ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 ||SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

CYBERSECURITY AWARENESS ACROSS THE URBAN-RURAL LANDSCAPES OF COIMBATORE

Sri Akila Ravi[1], Dr. A .Prasathkumar[2]
[1]*II MBA Sakthi Institute of Information and Management Studies, Pollachi-01*
[2]*Assistant Professor, Sakthi Institute of Information and Management Studies, Pollachi-01*

Article DOI: https://doi.org/10.36713/epra28056
DOI No: 10.36713/epra28056

ABSTRACT

The paper conducts an empirical comparative study on cybersecurity awareness, behaviours, and attitudes of residents from urban, rural, and semi-urban areas in the Coimbatore District, Tamil Nadu, India. Following a quantitative cross-sectional survey research approach, a dataset was generated from 392 participants recruited by means of a stratified random sample. The main instrument of measurement utilized for the study was the Cybersecurity Awareness Inventory (CAIN). Security behaviour measures and threat awareness attitudes were also included based on standardized psychometric scales. Statistical analysis of data consisted of simple percentages, weighted average calculations, and one-way ANOVA. Important insights obtained include an alarming level of knowledge gap since despite the majority of respondents (more than 75%) being aware of cybersecurity to some extent, over 54% proved to be "Not Aware" according to the knowledge-based objective assessment. It is worth mentioning that there was no significant difference in cybersecurity practice scores among residents from urban, rural, and semi-urban settings (p = 0.500). In other words, location became irrelevant as far as safe online behaviour is concerned. On the other hand, age, occupation, and education appeared to have a considerable impact on awareness and behaviour scores. The threats that participants could recognize best included phishing attacks and identity theft, while the technically complicated DoS attacks were less recognized. The results indicate that there is a need for cybersecurity campaigns targeting particular age groups, such as older people and salaried employees, using multiple languages. This research is in sync with SDG 4 (Quality Education), SDG 10 (Reduced Inequalities), and SDG 16 (Peace, Justice, and Strong Institutions) and suggests interventions that are specific, multilingual, and institution-based to close the cyber-security knowledge-doing gap.

KEYWORDS: *Cybersecurity Awareness, Digital Literacy, Rural–Urban Divide, CAIN, ANOVA, SDG 4, SDG 10, SDG 16,Coimbatore, Phishing, Online Safety Behaviour*

INTRODUCTION

The explosion in the use of digital technology has completely transformed the way people interact, conduct business and access services. The number of connected devices worldwide stood at more than 4.2 billion in 2020 and daily life is now inextricably linked to the virtual world. While the benefits associated with this digitalisation have been numerous, it has also made it easier for cybercriminals to exploit any weaknesses that may arise. In the year 2019 alone, the number of malware attacks exceeded 200,000 per day, ransomware attacks increased by 118%, and cybercrime cost the world economy more than one trillion dollars by 2018. Therefore, individuals and businesses need to be well aware of the threats of the digital age.

Cyber security, viewed generally as a broad area of study that involves the protection of computer systems, networks, data, and information systems from unauthorized access, manipulation, or damage, is no longer seen as merely a specialized area of study but rather an interdisciplinary field encompassing elements of software engineering, artificial intelligence, data science, and the social sciences. Modern literature shows that although technical tools are necessary, humans still form the weakest link in a cyber security chain; staff who fall for phishing schemes, those who reuse simple passwords, and even groups that don't have the language skills to recognize a threat are vulnerabilities in themselves.

In the case of India, the issue of raising awareness about cyber security has been complicated even further by the existence of significant socio-economic differences among different groups as well as by linguistic differences. There have been many efforts in making digital infrastructure available to rural areas, but the associated security training has not always followed. Thus, one sees a situation where accessibility is increasing while knowledge decreases, which means that understanding whether there is a meaningful difference in the levels of cyber security knowledge and practices between rural and urban populations becomes a relevant issue.

This research addresses the identified problem through the examination of the situation in the Coimbatore District of the Tamil Nadu State, which includes both an urban industrial area and rural and semi-urban areas undergoing digitalization. The most important thing about this study is that it takes place against the backdrop of the United Nations 2030 Agenda for Sustainable Development. Cybersecurity is not just a problem but also an essential precondition for sustainable, inclusive, and peaceful development in cyberspace. By basing our conclusions on the Sustainable Development Goals 4 (Quality education),

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 ||SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

10 (Reduced inequalities), and 16 (Peace, justice and strong institutions), we prove that cybersecurity awareness is a crucial part of sustainable human development.

