Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 20 No. 14 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijim.v20i14.62240

PAPER

Personalized AI-Based Cybersecurity Training for Older Adults

Sidnei Sales[1], Shahbaz Pervez[1] (✉), Muhammad Nadeem[2], Seyed Ebrahim Hosseini[1], Muhammad Kashif Siddhu[3]

[1]School of Applied IT, Whitecliffe, New Zealand

[2]College of Engineering and Technology, American University of the Middle East, Egaila, Kuwait

[3]Lahore Garrison University, Lahore, Pakistan

shahbazp@whitecliffe.ac.nz

ABSTRACT

This study explored the potential of artificial intelligence (AI) to enhance cybersecurity awareness among Brazilian senior citizens through personalized training programs. By integrating advanced AI technologies with gamification and adaptive learning, the research examined how modern technological developments can protect vulnerable elderly populations from cyber threats. The paper traced the evolution of cybersecurity and its increasing complexity, with a particular focus on social engineering tactics that exploit the unique vulnerabilities of older adults, such as cognitive decline, social isolation, and limited technological literacy. The study highlighted how these factors make elderly individuals particularly susceptible to scams and digital deception. The research utilized the CAIN questionnaire to assess cybersecurity knowledge and draws on key studies to demonstrate how gamification and AI-driven personalized learning can significantly improve user engagement, knowledge retention, and defensive practices. Ethical considerations, including adherence to Brazil's LGPD (General Data Protection Law), are addressed to ensure compliance with privacy and data protection standards. The study ultimately sought to answer the question: Can AI enhance cybersecurity awareness among elderly Brazilians through tailored training programs? Findings show that adaptive AI systems not only boost knowledge retention but also provide a scalable, cost-effective solution to reducing the risk of social engineering attacks, offering a promising approach to cybersecurity education for at-risk populations.

KEYWORDS

artificial intelligence (AI), cybersecurity awareness for elderly populations, psychological manipulation, AI-driven personalized training, digital vulnerabilities, human factors in cyber defense, AI-enabled defense mechanisms, data privacy and ethical considerations, gamified cybersecurity education

1 INTRODUCTION

Cybersecurity has become a major problem around the world that affects almost every part of modern life. Computer security has always been about protecting data,

Sales, S., Pervez, S., Nadeem, M., Hosseini, S. E., Siddhu, M. K. (2026). Personalized AI-Based Cybersecurity Training for Older Adults. *International Journal of Interactive Mobile Technologies (iJIM)*, 20(14), pp. 32–47. https://doi.org/10.3991/ijim.v20i14.62240

Article submitted 2026-03-06. Revision uploaded 2026-05-12. Final acceptance 2026-05-12.

networks, and systems from threats that change all the time and are often unexpected [1, 2]. The quick growth of technologies such as artificial intelligence (AI), machine learning, and big data analytics has made it much easier to find, understand, and deal with cybersecurity threats in real time [3]. These new technologies do make things safer, but they also create new risks, especially for groups that are already at risk, like the elderly, who may not know how to use computers [4].

AI-driven, interactive apps are changing the way people use technology and making it safer, but they also make it harder for some people to access and understand, especially those who aren't very good with computers [3, 5].

Cyberattacks have changed from random, opportunistic events to well-planned, complex campaigns. Cybercrime has changed because of the rise of AI-powered impersonation, phishing, and social engineering tactics that use human psychology to control people and businesses [3, 5, 6]. As technology keeps getting better, cybercriminals are getting better at taking advantage of both people's weaknesses and technology's weaknesses [7]. Recent research, including studies by Tempestini et al. [8], underscores that conventional countermeasures are progressively insufficient to combat the evolving characteristics of cyberattacks, which utilize various manipulation strategies.

The aging population in Brazil is growing steadily, with more seniors engaging in online activities such as banking, healthcare, and social interactions [4]. However, many elderly individuals still lack the necessary digital skills and awareness of the risks they face online, leaving them vulnerable to cybercriminals who exploit these gaps through scams and social engineering [9]. This lack of awareness has led to an increase in fraud cases, resulting in both financial losses and emotional distress for older Brazilians [10].

