Open Access Research Journal of
Multidisciplinary Studies
Journals home page: https://oarjpublication/journals/oarjms/
ISSN: 2783-0268 (Online)

(REVIEW ARTICLE)

Advancing cybersecurity awareness programs: A model for sustainable digital literacy in underserved communities

Sikirat Damilola Mustapha [1,*] and Abidemi Adeleye Alabi [2]

[1] *Kwara State University, Malete, Nigeria.*
[2] *Ericsson Telecommunications Inc., Lagos, Nigeria.*

Open Access Research Journal of Multidisciplinary Studies, 2022, 03(02), 111-128

Publication history: Received on 05 March 2022; revised on 14 April 2022; accepted on 16 April 2022

Article DOI: https://doi.org/10.53022/oarjms.2022.3.2.0048

Abstract

Cybersecurity threats continue to evolve, posing significant risks to individuals, organizations, and communities, particularly those in underserved regions. These communities often face barriers to accessing reliable digital literacy programs, leaving them vulnerable to cyber threats and data breaches. This study explores the development of an innovative model for advancing cybersecurity awareness programs tailored to underserved communities, emphasizing sustainable digital literacy and long-term resilience. The proposed model integrates context-specific educational tools, community-driven engagement strategies, and partnerships with local organizations and stakeholders to address unique challenges in these areas. By focusing on accessibility, cultural relevance, and practical application, the model aims to bridge the digital literacy gap, fostering a more inclusive approach to cybersecurity education. Key components of the model include localized content development, gamified learning techniques, and continuous capacity-building initiatives. Additionally, the program leverages digital platforms and mobile technology to extend its reach, ensuring scalability and adaptability. The study evaluates pilot programs implemented in selected underserved communities, assessing their impact on participants' cybersecurity awareness, knowledge retention, and practical skills. Findings demonstrate that community-tailored approaches significantly enhance participants' ability to recognize and mitigate common cybersecurity threats such as phishing, ransomware, and identity theft. Furthermore, the integration of culturally relevant teaching methods and mobile learning technologies proves instrumental in increasing engagement and reducing barriers to participation. The study concludes with recommendations for policymakers, educators, and technology providers on fostering sustainable digital literacy through collaborative efforts. By addressing the unique needs of underserved communities, the proposed model contributes to narrowing the cybersecurity awareness gap and promoting equitable access to safe digital practices.

Keywords: Cybersecurity Awareness; Digital Literacy; Underserved Communities; Sustainable Education; Digital Inclusion; Gamified Learning; Capacity-Building; Community Engagement; Cybersecurity Threats; Scalable Programs

1. Introduction

In today's increasingly connected world, cybersecurity awareness has become a critical aspect of personal, organizational, and national security. As digital platforms and services continue to expand globally, the threats posed by cybercrime, data breaches, and identity theft are growing exponentially. While individuals in urban and economically advanced regions are gaining greater access to digital security tools, underserved communities often remain vulnerable due to limited access to digital literacy education and cybersecurity training (Adepoju, et al., 2022, Bifulco, et al., 2022, Huang, et al., 2022). These communities face a wide range of challenges, including limited technological infrastructure, low internet penetration, and inadequate cybersecurity knowledge, all of which contribute to their heightened susceptibility to cyber threats.

* Corresponding author: Sikirat Damilola Mustapha

This disparity in digital literacy presents a significant issue, as underserved populations are often unaware of the risks they face online and lack the necessary skills to protect themselves. The absence of proper cybersecurity awareness programs in these communities can result in a perpetuating cycle of vulnerability, as individuals become targets of phishing, identity theft, and other forms of cybercrime. Addressing this gap is crucial for ensuring that no community is left behind in the fight against digital threats (Alsrehin, Klaib & Magableh, 2019, Jiang, et al., 2021).

The primary objective of this study is to develop a sustainable model for cybersecurity awareness tailored specifically for underserved communities. By focusing on culturally relevant educational content and employing accessible delivery methods, the model aims to foster long-term digital literacy and security practices. The approach will emphasize scalable, community-driven strategies that prioritize engagement and retention, ensuring that cybersecurity education becomes a lasting part of these communities' digital development (Ganesh & Xu, 2022, Gudala, et al., 2022, Pavel, Tan & Abdullah, 2022). Additionally, the model will address the digital literacy gap by integrating innovative teaching methods, such as gamified learning and mobile-based platforms, which can reach a broader audience in regions with limited infrastructure.

The significance of this effort lies in its potential to enhance digital safety across underserved communities, promoting inclusivity and empowering individuals with the knowledge and skills necessary to navigate the digital world securely. By advancing cybersecurity awareness, we can create a more resilient and informed digital society, reducing the risks and challenges posed by cyber threats in vulnerable populations (Lim & Taeihagh, 2018, Magyari, et al., 2021, Singh & Kathuria, 2021).

2. Literature Review

The rapid expansion of digital technology has brought about significant changes in society, transforming how we communicate, work, and access information. As the digital landscape evolves, so too does the nature of cybersecurity threats. Cyberattacks, such as phishing, ransomware, identity theft, and data breaches, have become increasingly sophisticated and prevalent. For many individuals in underserved communities, particularly those in rural areas or low-income regions, the dangers of cybersecurity threats are heightened due to limited digital literacy and access to reliable security tools (Abughalieh & Alawneh, 2020, Chen, Wawrzynski & Lv, 2021). In this context, cybersecurity awareness becomes a critical tool for mitigating the risks associated with online interactions. However, while the digital divide persists, it is essential to understand both the nature of these threats and the barriers faced by underserved communities to better design and implement effective cybersecurity awareness programs.

Cybersecurity threats are diverse and rapidly evolving, posing challenges for users across the globe. Phishing, one of the most common types of attack, involves deceiving individuals into revealing sensitive information, such as passwords, by pretending to be a trustworthy entity. Other prevalent threats include ransomware, where malicious software is used to lock users' data and demand payment for its release, and identity theft, which can lead to financial ruin and identity fraud (Adeniran, et al., 2022, Chauhan, et al., 2022, Wang, 2022). In underserved communities, individuals are often targeted by cybercriminals because they are less likely to recognize or understand these types of threats, making them more vulnerable to exploitation. For example, a user may unwittingly click on a fraudulent link in an email or download a malware-infected app because they lack the knowledge to distinguish between legitimate and malicious content. Additionally, deepfake technology and synthetic media are emerging threats that exploit the ability to fabricate convincing images, videos, and audio. These new technologies are not only used to create deceptive content for malicious purposes but can also compromise personal privacy and security by manipulating users into revealing personal information or falling for scams (Arvin, Kamrani & Khattak, 2019, Camara, et al., 2020, Wang, et al., 2020). In the face of these threats, cybersecurity awareness becomes a vital tool for preventing attacks and empowering individuals to make informed decisions about their online behavior. Muhirwe & White, 2016, presented the Path Coefficients as shown in figure 1.

While cybersecurity threats continue to evolve, the issue of digital literacy in underserved communities remains a significant concern. Digital literacy, which encompasses the knowledge and skills required to navigate the digital world securely and responsibly, is a critical determinant of an individual's ability to protect themselves online. However, underserved communities often lack access to the necessary resources to acquire these skills, exacerbating their vulnerability to cyber threats (Agu, et al., 2022, Kussl & Wald, 2022, Yuan, et al., 2022). Factors such as low internet penetration, limited access to devices, and inadequate infrastructure contribute to the digital divide, which disproportionately affects marginalized groups. Moreover, even when access to digital technology is available, many individuals in underserved regions have limited experience with online safety practices, making them ill-prepared to recognize and respond to cybersecurity risks.

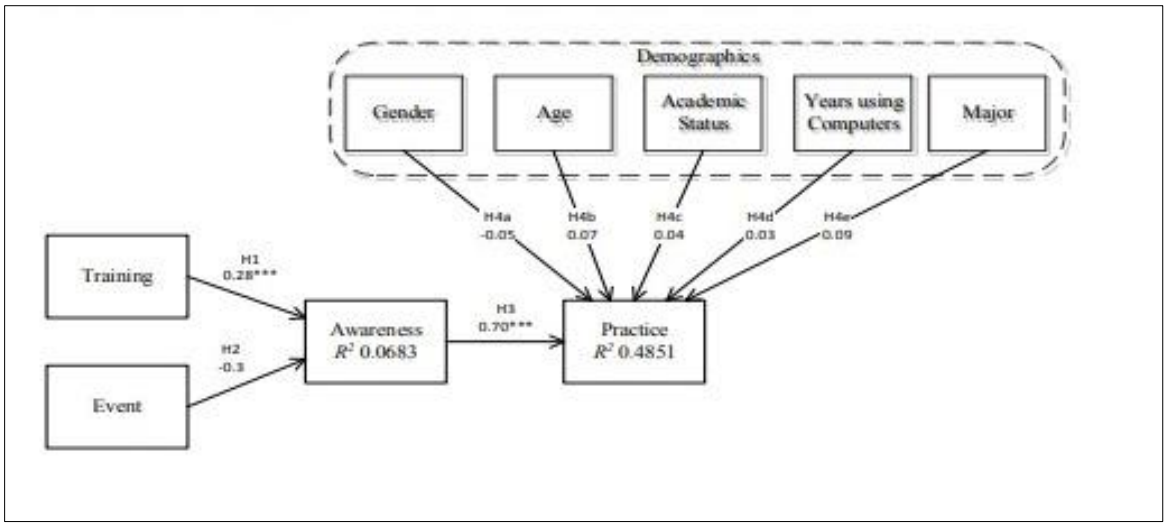

Figure 1 Path Coefficients (Muhirwe & White, 2016)