1.1 Research Objectives

The study was designed to achieve four interrelated objectives:
• To assess the overall level of cybersecurity awareness among respondents in urban, semi-urban, and rural settings.
• To identify prevalent cybersecurity practices and online behaviours across community types.
• To determine the types of cyber threats with which respondents are most and least familiar.
• To examine community attitudes toward cyber threats and evaluate the degree to which awareness translates into protective attitudes.

2. SUSTAINABLE DEVELOPMENT GOALS: CONCEPTUAL COHERENCE

The UN's Sustainable Development Goals (SDGs) serve as a normative blueprint for sustainable and equitable development on an international scale. Though there may be no direct mention of cybersecurity consciousness among the SDGs, the concept is inherently tied into several different SDGs as one of their underlying preconditions. There are three SDGs which have particular relevance to this research and will be analysed in greater detail below through the lenses of conceptual coherence, empirical foundation, and policy relevance.

2.1 SDG 4 – Quality Education (Primary SDG)

The call for SDG 4 is for ensuring inclusive and equitable quality education and promoting lifelong learning opportunities for all people. This includes awareness on cyber security as an essential element of digital literacy. The findings of this research, showing that 84% of the participants have attained university or even higher degrees, but only 54.59% are objectively assessed as "Not Aware" of cyber security issues, prove that academic qualifications do not guarantee awareness on digital security issues. Educational qualifications were found to have a significant relationship with CAIN index ($F = 6.226$, $p < 0.001$), where the participants who had postgraduate education scored highest with a mean of 21.64.

2.2 SDG 10 - Reduced Inequalities (Empirically Strongest Contribution)

SDG 10 focuses on promoting inclusivity socially, economically, and politically of all individuals. The greatest empirical contribution of this research regarding SDG 10 is the statistical similarity of cybersecurity practice scores among urban dwellers, semi-urban dwellers, and rural dwellers ($F = 0.695$, $p = 0.500$) with respective means of 35.06, 35.40, and 36.03. The geographic digital divide related to security behaviour has been bridged by the present study. Inequality has now emerged based on demographics (age, occupation, and educational attainment). It can be stated that age, occupation, and educational attainment are the critical predictors of both knowledge and practice. In fact, the farmers and allied workers have performed better than salaried individuals in terms of knowledge ($M = 21.64$) and attitude ($M = 23.03$).

2.3 SDG 16 – Peace, Justice and Strong Institutions (Policy Anchor)

SDG 16 advocates for institutions that are effective, responsive and inclusive, ensuring individual safety and access to justice. There is evidence of a recurring knowledge-action disconnect, since self-reported awareness does not correlate with practice scores ($p = 0.207$), hence, lack of knowledge does not translate into safer behaviour. Additionally, there is little trust exhibited among citizens regarding the use of cybercrime complaints systems. SDG 16 Target 16.6 (accountable and transparent institutions) and SDG 16 Target 16.b (equal access to protection) can be supported by advice to create easier complaint processes, launch campaigns in vernacular languages, and make institutions more responsive.

3. REVIEW OF RELATED LITERATURE

An abundant amount of related literature has been generated during the last decade with regards to cybersecurity awareness from the psychological, organizational, and policy standpoints. In an extensive systematic review carried out by Admassa, Munaye, and Diro (2024), the authors conclude that AI and ML have become vital tools for detecting cybersecurity threats, and the future of cyber resiliency depends on the establishment of cooperative threat sharing environments. In parallel, Alharthi, Alenezi, and Alrasheed (2024) found that the cause behind most successful cyber-attacks lies in human errors rather than vulnerabilities.

Awareness measurement studies have contributed greatly in terms of methodology. Tempestini et al. (2023) created the Cybersecurity Awareness Inventory (CAIN) which is a 46-item tool that relies on the standards established by ISO/IEC 27032. The results of a survey involving 277 college students showed that the relationship between lower scores on objective knowledge and greater cybersecurity risk was significant. It is therefore CAIN that served as the foundation for assessing the objective knowledge level in the current research. A PRISMA-based review performed by Rohan et al. (2023) on existing cybersecurity scales demonstrated that most lacked psychometric validation, highlighting the significance of using standardised tools like CAIN.