Traditional methods of cybersecurity training for the elderly have proven ineffective, often due to their generic, one-size-fits-all approach and lack of engagement. Balon and Baggili [11] highlight that incorporating gamification and AI-based personalization leads to higher levels of engagement and retention, thus enhancing the effectiveness of learning. Furthermore, personalized training tailored to individual learning needs has been shown to significantly improve cybersecurity awareness in older populations, as opposed to conventional, uniform training programs [12]. This ongoing debate underscores the limitations of traditional lecture-based training methods, particularly regarding long-term knowledge retention for elderly learners.

Proponents of traditional methods showed that they give people a strong base of knowledge, especially if they are new to the subject [13]. Nonetheless, there is increasing apprehension that these methods inadequately facilitate enduring knowledge retention, particularly within older demographics. Conversely, recent studies support AI-driven gamification and adaptive training techniques, which are regarded as more engaging, dynamic, and beneficial for enhanced long-term retention [1, 11].

The elderly are especially at risk for cybercrime because social engineering, phishing, and malware attacks are becoming more common and advanced [14]. Even though there are many cybersecurity training programs, many older people still don't know how cybercriminals work. This lack of awareness is mostly due to the fact that older adults don't get personalized training that takes into account their specific cognitive limitations and lack of digital literacy [10]. Current training methods frequently neglect the distinct requirements of the elderly, leading to ineffective knowledge transfer and inadequate retention, thus rendering this demographic insufficiently equipped to counter emerging threats.

This study suggested creating an AI-powered training app to help Brazil's older people become more aware of cybersecurity issues. The proposed solution focused on providing personalized, interactive training that is tailored to the needs and learning styles of older users. It was used in real-time feedback and adaptive learning techniques to keep users interested and help them remember what they learned. The app is built for mobile devices and runs on cloud infrastructure, which makes it easy to use, scalable, and secure. This new approach aims to build existing efforts to teach people about cybersecurity by providing a more effective and accessible training tool for a group of people who are becoming more vulnerable to cyber threats.

By targeting one of the most at-risk demographics for cybercrime, the goal of this project is to provide elderly Brazilians with the tools and resources to cultivate their understanding and knowledge of cybersecurity practices in such a way that would reduce their cyber victimization. The tools that provide these users with this information must be suitable for their environment and their digital literacy levels, which makes their development challenging, given the more complex and human-level cyber-attacks that we are beginning to see develop.

This project would therefore enable Brazilian elderly users to:

- Recognize and combat cyber threats, thus
- Reduce the risk of financial and emotional damages from cyber fraud, while also
- Providing a replicable, cost-effective solution for use by other at-risk populations in other settings, and
- Inform the wider discourse regarding the role of AI in the personalization of education, particularly in the realm of cybersecurity.

This study aims at the cybersecurity awareness improvement of Brazilian elderly individuals by designing and developing an AI-driven mobile application to soften the learning process.

2 LITERATURE REVIEW

2.1 The elderly and cybersecurity

Cyber threats are becoming more of a problem for people of all ages, but older people are especially at risk because they don't know much about computers and spend more time online. Older people may feel left out or uninterested in conversations about cybersecurity, but studies have shown that they are just as likely to be attacked online as people of other ages. As more and more daily tasks, like banking, healthcare, and socializing, move online, it's important for seniors to learn more about cyber threats and get better tools to protect themselves [15]. Morrison et al. [16] and Tamut and Dutta [4] stressed that the elderly are more likely to fall for social engineering scams because they are less able to think clearly, don't know how to use technology, and are socially isolated. These scams often take advantage of people's weaknesses instead of flaws in technology. The financial effects of these attacks can include identity theft and fraud, which can cause a lot of stress for the victims and their caregivers. Cybercrime can have a huge emotional and financial impact on older adults. Some studies argued that cybercrime has caused big financial losses and a noticeable drop in well-being [4]. These results show that we need to teach people about cybersecurity in a more focused way, so they are more aware and better able to resist manipulation.

Older adults have not been able to learn cybersecurity through traditional methods. Hosseini et al. [17–19] discussed that training programs that are too hard or require a lot of focus don't usually work for older people. Alnajim et al. [13] also mentioned that this group of people doesn't learn well when they have to deal with too much technical jargon and static modules. So, there is a strong need for new training programs that combine active, adaptive, and user-friendly features that are tailored to the cognitive and technological needs of older adults. Jawhar et al. [9] emphasized the necessity of offering a contextualized learning environment tailored to the unique requirements of each user, guaranteeing that the training content is both accessible and pertinent to their everyday experiences. Other research, such as Balon and Baggili [11], has shown that interactive and gamified learning methods greatly improve older people's interest and ability to remember what they learn. To close the gap between what people learn in school and what they do in real life, it's important to include examples and situations from real life that older adults can relate to. AI-driven personalized learning that changes the content based on the user's profile has also shown a lot of promise for making cybersecurity training for seniors more effective.