In addition to technological barriers, cultural and educational factors play a crucial role in shaping digital literacy in underserved communities. In many cases, digital literacy programs are not tailored to the specific needs or contexts of these communities, leading to disengagement or ineffective learning outcomes. For example, a generic cybersecurity training program may not resonate with individuals who have limited formal education or experience with technology, making it difficult for them to grasp complex cybersecurity concepts. Furthermore, language barriers and low levels of education in these communities may hinder the effectiveness of training programs (Pawar & Patil, 2017, Shirazi & Morris, 2016, Zhang & Fu, 2020). There is also the challenge of overcoming skepticism about the need for cybersecurity education, as some individuals may not perceive digital threats as immediate concerns due to a lack of awareness or understanding of their potential consequences. Without effective, culturally relevant interventions, these communities remain at a higher risk of becoming victims of cybercrime. The Five Main Functions of Cyber Security Framework presented by Perwej, et al., 2021, is shown in figure 2.

Figure 2 The Five Main Functions of Cyber Security Framework (Perwej, et al., 2021)

While several initiatives have been developed to improve cybersecurity awareness in underserved communities, these programs often fall short in terms of scale, reach, and sustainability. One such initiative is the National Cybersecurity Awareness Month (NCSAM), which has aimed to raise awareness of cybersecurity risks and promote safe online behavior. However, NCSAM and similar campaigns tend to be short-term efforts that do not provide lasting education or practical tools for individuals in underserved areas. These programs often target a broader audience without addressing the unique needs of marginalized communities, leaving gaps in outreach and engagement (Hamdar, Qin & Talebpour, 2016, Kolekar, et al.,, 2021). Additionally, many existing programs rely heavily on formal educational settings, which may not be accessible or appealing to individuals who lack the resources or time to participate. Moreover, in some cases, the focus on general cybersecurity awareness does not go far enough in teaching specific, actionable skills that can help individuals protect themselves from the most common online threats.

To address these shortcomings, more tailored, sustainable approaches are needed that provide long-term solutions to the digital literacy gap in underserved communities. One such approach is the integration of mobile technology into cybersecurity awareness programs. Given the widespread use of smartphones, particularly in areas where access to computers is limited, mobile-based solutions can provide an effective means of delivering cybersecurity education. Mobile platforms can deliver training in a format that is accessible and engaging, enabling individuals to learn at their own pace and revisit content as needed (Asaithambi,Kanagaraj & Toledo, 2016, Chen, Wawrzynski & Lv, 2021, Efunniyi, et al., 2022). Additionally, mobile-based programs can be easily scaled and updated, ensuring that participants have access to the most current information about emerging cybersecurity threats.

Sustainability in digital education is also an essential consideration when designing cybersecurity awareness programs. Traditional, one-off training sessions are insufficient for addressing the ongoing nature of cybersecurity threats. Instead, sustainable programs must emphasize continuous learning and adaptation to changing digital environments. Best practices for creating sustainable digital literacy programs include the use of community-based models that encourage peer learning, participation, and collaboration (Azadani & Boukerche, 2021, Ige, et al., 2022, Ojukwu, et al., 2022). In these models, local community leaders and educators can play a key role in delivering content, ensuring that the training resonates with participants and aligns with local cultural contexts. Peer-to-peer education can also enhance the effectiveness of these programs by allowing individuals to share knowledge, experiences, and solutions to common challenges. This model has the potential to create a more engaging and supportive learning environment, which is essential for long-term success.

Furthermore, sustainability in digital education can be achieved by leveraging existing infrastructure and partnerships. Collaborations between local governments, NGOs, and private sector entities can help pool resources and extend the reach of cybersecurity awareness programs. For instance, partnerships with mobile service providers could enable the distribution of cybersecurity training through SMS or mobile apps, making it more accessible to individuals who may not have access to high-speed internet or advanced devices (Charouh, et al., 2022, Chauhan, et al., 2022). Additionally, incorporating cybersecurity into the broader context of digital inclusion, such as efforts to improve internet access and digital skills, can help ensure that digital literacy programs address the full range of challenges faced by underserved communities.

The concept of integrating sustainable, community-driven cybersecurity education into underserved communities holds significant promise for bridging the digital literacy gap. By building on existing models and adapting them to the unique needs of these populations, it is possible to empower individuals with the knowledge and skills needed to protect themselves from cyber threats (Agu, et al., 2022, Lim & Taeihagh, 2018, Samira, et al., 2022). The success of such initiatives relies on designing programs that are culturally relevant, accessible, and adaptable, ensuring that individuals in underserved communities are not left behind in the digital age. Ultimately, advancing cybersecurity awareness in these areas not only strengthens personal security but also contributes to the broader goal of fostering a more inclusive, digitally secure society.

3. Theoretical Framework

The development of effective cybersecurity awareness programs for underserved communities requires a comprehensive theoretical framework that integrates various models of education, behavior change, and digital inclusion. By understanding the unique challenges faced by these communities, including limited access to technology, educational resources, and digital skills, it becomes possible to create programs that address these gaps while promoting long-term sustainability (Abdi & Meddeb, 2018, Fu & Liu, 2020, Nikitas, et al., 2020). This theoretical framework brings together community-centric education models, behavioral change theory, and the digital inclusion paradigm, all of which are essential for developing a holistic approach to advancing cybersecurity awareness in underserved areas.

A community-centric education model is grounded in the belief that learning is most effective when it is contextually relevant, culturally sensitive, and delivered in ways that engage and empower local communities. Such models emphasize the importance of local involvement in designing, implementing, and sustaining educational initiatives, as well as the role of community leaders and stakeholders in fostering trust and engagement (Mozaffari, et al., 2020, Muresan, 2021, Olayode, et al., 2020). In underserved communities, traditional top-down approaches to education often fail to resonate with individuals who are disconnected from formal educational systems or who face barriers such as language, socio-economic status, or limited access to digital resources. A community-centric approach recognizes that knowledge must be co-created with the community, rather than imposed from external sources. By engaging community members in the process, education becomes more meaningful, practical, and relevant to their daily lives.

In the context of cybersecurity awareness, community-centric education can take many forms, such as training programs led by local facilitators, peer-to-peer learning networks, and mobile-based platforms that reach individuals where they are. Community leaders and trusted figures within the community can serve as conduits for disseminating cybersecurity knowledge, as they are more likely to have the trust and credibility needed to influence behaviors (Li, Elefteriadou & Ranka, 2014, Mena-Yedra, 2020, Yuan, et al., 2019). Furthermore, localizing cybersecurity content ensures that it addresses the specific risks and concerns faced by the community, rather than relying on generic materials that may not be relatable or actionable. For example, in rural areas with limited internet connectivity, educational content might focus on protecting devices from offline threats, such as physical theft or unauthorized access. In urban settings with high internet penetration, the focus may shift to online safety and digital privacy. By tailoring content to the specific needs of the community, community-centric models ensure that cybersecurity awareness is both accessible and actionable.

Behavioral change theory is another key component of the theoretical framework for advancing cybersecurity awareness. At its core, behavioral change theory focuses on understanding how individuals make decisions and what factors influence their actions. In the context of cybersecurity, the goal is to not only raise awareness of digital threats but also to promote lasting changes in online behavior (Hunter, 2022, Wang, 2022). One of the central tenets of behavioral change theory is that individuals are more likely to adopt new behaviors when they perceive a clear benefit, understand the consequences of their actions, and feel supported in making the change. For cybersecurity awareness programs to be effective, they must go beyond simply providing information about risks; they must also motivate individuals to adopt protective behaviors and incorporate them into their daily routines.

The most widely used models for understanding and promoting behavioral change include the Health Belief Model, the Theory of Planned Behavior, and the Social Cognitive Theory. Each of these models emphasizes the importance of perceived susceptibility to a threat, perceived severity of the threat, and the benefits of adopting protective behaviors. In the case of cybersecurity, individuals may need to understand the risks of cyberattacks, such as financial loss, identity theft, or privacy violations, and weigh these risks against the perceived inconvenience or difficulty of adopting cybersecurity practices, such as using strong passwords or avoiding suspicious links (Peng, et al., 2020, Rui & Yan, 2018, Silasai & Khowfa, 2020). Effective programs should highlight the potential consequences of not adopting protective measures, while also demonstrating the ease and benefits of taking simple actions to secure one's digital life.