Studies related to demographic and environmental factors influencing awareness exhibit clear trends. In his survey of 1,230 Saudis, Alzubaidi (2021) discovered severe security vulnerabilities regarding passwords and phishing, combined with an alarmingly low level of reported cybercrimes. Alharbi, Alshammari, and Alotaibi (2024) employed TAM theory among students and found perceived usefulness to be the main predictor of security behaviour intention, with structured training programs greatly increasing awareness levels. Gratian et al. (2018) utilized the Big Five Personality Theory to demonstrate the significance of individual characteristics, such as conscientiousness and openness, in explaining 23% of variation in security behaviour.

In behavioural change theory, one of the first things that has been highlighted is the mistake made by assuming that knowledge leads to action. This was confirmed by Chaudhary (2024) with his Delphi research where he found out that the

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 ||SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

involvement of senior management and organisational norms played a much more important role in compliance with security rules than the dissemination of information. De Bruijn and Janssen (2017) also came to a similar conclusion regarding fear or overly optimistic awareness campaigns leading to public indifference.

Not much research work has been done on the rural/urban angle in the Indian setting. Creese et al. (2021) identified a very high positive association between national prosperity and cybersecurity capability maturity in their macro-level analysis and indicated the presence of a global digital divide with regard to capacity building. Keller et al. (2025) found that digital escape room games could help educate all types of learners, with age, gender, and occupational profile having little moderating effect—an outcome that could have implications for scalable rural education programmes.

4. RESEARCH METHODOLOGY

4.1 Research Design

In this research, a quantitative cross-sectional survey design was used to collect data at one point in time. It involved the use of a structured questionnaire consisting of four themes corresponding to the four research objectives namely; cybersecurity knowledge (as measured by CAIN test), cybersecurity practices, cyber threat awareness and attitudes towards cyber threats.

4.2 Population and Sampling

The target population consisted of all persons living in the Coimbatore district and accessing the internet at least once in a week which qualifies in this study as 'active internet users'. The population was stratified into three groups depending on their residence status: Urban (within Coimbatore city municipal corporation limits), Rural (within village panchayats) and Semi-urban areas.

Convenience sampling technique was employed in selecting samples within the stratified population. Sample size was calculated using Cochran's sample size formula applicable for large or unknown population at 95% confidence level (Z=1.96) and 5% margin of error hence sample size was calculated to be a minimum of 384 respondents. This study managed to collect data from 392 respondents.

4.3 Tools for Analysis

Four sections of the validated questionnaire were used to measure knowledge, practice, threat awareness, and attitudes toward cyber threats. The cybersecurity knowledge was assessed through 40 questions taken from the CAIN tool (Tempestini et al., 2023). Each question had only one option that could be either true or false. The cybersecurity practices were determined through 10 items developed by Alzubaidi (2021), which were rated based on a five-point frequency scale. The level of threat awareness was gauged by 6 questions related to common cyber-crime categories, including phishing, identity theft, malware, DoS attacks, hate speech/radicalisation, and extortion. These questions were rated based on a four-point familiarity scale. Finally, attitude towards cyber threats was gauged by seven questions taken from Schaltegger et al. and rated based on a five-point Likert scale.

4.4 Data Analysis Techniques

There were three data analysis techniques used on the data collected for the study. These included simple percentage analysis that gave a description of the demographics of the survey respondents. Weighted average technique determined the order of the six threats in terms of their level of familiarity among the respondents. The third technique involved one-way ANOVA, where CAIN scores, practice scores, and attitudes were tested for any significant difference between the various sub-populations at a 5% level of significance.

5. RESULTS AND DISCUSSION

5.1 Demographic Profile of Respondents

Table 1: Demographic Profile of Respondents (n = 392)

Variable	Category	Count	%
Age			
Age	Below 18	16	4.1
	18–25	178	45.4
	26–35	130	33.2
	36–50	57	14.5
	Above 50	11	2.8
Gender			
Gender	Male	193	49.2
	Female	199	50.8
Place of Residence			
Residence	Urban	129	32.9
	Rural	139	35.5
	Semi-Urban	124	31.6
Occupation			
Occupation	Student	147	37.5
	Business & Self-Employed	101	25.8

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 ||SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

	Salaried Professional	90	23.0
	Agriculture & Allied	33	8.4
	Non-Working	21	5.4
Educational Qualification			
Education	Undergraduate (UG)	180	45.9
	Postgraduate (PG)	148	37.8
	Diploma	40	10.2
	School Level	17	4.3
	No Formal Education	7	1.8
Primary Internet Access Device			
Device	Smartphone	182	46.4
	Laptop / Desktop	153	39.0
	Tablet	43	11.0
	Basic Feature Phone	14	3.6
Total Respondents		**392**	**100.0**