2.2 AI in cybersecurity: Machine learning, predictive analytics, and adaptive defenses

The quick progress of AI has led to new ways to find and stop threats. Fakhouri et al. [3] mentioned that AI can process large amounts of data, find small patterns, and help make decisions in real time. This makes it a powerful tool in the fight against cyber threats. Machine learning, which is a part of AI, is very important for these processes. By using historical data to train machine learning algorithms, systems can find possible attack paths and let administrators know before an attack turns into a security breach. This is a big change from how cybersecurity used to work, when attacks were often handled as if they had already happened. Predictive analytics lets systems look at trends and patterns all the time, which helps them stay one step ahead of threats that are changing.

Jawhar et al. [9] argued that being able to predict and get ready for attacks is very important in a world where threats are always changing. AI is very powerful, but it also raises moral issues, especially when it comes to making decisions and dealing with false positives. Finding a balance between ethics and efficiency has become a major focus of recent writing. Research conducted by Camilleri et al. [5] and Sivagumaran [20] illustrated that AI not only improves threat detection but also is essential in creating tailored adaptive training systems to address the specific requirements of vulnerable populations, including the elderly.

3 RESEARCH METHODOLOGY

This study utilized a quasi-experimental pre- and post-test design, facilitated by a mobile application intended to improve cybersecurity awareness among elderly individuals in Brazil. The study was unfolded in three principal phases: the First Phase (Pre-Test), the Second Phase (Training), and the Third Phase (Post-Test). A database kept all the data safe so that no one could see it, as shown in Figure 1.