For example, programs that incorporate interactive and practical activities, such as workshops on creating strong passwords or simulating phishing attacks, can help individuals develop the skills needed to protect themselves online. Additionally, programs should provide ongoing support and reinforcement, helping individuals to internalize cybersecurity habits over time. This might involve regular reminders, updates on emerging threats, or opportunities for individuals to share their experiences and learn from others (Galterio, Shavit & Hayajneh, 2018, Hara, et al., 2021). By integrating behavioral change theory into cybersecurity education, programs can increase the likelihood that participants will not only understand the risks but also adopt sustainable practices to mitigate those risks. The Goal-Question-Outcomes (GQO)+Strategies Approach for Cybersecurity Education and Training Curricula Improvement and Alignment to Cybersecurity Strategic Goals as AlDaajeh, et al., 2022, is shown in figure 3.

The digital inclusion paradigm is an essential element of the theoretical framework, as it ensures that cybersecurity awareness programs are accessible and equitable, especially for underserved communities. Digital inclusion refers to the idea that all individuals, regardless of their socio-economic background, geographic location, or physical ability, should have the opportunity to access and benefit from digital technologies. It encompasses not only access to devices and the internet but also the skills, knowledge, and confidence needed to use technology effectively and safely (Adeniran, et al., 2022, Nikitas, et al., 2020). In the context of cybersecurity, digital inclusion is crucial because individuals who lack digital literacy or who are excluded from the digital world are more likely to be unaware of online risks and unable to take necessary precautions.

For cybersecurity programs to be truly effective, they must be designed with accessibility in mind. This means that educational materials should be available in multiple formats, such as text, video, and audio, and should be accessible on a variety of devices, including smartphones, which are the most widely used technology in underserved communities. Additionally, programs must take into account factors such as language barriers, varying levels of educational attainment, and cultural differences that may impact how individuals understand and engage with cybersecurity concepts (Austin-Gabriel, et al., 2021, Guo,Li & Ban, 2019, Tian, et al., 2020). For example, offering cybersecurity training in local languages, using culturally relevant examples, and ensuring that the materials are appropriate for individuals with low literacy levels can significantly improve the effectiveness of the program.

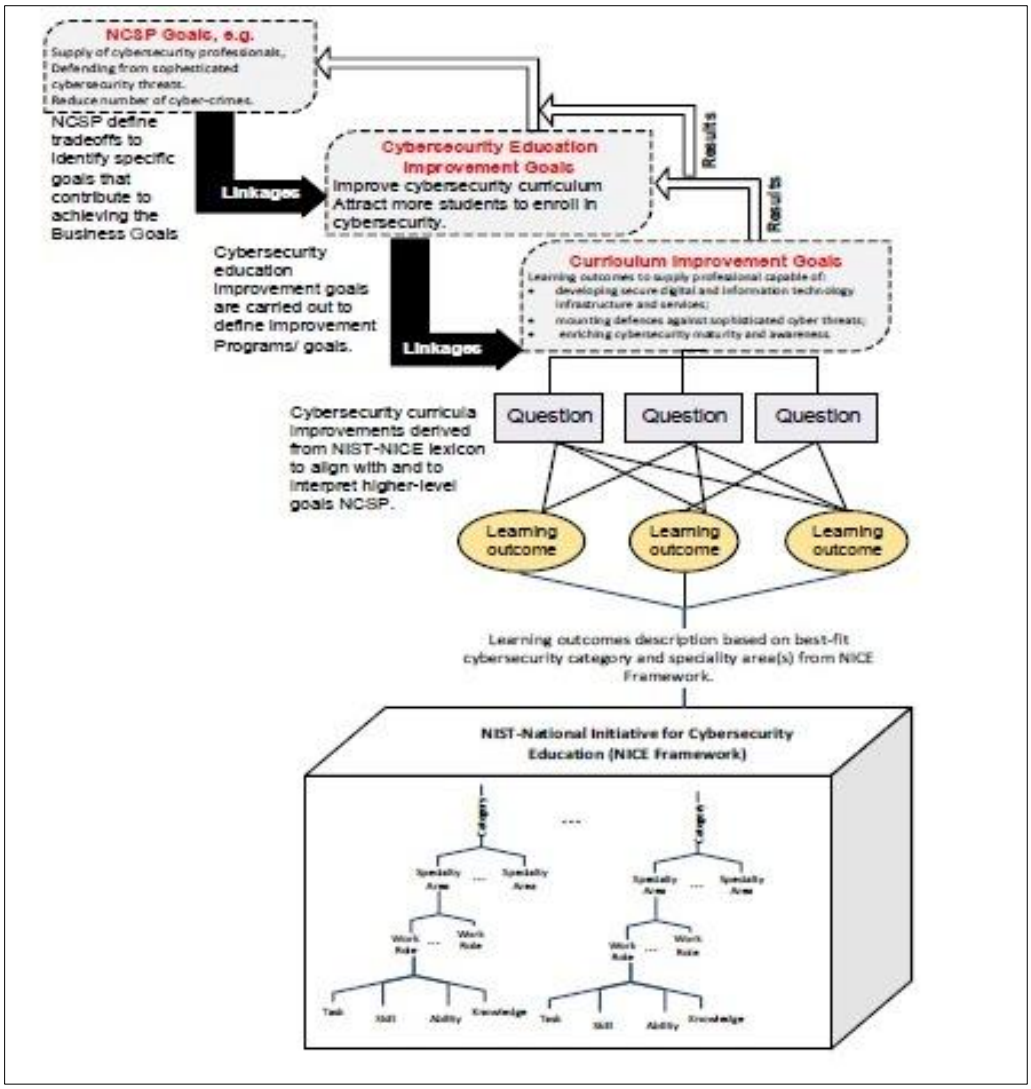

Figure 3 (GQO)+Strategies Approach for Cybersecurity Education and Training Curricula Improvement and Alignment to Cybersecurity Strategic Goals (AlDaajeh, et al., 2022)

Digital inclusion also involves addressing the affordability and availability of technology. In underserved communities, many individuals may not have access to high-speed internet or personal computers, which can create barriers to participation in online cybersecurity training programs. To overcome these barriers, programs can leverage mobile technology and offline resources, such as SMS-based alerts or printed guides, to reach individuals who may not have access to the internet or who live in areas with limited connectivity. In addition, collaborations with local organizations, governments, and private sector partners can help to expand access to digital tools and resources, ensuring that individuals in underserved communities have the infrastructure needed to participate in cybersecurity education.

Ultimately, the digital inclusion paradigm underscores the importance of creating an equitable digital ecosystem in which everyone, regardless of their background, has the opportunity to learn about cybersecurity, stay informed about risks, and take proactive steps to protect themselves online. Without a focus on inclusion, cybersecurity awareness programs may inadvertently perpetuate existing disparities, leaving certain groups more vulnerable to cyber threats.

Together, these three elements—community-centric education models, behavioral change theory, and the digital inclusion paradigm—form a robust theoretical framework for advancing cybersecurity awareness programs in underserved communities. By designing programs that are relevant to the local context, that motivate and support lasting behavioral changes, and that ensure equitable access to digital resources, it is possible to create a sustainable model for improving digital literacy and promoting cybersecurity in these communities (Alzubaidi & Kalita, 2016, Baheti, Gajre & Talbar, 2018). This approach not only helps individuals protect themselves from cyber threats but also contributes to the broader goal of creating a more digitally inclusive and secure society.

3.1. Proposed Model for Cybersecurity Awareness

Advancing cybersecurity awareness programs to foster sustainable digital literacy in underserved communities is an urgent need in our increasingly interconnected world. As digital technology permeates every facet of life, the risks associated with cyber threats grow exponentially. For individuals in underserved communities, however, the barriers to understanding and mitigating these risks can be insurmountable. A holistic approach to cybersecurity awareness, grounded in the unique needs and resources of these communities, is essential for addressing these gaps and empowering individuals to navigate the digital landscape safely.

A proposed model for advancing cybersecurity awareness programs focuses on integrating core components that are tailored to the specific needs and circumstances of underserved populations. By utilizing localized content development, gamified learning techniques, mobile technology, and continuous capacity-building initiatives, this model aims to create a sustainable foundation for digital literacy. These components are designed to not only educate individuals but also inspire them to adopt secure online practices as a way of life (Aksjonov & Kyrki, 2021, Soomro, et al., 2019, Tawari, Mallela & Martin, 2018).

Localized content development is crucial for creating relevant and relatable cybersecurity awareness programs. For underserved communities, particularly those that may have limited access to formal education or technological resources, the key to effective engagement lies in ensuring that the content resonates with their lived experiences. By developing materials that reflect local languages, cultural nuances, and community-specific digital behaviors, these programs can enhance understanding and encourage participation (Ojukwu, et al., 2022, Torbaghan, et al., 2022). Furthermore, content should address issues that are directly relevant to the community, such as protecting personal data on mobile devices, identifying common online scams, and securing access to public services through digital platforms. When community members see that the information being presented is pertinent to their daily lives, they are more likely to internalize the concepts and adopt safe practices.

Gamified learning techniques offer another powerful tool in fostering digital literacy. The use of games, simulations, and interactive learning experiences makes the process of acquiring cybersecurity skills more engaging, enjoyable, and memorable. This approach taps into the inherent human affinity for play while simultaneously reinforcing key security concepts, such as password management, recognizing phishing attempts, and understanding the importance of software updates (Mukherjee & Mitra, 2019, Neal & Woodard, 2016, Sun & Elefteriadou, 2014). Gamification can also introduce a competitive element, motivating individuals to apply what they have learned in a fun and challenging environment. This strategy is especially effective in communities where traditional forms of learning might be seen as dull or unappealing. Additionally, games can be designed to work across a range of devices, ensuring that individuals who may not have access to computers but own mobile phones can still benefit from the program.