Source: Primary Data

Demographically diverse but educationally homogeneous was the sample size of 392. The age groups of 18 to 25 and 26 to 35 years made up the two biggest categories, at 45.4 percent and 33.2 percent respectively, making up almost 79 percent of the whole population sampled. Almost an equal representation was observed when looking at gender; 50.8 percent were female respondents while 49.2 percent were male respondents. In terms of residency, rural respondents were the largest group (35.5%), followed by urban (32.9%) and semi-urban (31.6%) respondents.

Educationally, the respondents had good levels of education since undergraduates (45.9%) and postgraduates (37.8%) made up approximately 84 percent of the whole sample, while those with secondary school level education (diploma or less), and none at all, were 16 percent. Occupation wise, students (37.5%) were in the largest proportion, followed by people working in business and those who were self-employed (25.8%), and salaried professionals (23.0%). Agricultural/ allied and non-working respondents made up small proportions of the sample at 8.4% and 5.4% respectively.

5.2 Comparison of Self-Reported and Objective Cybersecurity Awareness

There arises an interesting revelation upon the comparison of self-reported and objective cybersecurity awareness measurements. Upon being asked directly about cybersecurity awareness, 46.2% indicated 'Yes' while 29.3% indicated 'Somewhat', implying that close to 75% believed they have knowledge in cybersecurity. Upon conducting objective measurement using the CAIN questions, however, the results are completely flipped where 54.59% were classified as 'Not Aware', compared with only 45.41% as 'Aware'. The gap of 9.18 percentage points between self-reported and objective cybersecurity awareness confirms the 'knowledge-action gap' hypothesis.

5.3 ANOVA: Determinants of Cybersecurity Knowledge (CAIN Score)

Table 2: One-Way ANOVA — CAIN Score by Demographic Variable

One-Way ANOVA: CAIN Score by Demographic Variable							
Variable	**Group**	**N**	**Mean**	**SD**	**F Value**	**p Value**	**Sig.**
Age	Below 18	16	20.13	7.238	5.685	0.000	***
	18–25	178	20.99	7.988			
	26–35	130	16.96	7.195			
	36–50	57	19.04	6.579			
	Above 50	11	18.18	2.994			
Place of Residence	Urban	129	19.42	8.525	4.983	0.007	**
	Rural	139	20.55	7.212			
	Semi-Urban	124	17.64	6.673			
Occupation	Student	147	20.81	9.004	4.785	0.001	***
	Salaried Professional	90	18.51	6.201			
	Business & Self-Employed	101	17.27	5.680			
	Agriculture & Allied	33	21.64	6.954			
	Non-Working	21	17.43	8.447			
Educational Qualification	School Level	17	18.12	4.986	6.226	0.000	***
	Diploma	40	17.30	4.386			
	Undergraduate (UG)	180	17.93	7.189			
	Postgraduate (PG)	148	21.64	8.537			

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 ||SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

	No Formal Education	7	17.14	2.795			
Internet Access Device	Smartphone	182	21.13	7.720	7.294	0.000	***
	Laptop / Desktop	153	17.54	7.698			
	Tablet	43	17.72	5.708			
	Basic Feature Phone	14	18.36	3.455			
Cybersecurity Awareness	Yes	181	20.78	8.760	6.964	0.001	***
	No	96	17.92	5.736			
	Somewhat	115	17.98	6.492			
*** $p < 0.001$ ** $p < 0.01$ * $p < 0.05$ (CAIN Score range: 0–46; higher = greater cybersecurity knowledge)							

Source: Primary Data

The one-way ANOVA showed a significant variation in the average scores in several demographic variables. Age was found to be significantly correlated ($F = 5.685$, $p<0.001$), as the highest CAIN Score average was found among those aged between 18 to 25 years old (Mean = 20.99) compared to those from the 26 to 35-year age group whose average scores were significantly lower (Mean = 16.96). This implies that there exists a non-linear relationship between age and cybersecurity awareness, where transitions from early to mid-career stages may result in disinterest in security issues. Place of residence was another significant variable ($F = 4.983$, $p = 0.007$). Rural dwellers recorded the highest average scores (Mean = 20.55), urban dwellers recorded an average score (Mean = 19.42), and semi-urban dwellers recorded the lowest score (Mean = 17.64).