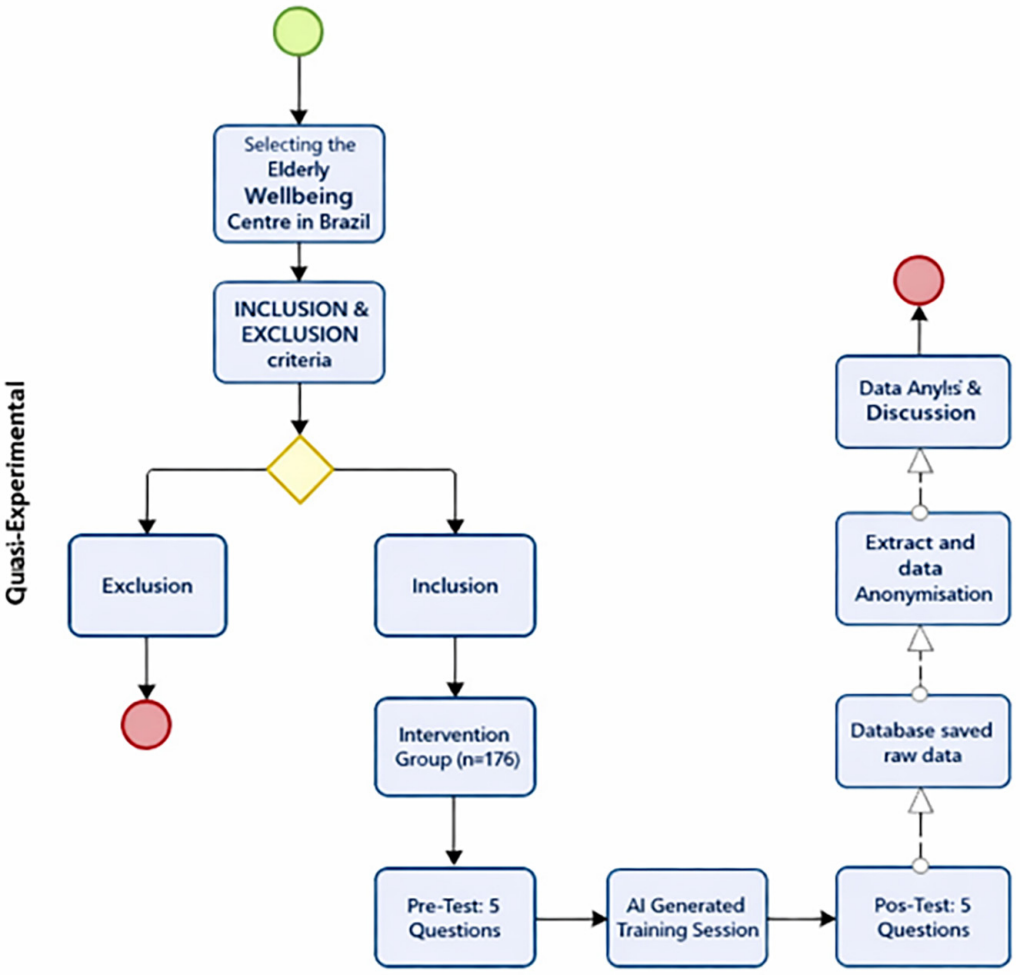

Fig. 1. Quasi-experimental study diagram

During the pre-test stage, five questions from the CAIN questionnaire were chosen at random and given to participants to see how much they already know about cybersecurity. The AWS Nova PRO AI model created a personalized training program for the mobile app during the training stage. The training program had simple explanations, examples that are relevant, and game-like elements that are made for older people. In the post-test stage, participants respond to the identical five questions from the pre-test to evaluate modifications in their knowledge. The AI model used personalized and adaptive learning principles to look at user data and create a training experience that is unique to each user. The app used simple language and game-like features to keep seniors interested and teach them.

The main goal of the study is to see how well the personalized AI intervention works by comparing how much the participants knew before and after the training. We directly measured how well the intervention works, and we used established ideas from AI, learning, and user-centered design to do so.

3.1 Study location

The Social Well-being Center, situated in Várzea Paulista, a small city in the São Paulo state of Southeast Brazil, covering an area of 35,120 square kilometers, hosted this study. According to IBGE 2022 data, 115,771 people resided in this municipality,

which revealed an annual population growth rate of 0.65% and indicated that 14% of the population is aged 60 years or older.

3.2 Solution design

Boopathi et al. [21] and Jawhar et al. [9] suggest that the solution included a training module with gamification built into interactive sessions. Users answered a series of questions about cybersecurity awareness, based on the CAIN framework and Tempestini et al. [8], to see how much they know about it. Some of the topics that these questions covered were malware, phishing attacks, social engineering, and the basics of cybersecurity. The app looked at how well the user did and gave them personalized learning paths that change based on how well they do. By using the right gamification method, the system was able to figure out how skilled each user is and make learning paths that change in real time. This made sure that the learning environment was both challenging and possible. The app works on all platforms thanks to Flutter and Dart, and it uses AWS DynamoDB to store data safely. As shown in Figure 2, the adaptive training module is powered by the AWS Bedrock LLM model.

Fig. 2. CATS – solution design

The app's main new feature is that it uses AI to make the learning experience more personal. It worked with Android devices and was made with Google Flutter and Dart. This made it easier for older people in Brazil to use, since they are less likely to have iOS devices. The Nova PRO LLM model on AWS Bedrock is a key part of the solution. In Phase 1, it was looking at user data and giving them personalized cybersecurity training based on their answers. The implementation happened in three steps: In Phase 1, users sign up, give their demographic information, and fill out a basic cybersecurity questionnaire. In Phase 2, users took part in the personalized training session led by AI. Finally, the same questionnaire was filled out in Phase 3 to see how much knowledge was gained and how well it was kept. We compared the data from Phase 1 and Phase 2 to see how well the intervention worked.

As shown in Figure 2, the main tools used in this study are the Flutter/Dart mobile app, the AWS Nova PRO AI model for personalizing content, AWS DynamoDB for storing data, and API Gateway/Lambda for safe access to user data and questionnaires. The study included elderly volunteers in Brazil who used their own Android devices to interact with the app. We used Python to analyze the data and write the final report.

3.3 Data collection

The app's workflow is designed with user-friendliness in mind, particularly for individuals with limited technical knowledge, such as elderly users. The first step involves user registration, where the user is prompted to provide a unique email address, which serves as the key for data analysis. A validation code is sent to the email to confirm the user's identity, ensuring voluntary participation and preventing duplicate responses. Once the email is validated, the user provides basic geographic and demographic information (e.g., gender, age, and education level), which is used to tailor the training to their specific needs.