The integration of mobile technology is vital in reaching underserved populations, where access to computers and broadband internet may be limited. Mobile phones, however, are ubiquitous and serve as a primary gateway to the internet for many individuals in these communities. By creating mobile-friendly cybersecurity awareness programs, organizations can ensure that digital literacy initiatives are accessible to a broader audience. Mobile applications, text-based services, and multimedia content such as videos and podcasts are just a few examples of how technology can be used to deliver valuable cybersecurity knowledge (Petraki, Ziakopoulos & Yannis, 2020, Rodrigues, et al., 2018). These mobile-first approaches are not only cost-effective but also ensure that the learning materials are available anytime, anywhere, giving users the flexibility to engage with the content at their convenience. Additionally, mobile platforms can be used to push regular security reminders and updates, keeping individuals informed about emerging threats and best practices.

Continuous capacity-building initiatives are essential for the long-term success of any cybersecurity awareness program. Cybersecurity is a rapidly evolving field, and what is considered secure today may be vulnerable tomorrow. For individuals in underserved communities to stay ahead of cyber threats, it is important that education does not end with an initial training session. Instead, programs should focus on providing ongoing learning opportunities, such as regular workshops, webinars, and refresher courses. These initiatives can be designed to keep participants informed about the latest threats, security practices, and tools available to protect themselves online (Adeniran, et al., 2022, Benrachou, et al., 2022, Kussl & Wald, 2022). In addition to formal learning, capacity-building should include peer-to-peer education, where community members who have mastered certain cybersecurity concepts can share their knowledge with others. This creates a culture of learning and mutual support, strengthening the overall resilience of the community against cyber risks.

Stakeholder involvement plays a critical role in ensuring the success and sustainability of cybersecurity awareness programs. Community leaders, educators, and policymakers must be actively engaged in these initiatives to foster a supportive environment for digital literacy. Local leaders can act as champions for cybersecurity awareness, advocating for its inclusion in local schools, community centers, and public spaces. Educators can integrate cybersecurity topics into their curriculum, ensuring that future generations are equipped with the skills necessary to navigate the digital world securely (Amado, et al., 2020, Eom & Kim, 2020, Ni, 2020, Zhang, et al., 2020). Policymakers, on the other hand, can help create an enabling environment by allocating resources for digital literacy programs and encouraging public-private partnerships to bridge the digital divide. Their involvement can also extend to creating legislation and policies that promote digital safety and protect vulnerable groups from cyber threats.

Partnerships with technology providers and NGOs are also crucial in driving the success of cybersecurity awareness programs. Technology companies can lend their expertise and resources to help develop high-quality, accessible learning materials. They can also offer software and tools that can be used by individuals in underserved communities to protect themselves online, such as antivirus programs, password managers, and encrypted messaging apps. NGOs, particularly those with experience in community development and digital inclusion, can facilitate outreach efforts, help tailor programs to the specific needs of local populations, and ensure that resources are effectively distributed (Abou Elassad, et al., 2020, Ghanipoor Machiani, 2015, Ye, et al., 2018). By working together, these stakeholders can create a comprehensive and sustainable model for cybersecurity awareness that is both relevant and impactful.

In conclusion, advancing cybersecurity awareness in underserved communities requires a multifaceted approach that leverages localized content, interactive learning methods, and mobile technology. By focusing on continuous capacity-building and engaging a diverse group of stakeholders, this proposed model aims to create a sustainable digital literacy framework that empowers individuals to protect themselves and their communities from cyber threats. This model not only equips people with the knowledge they need to stay safe online but also fosters a culture of digital responsibility that can endure for generations to come (Huang, et al., 2022, Karbasi & O'Hern, 2022, Ozioko, Kunkel & Stahl, 2022). In an increasingly digital world, this type of education is not just a necessity but a vital step toward ensuring that all individuals, regardless of their circumstances, are equipped to thrive in the digital age.

4. Methodology

The methodology for advancing cybersecurity awareness programs in underserved communities is designed to ensure that the programs are both effective and sustainable in fostering digital literacy. This approach is grounded in understanding the unique needs and contexts of these communities and developing targeted strategies to improve their cybersecurity knowledge. A well-structured methodology is essential for evaluating the program's impact, refining its components, and ensuring that it achieves its intended outcomes.

A key aspect of the methodology is the use of a mixed-methods approach, combining both quantitative and qualitative research to provide a comprehensive understanding of how participants engage with the program and how their knowledge evolves. This combined approach allows for a deeper insight into the effectiveness of the program, capturing not only measurable changes in knowledge but also the lived experiences and perspectives of participants (Li, et al., 2020, Maldonado Silveira Alonso Munhoz, et al., 2020). The quantitative aspect can include surveys that measure specific knowledge gains, while qualitative data gathered through interviews and focus groups provide context and help explain the numbers behind the data.

The data collection phase is fundamental in shaping the development of the program and assessing its impact. Surveys and interviews with community members form the core of the data collection process, providing direct feedback from participants about their understanding of cybersecurity before and after engaging with the program. Surveys can be designed to evaluate knowledge about common cyber threats, best practices for securing digital devices, and awareness of online privacy issues (Maldonado Silveira Alonso Munhoz, et al., 2020, Vemori, 2020). These surveys can be administered both before the program begins (pre-assessment) and after its completion (post-assessment), allowing for an analysis of how much participants have learned and retained. Interviews can further deepen the understanding of the participants' experiences, revealing how well the program resonated with them, any barriers to learning they faced, and the aspects of the program they found most useful. These interviews can be semi-structured, allowing for flexibility while ensuring that key topics are covered.

Focus groups with educators and other stakeholders play a crucial role in the methodology. These groups provide an opportunity to gather insights from those involved in delivering the program and those who support it. Educators can offer feedback on the educational materials, teaching strategies, and the overall engagement of the participants. They can also highlight challenges they face in communicating complex cybersecurity concepts to underserved populations

and suggest ways to improve the training (AbuAli & Abou-Zeid, 2016, Essa, 2020, Katrakazas, et al., 2015). Stakeholders, such as community leaders and local policymakers, can provide valuable insights into the program's alignment with local needs, the potential for scaling it within the community, and the broader social and cultural factors that might affect its success. By gathering input from a diverse range of individuals involved in the program, the focus groups ensure that all aspects of the program are well-rounded and inclusive of different perspectives.

The pilot implementation of the cybersecurity awareness program is a critical step in testing its feasibility, effectiveness, and scalability. Selecting underserved communities for the pilot programs is a thoughtful process, as the chosen communities must represent a diverse range of socio-economic conditions, cultural backgrounds, and access to technology. Communities with varying levels of digital access should be prioritized to understand how the program performs across different contexts and what adjustments might be necessary (Zukarnain, Muneer & Ab Aziz, 2022). The pilot allows for the testing of tailored cybersecurity training modules designed specifically for the local population, ensuring that the content is relevant to their daily lives. For example, in communities where mobile phones are the primary access point for the internet, the program could focus on mobile security practices, such as safe use of apps and protecting personal information on mobile devices.

Delivering the cybersecurity training in these communities involves a combination of in-person workshops, mobile-based learning, and online modules, depending on the technological resources available. In-person sessions can facilitate direct engagement, hands-on demonstrations, and peer-to-peer learning, while mobile and online platforms can extend the reach of the program to individuals who may not be able to attend in person due to logistical or financial constraints (Zhang, et al., 2020). These training modules are designed to address the specific digital challenges faced by underserved populations, such as protecting personal data, recognizing online scams, securing mobile devices, and ensuring privacy when accessing online services. By delivering these training sessions in formats that align with participants' daily habits and preferences, the program becomes more accessible and impactful.

Data analysis is essential for understanding the effectiveness of the program and identifying areas for improvement. The pre- and post-assessment of participants' knowledge provides quantitative data that can be used to measure the knowledge gained throughout the program. This analysis helps quantify the success of the program in improving participants' cybersecurity literacy, providing concrete evidence of the program's impact. A comparison of pre- and post-assessment scores enables the identification of specific areas where participants may have struggled or where further attention is needed. Additionally, tracking long-term retention of the knowledge gained can provide valuable insights into the sustainability of the learning outcomes.

Thematic analysis of feedback gathered through interviews and focus groups is crucial for understanding the qualitative impact of the program. This type of analysis helps identify recurring themes, such as common concerns or challenges faced by participants, areas where they felt the program was most beneficial, and suggestions for improvement. For example, feedback might reveal that participants found mobile security tips particularly useful, or that they struggled to understand more technical concepts such as encryption or firewalls. By identifying these themes, the program developers can refine the content to better meet the needs of the community, adjust delivery methods, and ensure that the program remains relevant and engaging.