Occupation was another important variable that showed a statistically significant effect on CAIN Scores ($F = 4.785$, $p = 0.001$). The participants who worked in agriculture and allied services had the highest mean score (M = 21.64) because digital instruments used by this group of participants could be described as more practical and transactional (digital transactions, applications for agriculture). The lowest score (M = 17.27) belonged to business persons and self-employed people. Educational qualification was identified as one of the main factors influencing CAIN Scores ($F = 6.226$, $p < 0.001$). Postgraduates achieved the highest scores (M = 21.64), whereas uneducated respondents got the lowest scores (M = 17.14). Another independent variable that had an impact on CAIN Score was the way of accessing the internet ($F = 7.294$, $p < 0.001$). Those who had smartphones received the highest score (M = 21.13) than laptop/desktop users (M = 17.54).

5.4 ANOVA: Predictors of Cybersecurity Practice Scores

The practice scores showed a different trend. Notably, there was no statistically significant effect of the participants' place of residence on their practice scores ($F = 0.695$, $p = 0.500$), with residents from rural, urban, and semi-urban areas displaying an almost identical behavioural pattern. In other words, it seems that the digital divide in cybersecurity behaviour, which is commonly associated with the digital lagging behind by people living in the countryside, has diminished significantly among participants from the Coimbatore District, probably because they all own smartphones.

Significant variations in the participants' practice scores were observed for age ($F = 3.312$, $p = 0.011$), occupation ($F = 5.574$, $p < 0.001$), and educational qualification ($F = 2.937$, $p = 0.021$), whereas there were no such differences in regard to the participants' method of internet access ($p = 0.211$) and awareness of the cybersecurity topic ($p = 0.207$). The lack of a significant effect of awareness on cybersecurity behaviour confirms the knowledge-practice gap.

5.5 ANOVA: Factors Influencing Cybersecurity Attitude

Attitude ratings did not vary much based on demographics. Occupation was the only factor that had any influence ($F = 4.133$, $p = 0.003$). Agricultural workers and allied occupations had the most concern-based attitudes (M = 23.03), whereas salaried employees had the least concern for cybersecurity (M = 20.02). This could be attributed to their being used to security processes in an organizational setting. Age, place of residence, level of education attained, source of internet access, and awareness all proved to be non-significant factors in predicting attitude differences towards cyber insecurity. The results show that there is wide concern about cyber dangers among individuals irrespective of their demographic makeup—findings that support those by Supti et al. (2025).

5.6 Threat Recognition: Weighted Average Analysis

The use of weighted averages in threat recognition yielded a clear hierarchy. Phishing, which had a weighted average score of 120.67, and identity theft, with a weighted average of 118.00, came out on top due to their visibility in the mass media and because they often involve fraudulent communications. In third place came extortion with a score of 115.83, after which came Denial-of-Service (DoS) attacks and hate speech/radicalization (both scored 111.17), and finally, malware and viruses, with an overall score of 105.50. The relatively low score for malware can be attributed to "background normalisation," where the individual knows that anti-virus programs exist and function automatically, lowering awareness about their threat level.

6. DISCUSSION

The overall result of this study is a picture of superficial awareness existing alongside substantive knowledge gaps. Despite the very high educational levels of Coimbatore District respondents—with over 80% possessing at least an undergraduate degree—their levels of objective cybersecurity knowledge remained low. This corroborates Taherdoost's (2024) observation that higher general education levels cannot translate to security literacy; rather, special training must be sought.

Geographic homogeneity of practice scores emerges as possibly the most practically relevant aspect of this study. Interventions designed for raising security awareness among

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 ||SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

rural populations, under the assumption that such populations lag behind urban populations, could be misdirecting efforts. Instead, age (specifically 35+ and 50+) occupation (specifically those on salary and unemployed), and education levels (specifically diploma and school levels) could matter more.

Since knowledge is not leading to any kind of behaviour change, there should be some other way in which such programs must design themselves. The work done by Chaudhary (2024), who talks about nudge theory and protection motivation, along with the evidence-based framing strategies mentioned in the work of de Bruijn and Janssen (2017) and Keller et al.'s (2025) study on the use of digital educational escape rooms, indicate that such game-based interventions that can be customized based on the local context and language will yield more behavioural changes.