After completing the demographic section, the user proceeds to the baseline cybersecurity assessment based on the CAIN Questionnaire [8]. These questions serve as the user's first introduction to the training material and are used to evaluate their initial understanding of cybersecurity concepts. Following the baseline assessment, users receive a brief overview of the training phase. In this phase, the app delivers personalized cybersecurity training, adapting the content based on the user's demographic information and baseline results. The training features simple language, real-world examples, and gamified activities to ensure the content is engaging and accessible. As outlined by Jawhar et al. [9], the training follows a two-step assessment model. In the second phase, the same set of questions from Phase 1 is re-administered to assess the user's knowledge gain and retention. All responses from both phases are stored, enabling analysis of the user's progress and learning outcomes.

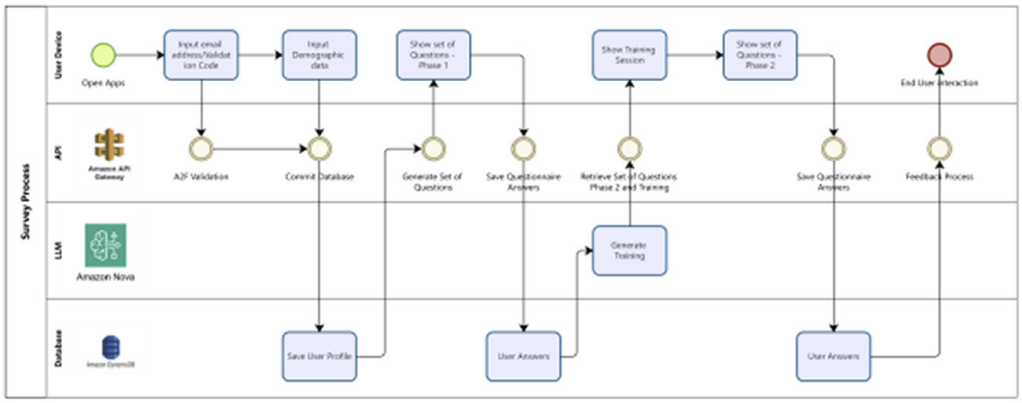

Fig. 3. User journey

3.4 Technical architecture

The proposed solution infrastructure utilizes cloud-based services to achieve the objectives of scalability and performance. The LLM model is deployed in AWS Bedrock, which is a secure and performant platform for running the Nova PRO model. The user profiles, learning data, and training history are stored in the AWS DynamoDB database hosted in the AWS Cloud. The AWS API Gateway and AWS Lambda facilitated access and management of the data and facilitated secure communication between the application, AI modules, and the database. Such architecture

not only guarantees the high availability and scalability of the application, but it also meets security requirements Fakhouri et al. [3].

3.5 Study variables

Based on Cochran's formula, this study required a total of 176 participants to ensure a diverse range of profiles. They were selected based on the following INCLUSION criteria:

- Age: 60 and above.
- Country: Brazil.
- City: Varzea Paulista.
- Must have a smartphone, use Android and have internet access.

Also, the EXCLUSION criteria are weighed in the evaluation.
Elders who:

- Don't use smartphones in their daily lives, or the device is too old and can't support the App and don't have access to the internet.
- Those who don't usually use their mobile to execute daily tasks like banking, public services, etc.
- Those who are below the age target.
- Those who have any kind of mental issue or physical disability that restricts the operation of the App.

All project-related constraints were adequately addressed.

3.6 Data analysis

A Python script was created to anonymize and summarize the raw data from the DynamoDB database. This script generates a JSON file that contains only the essential data needed to create statistical reports, tables, and graphs. In the next step, another Python script was developed to load the JSON file. This script merges and filters the contents to calculate and summarize all the statistical data presented in this study. Additionally, it generates graphs and tables as part of this process.

3.7 Ethical considerations

As the solution is used in Brazil, we need to take it seriously and follow Brazilian law, LGPD (Lei Geral de Protecão de Dados). The user received all information on the project and provided informed consent. The details of the project, including information about the data collected, the scope of the proposal, and the options for consent, are clearly explained to the user on the second screen, following the splash screen. The user needed to provide consent to continue, preventing any collection of data in the case of the app being installed by accident without any user knowledge. The system had access limited through a highly manageable network infrastructure set up using various AWS services.