In addition to assessing knowledge and feedback, the data analysis process also helps evaluate the overall effectiveness of the program's structure. This includes evaluating how well the program's objectives align with the needs of the community and whether the delivery methods were appropriate. For example, if the program was designed to be mobile-first but participants in the pilot communities lacked reliable access to mobile phones, the data analysis could reveal the need to adapt the program to incorporate more in-person or offline elements (Zukarnain, Muneer & Ab Aziz, 2022). Furthermore, the analysis of the community engagement during the pilot phase can provide insights into the scalability of the program. If community members actively participate and demonstrate a willingness to continue learning, it suggests that the program can be scaled to reach a broader audience.

The methodology for advancing cybersecurity awareness in underserved communities is designed to create a comprehensive, sustainable approach to digital literacy. By integrating quantitative and qualitative research methods, pilot testing, and ongoing data analysis, the program can be continuously refined and adapted to meet the evolving needs of the community. The ultimate goal is to empower individuals to navigate the digital world securely, protecting themselves from cyber threats and fostering a culture of digital responsibility that can extend across generations. Through this methodology, cybersecurity awareness programs can transform the lives of underserved individuals, helping them thrive in an increasingly digital society.

5. Results and Discussion

The results and discussion of advancing cybersecurity awareness programs for underserved communities reveal significant strides in improving digital literacy and cybersecurity skills, alongside challenges and key lessons learned that are critical for refining and scaling the program. Through the implementation of a tailored model for cybersecurity education, the impact on participants has been positive, with substantial improvements in awareness and skills. However, as with any initiative of this nature, several barriers have emerged that require attention to enhance participation and scalability (Zhang, et al., 2020). The lessons learned through this process provide valuable insights into how such programs can be further developed to ensure their effectiveness and sustainability in diverse community settings.

The impact of the model has been considerable in terms of improvement in cybersecurity awareness and skills. Participants in the pilot program demonstrated marked gains in their understanding of basic cybersecurity concepts, including the importance of securing personal devices, recognizing phishing attempts, and adopting safe practices when using online platforms. Surveys conducted before and after the training sessions showed significant improvements in participants' ability to identify common cyber threats and understand the steps required to protect themselves online (Zukarnain, Muneer & Ab Aziz, 2022). Participants also reported a higher sense of confidence in their ability to navigate digital spaces securely. This increased sense of security is crucial, as it empowers individuals to make informed decisions about their online activities and safeguard personal information.

A key factor contributing to this success was the use of culturally relevant content, which enhanced engagement and improved knowledge retention. By tailoring the training materials to the specific needs and experiences of the community, the program was able to break down the barriers that often make traditional cybersecurity education feel disconnected from real life. Localized content that incorporated community-specific examples, such as common scams or threats faced by individuals in these communities, made the training more relatable and easier to understand. Participants were able to see the direct application of the information in their daily lives, which increased their motivation to engage with the program (Zwilling, et al., 2022). Furthermore, the use of local languages and culturally appropriate references helped ensure that the material was accessible to a broader audience, including those with limited proficiency in mainstream languages.

Gamified learning techniques also played a significant role in enhancing engagement. Participants, particularly in underserved communities where traditional forms of learning may not always be as engaging, responded positively to the interactive and enjoyable nature of the training. By incorporating elements of play into the learning process, the program made complex cybersecurity concepts more accessible and memorable (AlDaajeh, et al., 2022). The competitive aspect of gamification, where participants could test their knowledge and compare their scores with others, created a sense of achievement and motivation to continue learning. This gamified approach was particularly effective in communities where participants might have been skeptical about the value of cybersecurity education, as it made the learning process more fun and less intimidating.

Despite these positive outcomes, several challenges were identified that affected both participation and scalability. One of the most significant barriers was access to technology. While mobile phones are ubiquitous in many underserved communities, the lack of reliable internet access and the use of outdated devices created challenges for the effective delivery of online modules. Some participants faced difficulties in accessing training materials due to slow or intermittent internet connections, which hindered their ability to complete the program (De Bruijn & Janssen, 2017). Additionally, the cost of data for mobile phones posed a barrier for some individuals, limiting their ability to participate in the program fully. To address this, the program could explore alternative delivery methods, such as offline modules or community-based hubs with internet access, to ensure that those with limited access to technology are not excluded from the training.

Another challenge was the diversity in digital literacy levels among participants. While some community members were already somewhat familiar with basic cybersecurity concepts, others were entirely new to the digital world. This created a gap in knowledge that required the program to be highly adaptive in its delivery. Some participants needed more foundational training, while others were ready to tackle more advanced topics (White, 2016). Striking a balance between catering to the needs of individuals with different levels of digital literacy posed a challenge in maintaining the interest and engagement of all participants. Future iterations of the program could benefit from segmenting participants based on their initial knowledge and providing more tailored learning pathways that allow individuals to progress at their own pace.

A significant challenge for scalability was the reliance on local community leaders, educators, and stakeholders to deliver the program. While their involvement was essential for the program's success in local communities, it also created logistical challenges. Training local facilitators and ensuring they had the necessary skills and resources to deliver high-quality cybersecurity education was time-consuming and required a substantial investment in capacity-building (Uchendu, et al., 2021). Furthermore, without ongoing support and training, the quality of the delivery could vary, affecting the consistency of the program's impact. To scale the program effectively, it will be important to develop robust training programs for facilitators, along with a system for continuous support and feedback to ensure the delivery of effective and up-to-date content.

Despite these challenges, the lessons learned from the pilot program offer valuable insights for refining the model and improving its effectiveness. One key lesson is the importance of continuous adaptation and feedback. Throughout the pilot, it became clear that the needs and preferences of the community were evolving, and the program needed to be flexible in responding to these changes (Perwej, et al., 2021). Regular feedback from participants, educators, and stakeholders allowed the program to be adjusted in real time, ensuring that it remained relevant and effective. For instance, when it was discovered that certain topics were too complex for participants at lower literacy levels, the training materials were simplified, and additional support was provided through one-on-one coaching sessions.

Another important lesson was the need to integrate ongoing support and reinforcement into the program. While initial gains in knowledge were evident, sustaining those gains over time required continued engagement. To address this, the program could include periodic refresher courses, follow-up workshops, and reminders through mobile text messages or social media channels to keep participants informed about emerging threats and best practices. Continuous engagement ensures that participants retain what they have learned and stay up to date with the evolving landscape of cybersecurity (Stewart & Jürjens, 2017).

The pilot also highlighted the significance of collaboration with external partners, such as technology providers and NGOs, to ensure the program's sustainability. By working with technology providers to secure resources like free or discounted software, tools, and internet access, the program can alleviate some of the technological barriers faced by participants. Partnerships with NGOs can also provide valuable expertise in community outreach and capacity-building, helping to extend the reach of the program to more underserved populations.

In conclusion, the results of advancing cybersecurity awareness programs in underserved communities have shown promising improvements in digital literacy, engagement, and knowledge retention. While challenges related to access to technology, digital literacy levels, and scalability remain, the lessons learned from the pilot phase provide a solid foundation for refining and scaling the program (Hasan, et al., 2021). By focusing on continuous adaptation, ongoing support, and collaboration with external partners, the model can be further developed to empower underserved communities with the skills and knowledge they need to navigate the digital world securely and confidently. This approach holds the potential to create a more digitally literate society, reducing vulnerabilities and enhancing the overall resilience of communities in the face of growing cyber threats.

5.1. Recommendations

Advancing cybersecurity awareness programs in underserved communities is essential for bridging the digital divide and ensuring that all individuals are equipped with the necessary skills to navigate the increasingly complex online world securely. As technology continues to evolve, so too do the threats that individuals face online, making it crucial to establish sustainable models that empower communities to protect themselves from cyber risks (Kortjan & Von Solms, 2014). There are several recommendations that can help enhance the effectiveness, reach, and sustainability of cybersecurity awareness programs. These recommendations encompass policy suggestions, strategies for sustainability, and the importance of continued community engagement and partnerships.

First, policy initiatives can play a pivotal role in driving the adoption of cybersecurity awareness programs, particularly in underserved regions where access to digital literacy programs may be limited. One of the primary policy recommendations is to create incentives for cybersecurity education in underserved areas. Governments and international organizations can introduce subsidies or grants that encourage educational institutions, non-profits, and community organizations to implement cybersecurity training programs (Muhirwe & White, 2016). By providing financial incentives, these entities can offer free or low-cost training to individuals who would otherwise not have access to such resources. These incentives can also extend to the provision of digital tools, such as smartphones, tablets, or internet connectivity, to facilitate participation in online learning modules. Providing these resources will help bridge the technological gap in underserved communities, where access to devices and internet connections can be limited.

Moreover, integrating cybersecurity education into formal education systems is another key policy suggestion. By embedding cybersecurity awareness into school curricula at an early age, children and young adults can develop critical digital literacy skills that will serve them throughout their lives. Integrating cybersecurity education into existing subjects such as computer science, information technology, or social studies can ensure that students are exposed to the fundamental concepts of online safety, data protection, and ethical online behavior (Martin, 2017). Moreover, this integration should extend to higher education institutions, where specialized programs focused on cybersecurity can be developed to nurture a new generation of cybersecurity professionals. As the demand for cybersecurity experts continues to grow, these educational pathways will help meet the global demand for skilled workers while simultaneously contributing to the overall digital security of underserved communities.