Another very interesting result from this analysis is the very good results obtained by agriculture and allied workers when it comes to knowledge and attitudes, despite them not being considered to have high levels of digital literacy. This could be attributed to the increasing availability of digital payments platforms, apps for farmers that help give advice, and the portals provided by the government that deal with social welfare issues.

This insight is pertinent to the accomplishment of the three SDGs: SDG 4 should take into consideration that learning should extend beyond the classroom setting; SDG 10 should note that it cannot be automatically assumed that rural occupation-based communities are the most vulnerable to digital exclusion; and SDG 16 should make use of the occupation and community network structures as trusted communicators on matters of cybersecurity.

7. CONCLUSION

In this way, this study provides an empirical examination of cybersecurity awareness in the Coimbatore District in line with three SDGs. The first conclusion relates directly to the first chosen SDG. Knowledge deficiencies are common even amongst respondents with high levels of education (SDG 4). As such, cybersecurity awareness must be cultivated through domain-specific education programs that are accessible and provided in regional languages. It is not something that can automatically be derived from education alone.

The second conclusion relates directly to the second SDG. It seems that there is no longer a statistically significant digital divide in the implementation of security practices between urban, rural, and semi-urban areas (SDG 10). It is now time for policy to direct its attention from geographic to demographic inequalities.

Thirdly, the knowledge-action gap is the main behavioural obstacle (SDG 16). Knowing better and feeling differently does not necessarily translate to action; structures must exist to motivate, demand, and facilitate safe cyber practices. As a remedy, this study suggests an intervention framework spanning three sectors: government ministries undertaking cybersecurity advocacy and making cybercrime complaints easier (SDG 16); schools implementing a comprehensive approach of cybersecurity through curriculum integration at all levels of education (SDG 4); and finally, the finance sector adopting AI technology for fraud detection and gaming apps for teaching financial literacy to all demographics (SDG 10). This will not only address cybersecurity issues in Coimbatore but also contribute to sustainable development efforts as a whole.

Future studies need to explore how such an approach performs longitudinally by measuring the effectiveness of specific interventions that have been made, increase its geographical range beyond the specific districts and states covered here, and use qualitative analysis to identify the informal pathways to success in cybersecurity that agricultural workers use.

REFERENCES

1. *Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031.*
2. *AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2024). FinTech cybersecurity challenges and regulations: Bahrain case study. Journal of Computer Information Systems, 64(6), 835–851.*
3. *Alharbi, A., Alshammari, A., & Alotaibi, M. (2024). Cybersecurity awareness among students. [Proceedings/Journal reference].*
4. *Alharthi, A., Alenezi, M., & Alrasheed, M. (2024). Digital transformation and cybersecurity challenges. [Proceedings/Journal reference].*
5. *Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016.*
6. *Chang, V., Golightly, L., Xu, Q. A., Boonmee, T., & Liu, B. S. (2023). Cybersecurity for children: An investigation into the application of social media. Enterprise Information Systems, 17(11), 2188122.*
7. *Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. Computers & Security, 142, 103858.*
8. *Creese, S., Dutton, W. H., Esteve-González, P., & Shillair, R. (2021). Cybersecurity capacity-building: Cross-national benefits and international divides. Journal of Cyber Policy, 6(2), 214–235.*
9. *de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1–7.*
10. *Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. Computers & Security, 73, 345–358.*
11. *Keller, T., Guggemos, J., & Warwas, J. (2025). Digital educational escape rooms as a novel approach to cybersecurity education. Computers in Human Behaviour Reports, 20, 100785.*
12. *Pimentel, J. et al. (2026). The implementation of public chatbots to raise awareness of computer crime. [Proceedings/Journal reference].*
13. *Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, 100343.*
14. *Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon, 9(3), e14234.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 ||SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

15. *Supti, T. I., Khan, K. M., Yankouskaya, A., Abuelezz, I., Barhmagi, M., Erbad, A., & Ali, R. (2025). Examining the role of self-construal on cybersecurity attitudes and perceptions of vulnerability. Journal of Applied Security Research, 20(3), 355–381.*
16. *Taherdoost, H. (2024). A critical review on cybersecurity awareness frameworks and training models. Procedia Computer Science, 235, 1649–1663.*
17. *Tempestini, G., Rovira, E., Pyke, A., & Di Nocera, F. (2023). The Cybersecurity Awareness Inventory (CAIN): Early phases of development of a tool for assessing cybersecurity knowledge based on the ISO/IEC 27032. Journal of Cybersecurity and Privacy, 3(1), 61–75.*