The system design supported measures to enable data anonymization and purge where needed to preserve the privacy of users [3, 6]. Only quantitative and aggregated data entered the final report. All data collected were segmented into three demographic groups that included age, gender, and education level; no personally identifiable information (PII) was exported to the analytic database.

4 RESULTS

Sample Characteristics: 118 of the candidates took a random set of five items from the full 46-item CAIN. For gender, the vast majority of the sample are female, so caution must be applied when generalizing to males. For education level, 51.7% of the sample have only Primary/Intermediate levels of education, 39.0% went as far as High School, and a combined 90.7% of the sample can therefore be considered to have a "low" level of education. In contrast, only 8.5% of the sample have a Bachelor's/Graduate degree, while an extremely small 0.8% have a Master's level education. Age is also highly skewed towards the lower range: the largest group of the sample is 60–64, with 60.2% of the sample. This is followed by 65–69 at 22.0%, so combined, the respondents that fall into age groups 60–64 and 65–69 account for 82.2% of the total sample. Adding in the next nearest age group of 70–75 (11.9%), we get a combined 94.1% of the total sample accounted for by people between the ages of 60 and 75. This is in contrast with the 75–79 group at only 4.2%, as well as the two smallest age groups of 80–84 and 85–89, both at 1.0%. The fact that the vast majority of the sample is on the "younger" end of the older adult spectrum means that the study primarily demonstrates outcomes in the "younger-old" range and less so in the very elderly.

4.1 Comparison of pre- and post-test performance

Performance on the five target items in general was good, with an overall increase from the Pre Test (P1) to the Post Test (P2) for the items (see Figure 4). The average rate of correct answers was 66.6% in P1 and 79.5% in P2, an absolute gain of 12.9 percentage points (or a gain of approximately 19%). This increase is also supported by the Gain and Loss breakdown (see Figure 5), with the bar chart clearly showing that the P2 value for the majority of the 5 items had a higher rate of correct answers in P2 when compared with the P1 values. On the other hand, from the Net Waterfall Chart (see Figure 6), we can see which of the items had negative (decreasing) results for P2 when compared with P1, i.e., a lower percentage of correct answers in P2. Items #3, #6, #9, #17, #18, #23, #26, #40, and #42 had decreasing P2 percentages when compared with their respective P1 percentages. We can see from the 46 total items in the CAIN items that nine items had worse performance, which goes to show why we must look at the individual items as well: the average may be fine (a gain of 12.9%), but not every item is going to improve from pre- to post-test, not immediately, at least. Certain questions may simply not have been sensitive enough to show improvement in P2, or, indeed, worse performance in P2 may be indicative of ineffective training.