In addition to policy recommendations, strategies for sustainability are crucial for ensuring the long-term success of cybersecurity awareness programs. One of the most effective strategies for sustainability is ongoing community involvement. Cybersecurity awareness programs should not be seen as one-time interventions but rather as part of an ongoing effort to build a culture of security within communities. This can be achieved by establishing local community hubs or digital literacy centers that offer continuous training and support. These hubs can serve as safe spaces for individuals to learn about cybersecurity, ask questions, and receive personalized assistance (Iivari, Sharma & Ventä-Olkkonen, 2020). By involving local community leaders, educators, and influencers in the delivery of training programs, the initiative will be better rooted in the local context and more likely to resonate with the community. Additionally, community leaders can help spread the message of cybersecurity awareness to a wider audience, ensuring that the program reaches as many individuals as possible.

Another important aspect of sustainability is the need for flexible and adaptable training programs. As cybersecurity threats evolve, so too should the content and delivery methods of training programs. The ongoing assessment of threats, technological advancements, and the evolving needs of the community will help ensure that the programs remain relevant and effective. This requires continuous investment in training facilitators and updating training materials to reflect the latest developments in the cybersecurity landscape (Van Deursen & Van Dijk, 2014). Localized and gamified learning approaches, which have been shown to be effective in engaging underserved communities, should also be incorporated into these ongoing programs to maintain participant interest and motivation. By regularly evaluating the effectiveness of training programs and incorporating feedback from participants, educators can ensure that the content meets the needs of the community and addresses any gaps in knowledge.

Leveraging partnerships and funding opportunities is another critical strategy for the sustainability of cybersecurity awareness programs. Collaboration with technology providers, non-governmental organizations (NGOs), and international development agencies can help expand the reach and impact of the program. Partnerships with technology companies can provide access to the latest tools, software, and resources that will enhance the learning experience for participants (Dwivedi, et al., 2020). For example, technology companies can donate cybersecurity software or provide access to online learning platforms that are essential for the success of the program. Additionally, NGOs can offer expertise in community mobilization, outreach, and evaluation, helping to ensure that the program is implemented effectively and reaches the target audience.

Furthermore, seeking funding opportunities from both public and private sectors can provide the financial resources needed to scale the program and ensure its sustainability. Governments, foundations, and corporate social responsibility (CSR) initiatives often provide grants and funding for digital literacy and cybersecurity programs aimed at underserved communities. By tapping into these funding sources, the program can secure the resources needed for long-term success (Schwertner, K. 2017). Furthermore, as the program grows, it can create a model of self-sustainability, where community members and local organizations take on a more active role in funding and delivering the program. This approach can ensure that the program remains responsive to local needs and does not rely solely on external funding.

In addition to leveraging partnerships, it is essential to incorporate a strong evaluation and monitoring framework into the program. By regularly evaluating the program's effectiveness, stakeholders can identify areas for improvement and ensure that the objectives of the program are being met (Schmidt & Cohen, 2015). This evaluation process should include both quantitative and qualitative measures, such as pre- and post-assessments of participants' cybersecurity knowledge, as well as feedback from participants, trainers, and community leaders. Continuous monitoring of the program's impact will help identify challenges early on and enable course corrections to ensure that the program remains aligned with its goals.

Another recommendation is to incorporate a holistic approach to digital literacy that goes beyond just cybersecurity. While cybersecurity education is critical, it should be integrated into a broader framework of digital literacy that

encompasses other aspects of online behavior, such as privacy protection, responsible digital citizenship, and media literacy. By broadening the scope of the program, communities can gain a more comprehensive understanding of how to navigate the digital world safely and responsibly (Cascio & Montealegre, 2016). This integrated approach will also help individuals become more aware of the broader implications of digital technology on their lives, empowering them to make informed decisions about their online activities.

Lastly, creating a peer-to-peer support system can further enhance the sustainability and effectiveness of cybersecurity awareness programs. In many underserved communities, peer relationships are highly influential, and individuals are more likely to trust and learn from their peers than from external trainers (Lee, et al., 2018). By training local champions or cybersecurity ambassadors within the community, the program can build a network of individuals who are passionate about cybersecurity and are willing to share their knowledge and experiences with others. These peer educators can play a vital role in reinforcing key messages, answering questions, and ensuring that the program has a lasting impact.

In conclusion, advancing cybersecurity awareness programs in underserved communities requires a multifaceted approach that combines policy initiatives, strategies for sustainability, and ongoing community engagement. By providing incentives for cybersecurity education, integrating it into formal education systems, and leveraging partnerships and funding opportunities, these programs can reach and empower a wider audience (Legner, et al., 2017). Ongoing community involvement, adaptable training methods, and a broader approach to digital literacy will ensure that the programs remain relevant, effective, and sustainable. Through these efforts, we can build a more digitally literate and resilient society, capable of navigating the challenges of the digital age securely.

6. Conclusion

In conclusion, advancing cybersecurity awareness programs in underserved communities presents a crucial opportunity to bridge the digital divide and ensure that individuals are equipped with the necessary skills to protect themselves in an increasingly connected world. The implementation of such programs fosters digital literacy, which is not only critical for personal security but also vital for the long-term empowerment of these communities. By addressing barriers to participation, tailoring content to local contexts, and providing resources that resonate with participants, these programs have shown promise in improving cybersecurity awareness and skills. However, challenges such as limited access to technology, infrastructure, and financial constraints must be overcome to ensure the success and sustainability of these initiatives.

The findings underscore the importance of localized and culturally relevant content, as well as the need for continuous capacity-building initiatives. The integration of mobile technology, gamified learning approaches, and flexible, ongoing training can greatly enhance engagement and participation, ensuring that individuals are empowered to navigate the digital world securely. Moreover, partnerships with technology providers, NGOs, and local community leaders play a pivotal role in scaling these programs and ensuring their long-term viability.

Looking forward, the future of advancing digital literacy through cybersecurity awareness lies in further collaboration between governments, educational institutions, community organizations, and the private sector. As technology continues to evolve, so too must the methods and tools used in cybersecurity education. Expanding access to digital learning platforms, incorporating advanced cybersecurity concepts into formal educational curricula, and increasing investments in underserved communities will be essential steps in advancing digital literacy. Furthermore, strengthening the infrastructure for remote and mobile learning can help overcome geographical and economic barriers, ensuring that cybersecurity education is accessible to all.

Future directions should also focus on the continuous refinement of training materials and delivery methods to stay ahead of emerging cybersecurity threats. The model for advancing digital literacy should remain flexible, adapting to the evolving needs of communities and addressing the dynamic nature of the cybersecurity landscape. Ultimately, a sustainable approach to cybersecurity education will require the collective effort of stakeholders from various sectors, all working together to create a more digitally literate and secure society for underserved communities.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdi, L., & Meddeb, A. (2018). Driver information system: a combination of augmented reality, deep learning and vehicular Ad-hoc networks. *Multimedia Tools and Applications*, *77*, 14673-14703.

[2] Abou Elassad, Z. E., Mousannif, H., Al Moatassime, H., & Karkouch, A. (2020). The application of machine learning techniques for driving behavior analysis: A conceptual framework and a systematic literature review. *Engineering Applications of Artificial Intelligence*, *87*, 103312.

[3] AbuAli, N., & Abou-Zeid, H. (2016). Driver behavior modeling: Developments and future directions. *International journal of vehicular technology*, *2016*(1), 6952791.

[4] Abughalieh, K. M., & Alawneh, S. G. (2020). Predicting pedestrian intention to cross the road. *IEEE Access*, *8*, 72558-72569.

[5] Adeniran, A. I., Abhulimen, A. O., Obiki-Osafiele. A. N., Osundare, O. S., Efunniyi, C. P., Agu, E. E. (2022). Digital banking in Africa: A conceptual review of financial inclusion and socio-economic development. International Journal of Applied Research in Social Sciences, 2022, 04(10), 451-480, https://doi.org/10.51594/ijarss.v4i10.1480

[6] Adeniran, I. A, Abhulimen A.O, Obiki-Osafiele, A.N, Osundare O.S, Efunniyi C.P, & Agu E.E. (2022): Digital banking in Africa: A conceptual review of financial inclusion and socio-economic development. International Journal of Applied Research in Social Sciences, Volume 4, Issue 10, P.No. 451-480, 2022

[7] Adepoju, P. A., Austin-Gabriel, B., Ige, A. B., Hussain, N. Y., Amoo, O. O., & Afolabi, A. I. (2022). Machine learning innovations for enhancing quantum-resistant cryptographic protocols in secure communication. *Open Access Research Journal of Multidisciplinary Studies*, 4(1), 131–139. https://doi.org/10.53022/oarjms.2022.4.1.0075

[8] Agu, E.E, Abhulimen A.O, Obiki-Osafiele, A.N, Osundare O.S, Adeniran I.A & Efunniyi C.P. (2022): Artificial Intelligence in African Insurance: A review of risk management and fraud prevention. International Journal of Management & Entrepreneurship Research, Volume 4, Issue 12, P.No.768-794, 2022.

[9] Aksjonov, A., & Kyrki, V. (2021, September). Rule-based decision-making system for autonomous vehicles at intersections with mixed traffic environment. In 2021 IEEE International Intelligent Transportation Systems Conference (ITSC) (pp. 660-666). IEEE.

