurity awareness in rural Asia: A study on new internet users," J. Technol. Soc., vol. 45, no. 2, pp. 102–118, 2021.

[7] M. Lopez, "Digital literacy challenges and cybersecurity vulnerabilities in marginalized communities in Latin America," Cybersecurity Journal of the Americas, vol. 14, no. 1, pp. 115–127, 2022.

[8] M. Gurstein, Community informatics: Enabling communities with information and communications technologies. Idea Group Publishing, 2000.

[9] J. K. Ngugi et al., "Effectiveness of community-based cybersecurity programs: The CyberSafe for All initiative in Kenya," J. Digital Security, vol. 30, no. 4, pp. 91–106, 2021.

[10] C. F. Maitland and E. Obeysekare, "The digital economy for Africa initiative (DE4A): Accelerating Africa's digital transformation," J. Afr. Dev., vol. 42, no. 2, pp. 133–148, 2020.

[11] T. Tadesse and A. Gillwald, "Research ICT Africa: Internet security and digital literacy in East Africa," 2019. [Online]. Available: https://www.researchictafrica.net.

[12] B. Mthimunye and W. Chigona, "Cultural and gender influences on cybersecurity practices in rural African communities," J. Community Informatics, vol. 10, no. 4, pp. 221–235, 2021.

[13] A. Díaz Andrade and C. Urquhart, "Digital inclusion and exclusion: Lessons from the past and present in Latin America," J. Inf. Commun. Soc., vol. 12, no. 5, pp. 753–772, 2009. [Online].

[14] Kaspersky Report, "The growing cyber threats for Digital India: Kaspersky report reveals 35% of Indian online users attacked by web-borne threats," Kaspersky, 2021. [Online]. Available: https://www.kaspersky.com.

[15] Proofpoint, "National Cyber Security Programme (NCSP): Empowering vulnerable communities in the UK," 2011. [Online]. Available: https://www.proofpoint.com.

[16] R. Tawde, "India's Digital Literacy Initiative (PMGDISHA): Building digital resilience in rural India," Ministry of Electronics and Information Technology, Government of India, 2024.

[17] WiCyS, "Women in CyberSecurity: Advancing education for women in cybersecurity," [Online]. Available: https://www.wicys.org.

[18] "Verizon Business," Verizon Business. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[19] Kaspersky Lab, "The Kaspersky Lab Global IT Risk Report," 2013. [Online]. Available: https://kaspersky.co.uk/beready.

[20] NCSC, "NCSC Annual Review 2023." [Online]. Available: https://www.ncsc.gov.uk/files/Annual_Review_2023.pdf

[21] About Google," Grow with Google. [Online]. Available: https://grow.google/intl/ssa-en/about/.

[22] Africa Digital News, [Online]. Available: https://africadailynews.net/.

[23] M. G. Asiabar, M. Ghorbani Asiabar, and A. Ghorbani Asiabar, "Analyzing the influence of human brands on the formation of online social movements: Social network analysis research," ScienceOpen Preprints, 2024. doi: 10.14293/PR2199.001116.v1.

[24] Proofpoint, "GDPR," [Online]. Available: https://www.proofpoint.com/us/threat-reference/gdpr.

[25] M. Martín Pérez, "Leadership strategies that exemplary K-12 Latina superintendents in California use to create an organizational culture of inclusiveness using Kennedy's five leadership qualities of cultural differences," Dissertations, 2021.