[10] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754.

[11] Alsrehin, N. O., Klaib, A. F., & Magableh, A. (2019). Intelligent transportation and control systems using data mining and machine learning techniques: A comprehensive study. IEEE Access, 7, 49830-49857.

[12] Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. IEEE Communications Surveys & Tutorials, 18(3), 1998-2026.

[13] Amado, H., Ferreira, S., Tavares, J. P., Ribeiro, P., & Freitas, E. (2020). Pedestrian–vehicle interaction at unsignalized crosswalks: a systematic review. Sustainability, 12(7), 2805.

[14] Arvin, R., Kamrani, M., & Khattak, A. J. (2019). How instantaneous driving behavior contributes to crashes at intersections: Extracting useful information from connected vehicle message data. Accident Analysis & Prevention, 127, 118-133.

[15] Asaithambi, G., Kanagaraj, V., & Toledo, T. (2016). Driving behaviors: Models and challenges for non-lane based mixed traffic. Transportation in Developing Economies, 2, 1-16.

[16] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. Open Access Research Journal of Engineering and Technology, 1(1), 47–55. https://doi.org/10.53022/oarjet.2021.1.1.0107

[17] Azadani, M. N., & Boukerche, A. (2021). Driving behavior analysis guidelines for intelligent transportation systems. IEEE transactions on intelligent transportation systems, 23(7), 6027-6045.

[18] Baheti, B., Gajre, S., & Talbar, S. (2018). Detection of distracted driver using convolutional neural network. In Proceedings of the IEEE conference on computer vision and pattern recognition workshops (pp. 1032-1038).

[19] Benrachou, D. E., Glaser, S., Elhenawy, M., & Rakotonirainy, A. (2022). Use of social interaction and intention to improve motion prediction within automated vehicle framework: A review. IEEE Transactions on Intelligent Transportation Systems, 23(12), 22807-22837.

[20] Bifulco, G. N., Coppola, A., Petrillo, A., & Santini, S. (2022). Decentralized cooperative crossing at unsignalized intersections via vehicle-to-vehicle communication in mixed traffic flows. Journal of Intelligent Transportation Systems, 28(2), 211-236.

[21] Camara, F., Bellotto, N., Cosar, S., Weber, F., Nathanael, D., Althoff, M., ... & Fox, C. (2020). Pedestrian models for autonomous driving part ii: high-level models of human behavior. IEEE Transactions on Intelligent Transportation Systems, 22(9), 5453-5472.

[22] Cascio, W. F., & Montealegre, R. (2016). How technology is changing work and organizations. Annual review of organizational psychology and organizational behavior, 3(1), 349-375.

[23] Charouh, Z., Ezzouhri, A., Ghogho, M., & Guennoun, Z. (2022). Video analysis and rule-based reasoning for driving maneuver classification at intersections. IEEE Access, 10, 45102-45111.

[24] Chauhan, S., Singh, R., Gehlot, A., Akram, S. V., Twala, B., & Priyadarshi, N. (2022). Digitalization of supply chain management with industry 4.0 enabling technologies: a sustainable perspective. Processes, 11(1), 96.

[25] Chen, D., Wawrzynski, P., & Lv, Z. (2021). Cyber security in smart cities: a review of deep learning-based applications and case studies. Sustainable Cities and Society, 66, 102655.

[26] De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1-7.

[27] Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., ... & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. International journal of information management, 55, 102211.

[28] Efunniyi, C.P, Abhulimen A.O, Obiki-Osafiele, A.N,Osundare O.S , Adeniran I.A , & Agu E.E. (2022): Data analytics in African banking: A review of opportunities and challenges for enhancing financial services. International Journal of Management & Entrepreneurship Research, Volume 4, Issue 12, P.No.748-767, 2022.3.

[29] Eom, M., & Kim, B. I. (2020). The traffic signal control problem for intersections: a review. European transport research review, 12, 1-20.

[30] Essa, M. (2020). Real-time safety and mobility optimization of traffic signals in a connected-vehicle environment (Doctoral dissertation, University of British Columbia).

[31] Fu, C., & Liu, H. (2020). Investigating influence factors of traffic violations at signalized intersections using data gathered from traffic enforcement camera. PLoS one, 15(3), e0229653.

[32] Galterio, M. G., Shavit, S. A., & Hayajneh, T. (2018). A review of facial biometrics security for smart devices. Computers, 7(3), 37.

[33] Ganesh, A. H., & Xu, B. (2022). A review of reinforcement learning based energy management systems for electrified powertrains: Progress, challenge, and potential solution. Renewable and Sustainable Energy Reviews, 154, 111833.

[34] Ghanipoor Machiani, S. (2015). Modeling Driver Behavior at Signalized Intersections: Decision Dynamics, Human Learning, and Safety Measures of Real-time Control Systems.

[35] Gudala, L., Reddy, A. K., Sadhu, A. K. R., & Venkataramanan, S. (2022). Leveraging Biometric Authentication and Blockchain Technology for Enhanced Security in Identity and Access Management Systems. *Journal of Artificial Intelligence Research*, *2*(2), 21-50.

[36] Guo, Q., Li, L., & Ban, X. J. (2019). Urban traffic signal control with connected and automated vehicles: A survey. *Transportation research part C: emerging technologies*, *101*, 313-334.

[37] Hamdar, S. H., Qin, L., & Talebpour, A. (2016). Weather and road geometry impact on longitudinal driving behavior: Exploratory analysis using an empirically supported acceleration modeling framework. *Transportation research part C: emerging technologies*, *67*, 193-213.

[38] Hara, K., Kataoka, H., Inaba, M., Narioka, K., Hotta, R., & Satoh, Y. (2021). Predicting appearance of vehicles from blind spots based on pedestrian behaviors at crossroads. *IEEE transactions on intelligent transportation systems*, *23*(8), 11917-11929.

[39] Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.

[40] Huang, Y., Wang, Y., Yan, X., Duan, K., & Zhu, J. (2022). Behavior model and guidance strategies of the crossing behavior at unsignalized intersections in the connected vehicle environment. *Transportation research part F: traffic psychology and behaviour*, *88*, 13-24.

[41] Huang, Y., Wang, Y., Yan, X., Li, X., Duan, K., & Xue, Q. (2022). Using a V2V-and V2I-based collision warning system to improve vehicle interaction at unsignalized intersections. *Journal of safety research*, *83*, 282-293.

[42] Hunter, J. D. (2022). *Improvement of unsignalized intersections faced with poor visibility weather conditions on South African regional routes* (Doctoral dissertation, Stellenbosch: Stellenbosch University).

[43] Iivari, N., Sharma, S., & Ventä-Olkkonen, L. (2020). Digital transformation of everyday life–How COVID-19 pandemic transformed the basic education of the young generation and why information management research should care?. *International journal of information management*, *55*, 102183.

[44] Jiang, Q., Huang, H., Zhao, W., Baig, F., Lee, J., & Li, P. (2021). Intention of risk-taking behavior at unsignalized intersections under the connected vehicle environment. *IEEE Access*, *9*, 50624-50638.

[45] Karbasi, A., & O'Hern, S. (2022). Investigating the impact of connected and automated vehicles on signalized and unsignalized intersections safety in mixed traffic. *Future transportation*, *2*(1), 24-40.

[46] Katrakazas, C., Quddus, M., Chen, W. H., & Deka, L. (2015). Real-time motion planning methods for autonomous on-road driving: State-of-the-art and future research directions. *Transportation Research Part C: Emerging Technologies*, *60*, 416-442.

[47] Kolekar, S., Gite, S., Pradhan, B., & Kotecha, K. (2021). Behavior prediction of traffic actors for intelligent vehicle using artificial intelligence techniques: A review. *IEEE Access*, *9*, 135034-135058.

[48] Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, *52*(1), 29-41.

[49] Kussl, S., & Wald, A. (2022). Smart mobility and its implications for road infrastructure provision: a systematic literature review. *Sustainability*, *15*(1), 210.

[50] Lee, M., Yun, J. J., Pyka, A., Won, D., Kodama, F., Schiuma, G., ... & Zhao, X. (2018). How to respond to the fourth industrial revolution, or the second information technology revolution? Dynamic new combinations between technology, market, and society through open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, *4*(3), 21.

[51] Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., ... & Ahlemann, F. (2017). Digitalization: opportunity and challenge for the business and information systems engineering community. *Business & information systems engineering*, *59*, 301-308.

[52] Li, G., Li, S., Li, S., Qin, Y., Cao, D., Qu, X., & Cheng, B. (2020). Deep reinforcement learning enabled decision-making for autonomous driving at intersections. *Automotive Innovation*, *3*, 374-385.

[53] Li, Z., Elefteriadou, L., & Ranka, S. (2014). Signal control optimization for automated vehicles at isolated signalized intersections. *Transportation Research Part C: Emerging Technologies*, *49*, 1-18.

[54] Lim, H. S. M., & Taeihagh, A. (2018). Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies*, *11*(5), 1062.

[55] Magyari, Z., Koren, C., Kieć, M., & Borsos, A. (2021). Sight distances at unsignalized intersections: A comparison of guidelines and requirements for human drivers and autonomous vehicles. *Archives of transport*, *59*(3), 7-19.

[56] Maldonado Silveira Alonso Munhoz, P. A., da Costa Dias, F., Kowal Chinelli, C., Azevedo Guedes, A. L., Neves dos Santos, J. A., da Silveira e Silva, W., & Pereira Soares, C. A. (2020). Smart mobility: The main drivers for increasing the intelligence of urban mobility. *Sustainability*, *12*(24), 10675.

[57] Martin, W. J. (2017). *The global information society*. Routledge.

[58] Mena-Yedra, R. (2020). An adaptive, fault-tolerant system for road network traffic prediction using machine learning.

[59] Mosco, V. (2017). *Becoming digital: Toward a post-internet society*. Emerald Publishing Limited.

[60] Mozaffari, S., Al-Jarrah, O. Y., Dianati, M., Jennings, P., & Mouzakitis, A. (2020). Deep learning-based vehicle behavior prediction for autonomous driving applications: A review. *IEEE Transactions on Intelligent Transportation Systems*, *23*(1), 33-47.

[61] Muhirwe, J., & White, N. (2016). Cybersecurity Awareness And Practice Of Next Generation Corporate Technology Users. *Issues in Information Systems*, *17*(2).

[62] Mukherjee, D., & Mitra, S. (2019). A comparative study of safe and unsafe signalized intersections from the view point of pedestrian behavior and perception. *Accident Analysis & Prevention*, *132*, 105218.

[63] Muresan, M. (2021). Deep Reinforcement Learning Models for Real-Time Traffic Signal Optimization with Big Traffic Data.

[64] Neal, T. J., & Woodard, D. L. (2016). Surveying biometric authentication for mobile device security. *Journal of Pattern Recognition Research*, *1*(74-110), 4.

[65] Ni, D. (2020). *Signalized Intersections*. Cham, Swizerland: Springer International Publishing.

[66] Nikitas, A., Michalakopoulou, K., Njoya, E. T., & Karampatzakis, D. (2020). Artificial intelligence, transport and the smart city: Definitions and dimensions of a new mobility era. *Sustainability*, *12*(7), 2789.

[67] Olayode, I. O., Tartibu, L. K., Okwu, M. O., & Uchechi, D. U. (2020). Intelligent transportation systems, un-signalized road intersections and traffic congestion in Johannesburg: A systematic review. Procedia CIRP, 91, 844-850.

[68] Onoja, J. P., & Ajala, O. A. (2022). Innovative telecommunications strategies for bridging digital inequities: A framework for empowering underserved communities. GSC Advanced Research and Reviews, 13(01), 210–217. https://doi.org/10.30574/gscarr.2022.13.1.0286

[69] Onoja, J. P., Ajala, O. A., & Ige, A. B. (2022). Harnessing artificial intelligence for transformative community development: A comprehensive framework for enhancing engagement and impact. GSC Advanced Research and Reviews, 11(03), 158–166. https://doi.org/10.30574/gscarr.2022.11.3.0154

[70] Ozioko, E. F., Kunkel, J., & Stahl, F. (2022, July). Road intersection coordination scheme for mixed traffic (human driven and driver-less vehicles): A systematic review. In Science and Information Conference (pp. 67-94). Cham: Springer International Publishing.

[71] Pavel, M. I., Tan, S. Y., & Abdullah, A. (2022). Vision-based autonomous vehicle systems based on deep learning: A systematic literature review. Applied Sciences, 12(14), 6831.

[72] Pawar, D. S., & Patil, G. R. (2017). Minor-street vehicle dilemma while maneuvering at unsignalized intersections. Journal of Transportation Engineering, Part A: Systems, 143(8), 04017039.

[73] Peng, H., Wang, H., Du, B., Bhuiyan, M. Z. A., Ma, H., Liu, J., ... & Philip, S. Y. (2020). Spatial temporal incidence dynamic graph neural networks for traffic flow forecasting. *Information Sciences*, *521*, 277-290.

[74] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710.

[75] Petraki, V., Ziakopoulos, A., & Yannis, G. (2020). Combined impact of road and traffic characteristic on driver behavior using smartphone sensor data. *Accident Analysis & Prevention*, *144*, 105657.

[76] Rodrigues, M., McGordon, A., Gest, G., & Marco, J. (2018). Autonomous navigation in interaction-based environments—A case of non-signalized roundabouts. *IEEE Transactions on Intelligent Vehicles*, *3*(4), 425-438.

[77] Rui, Z., & Yan, Z. (2018). A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE access*, *7*, 5994-6009.

[78] Schmidt, E., & Cohen, J. (2015). The new digital age: Reshaping the future of people, nations and business.

[79] Schwertner, K. (2017). Digital transformation of business. *Trakia Journal of Sciences*, *15*(1), 388-393.

[80] Shirazi, M. S., & Morris, B. T. (2016). Looking at intersections: a survey of intersection monitoring, behavior and safety analysis of recent studies. *IEEE Transactions on Intelligent Transportation Systems*, *18*(1), 4-24.

[81] Silasai, O., & Khowfa, W. (2020). The study on using biometric authentication on mobile device. *NU Int. J. Sci*, *17*, 90-110.

[82] Singh, H., & Kathuria, A. (2021). Analyzing driver behavior under naturalistic driving conditions: A review. *Accident Analysis & Prevention*, *150*, 105908.

[83] Soomro, K., Bhutta, M. N. M., Khan, Z., & Tahir, M. A. (2019). Smart city big data analytics: An advanced review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(5), e1319.

[84] Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, *25*(5), 494-534.

[85] Sun, D., & Elefteriadou, L. (2014). A driver behavior-based lane-changing model for urban arterial streets. *Transportation science*, *48*(2), 184-205.

[86] Tawari, A., Mallela, P., & Martin, S. (2018, November). Learning to attend to salient targets in driving videos using fully convolutional RNN. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)* (pp. 3225-3232). IEEE.

[87] Tian, R., Li, N., Kolmanovsky, I., Yildiz, Y., & Girard, A. R. (2020). Game-theoretic modeling of traffic in unsignalized intersection network for autonomous vehicle control verification and validation. *IEEE Transactions on Intelligent Transportation Systems*, *23*(3), 2211-2226.

[88] Torbaghan, M. E., Sasidharan, M., Reardon, L., & Muchanga-Hvelplund, L. C. (2022). Understanding the potential of emerging digital technologies for improving road safety. *Accident Analysis & Prevention*, *166*, 106543.

[89] Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387.

[90] Van Deursen, A. J., & Van Dijk, J. A. (2014). *Digital skills: Unlocking the information society*. Springer.

[91] Vemori, V. (2020). Towards Safe and Equitable Autonomous Mobility: A Multi-Layered Framework Integrating Advanced Safety Protocols and XAI for Transparent Decision-Making in Self-Driving Vehicles. *Journal of Science & Technology*, *1*(1), 130-161.

[92] Wang, C. (2022). *The brain of the smart transportation system: exploring the role of future expectations and sociotechnical imaginaries in cutting-edge science and technology policymaking in China* (Doctoral dissertation, University of Warwick).

[93] Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. *Computer Networks*, *170*, 107118.

[94] Wang, K., Zhang, W., Jin, L., Feng, Z., Zhu, D., Cong, H., & Yu, H. (2022). Diagnostic analysis of environmental factors affecting the severity of traffic crashes: From the perspective of pedestrian–vehicle and vehicle–vehicle collisions. *Traffic injury prevention*, *23*(1), 17-22.

[95] White, J. (2016). Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. *Global Security Studies*, *7*(4).

[96] Ye, F., Hao, P., Qi, X., Wu, G., Boriboonsomsin, K., & Barth, M. J. (2018). Prediction-based eco-approach and departure at signalized intersections with speed forecasting on preceding vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *20*(4), 1378-1389.

[97] Yuan, T., da Rocha Neto, W. B., Rothenberg, C., Obraczka, K., Barakat, C., & Turletti, T. (2019). Harnessing machine learning for next-generation intelligent transportation systems: a survey. *Proceedings of the computational intelligence, communication systems and networks (CICSyN)*.

[98] Yuan, T., da Rocha Neto, W., Rothenberg, C. E., Obraczka, K., Barakat, C., & Turletti, T. (2022). Machine learning for next-generation intelligent transportation systems: A survey. *Transactions on emerging telecommunications technologies*, *33*(4), e4427.

[99] Zhang, C., Li, R., Kim, W., Yoon, D., & Patras, P. (2020). Driver behavior recognition via interwoven deep convolutional neural nets with multi-stream inputs. *Ieee Access*, *8*, 191138-191151.

[100] Zhang, H., & Fu, R. (2020). A hybrid approach for turning intention prediction based on time series forecasting and deep learning. *Sensors*, *20*(17), 4887.

[101] Zhang, Y., Yan, X., Wu, J., & Duan, K. (2020). Effect of warning system on interactive driving behavior at unsignalized intersection under fog conditions: a study based on multiuser driving simulation. *Journal of advanced transportation*, *2020*(1), 8871875.

[102] Zukarnain, Z. A., Muneer, A., & Ab Aziz, M. K. (2022). Authentication securing methods for mobile identity: Issues, solutions and challenges. *Symmetry*, *14*(4), 821.

[103] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97.