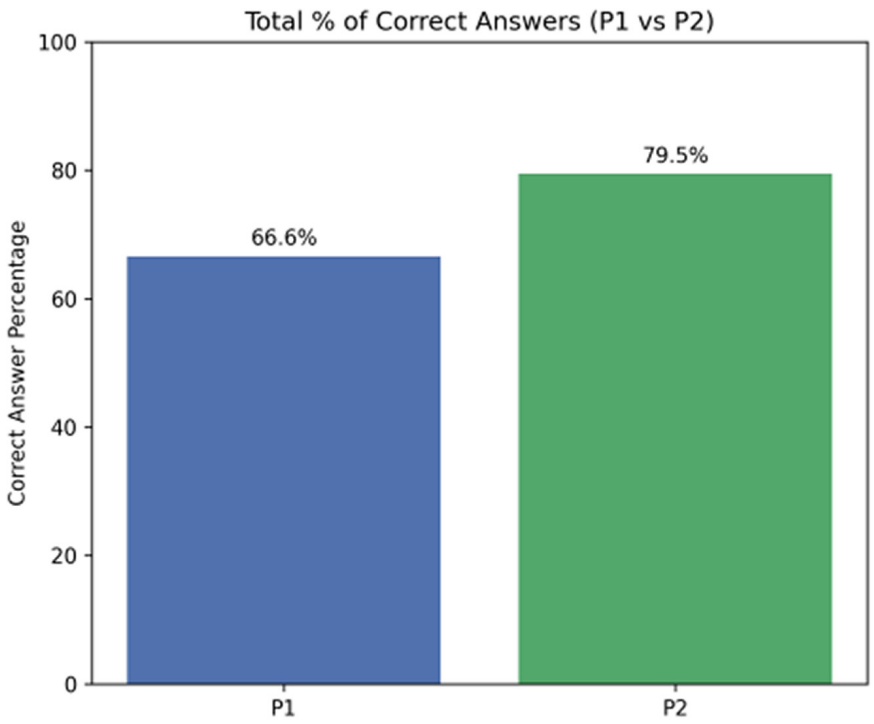

Fig. 4. Total correct answers P1 vs. P2

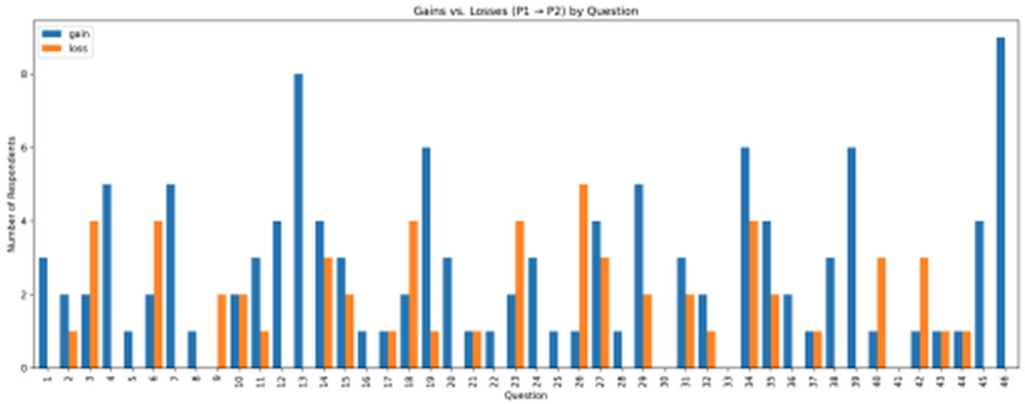

Fig. 5. Gain and loss chart

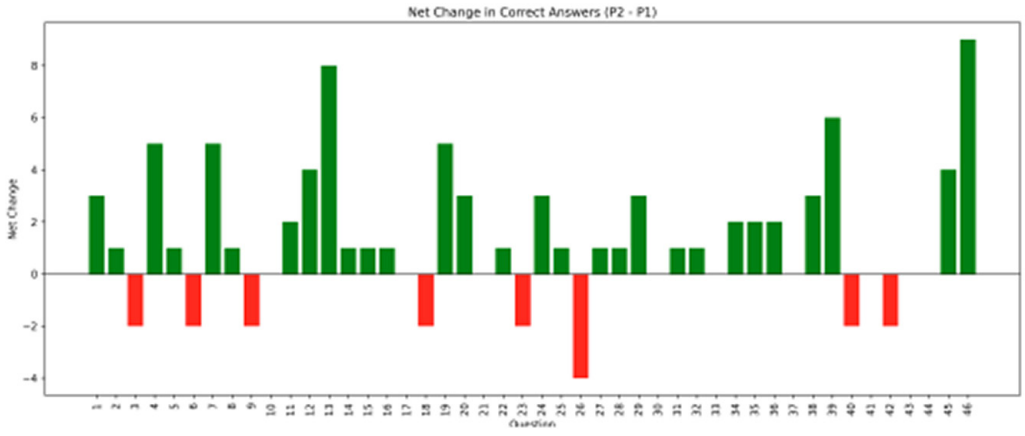

Fig. 6. Net waterfall chart

4.2 Performance within demographic subgroups

As displayed in Table 1, when performance is divided between the different demographic subgroups, we begin to see some interesting trends, although we have to be careful with the small sample size subgroups (e.g., age group 85–89 with n ¡ 5). For age, we see that all groups under 80 years of age had significant improvements in P2, the biggest of which was in the 70–75 age group with an improvement of 27.2 percentage points (57.1% to 84.3%).

The other large improvements were found in the 65–69 age group with an improvement of 20.8 percentage points and the 60–64 age group with an improvement of 8.7 percentage points. We also see that the 80–84 age group, with an extremely small sample size of n = 2, had a decrease of 60% (100% to 40%), while the 85–89 age group had an improvement of 20 percentage points, also with an extremely small sample size of n = 4. For gender, the male and female groups both had similar improvements from P1 to P2, with the male group having an improvement of 11.5 percentage points (67.6% to 79.1%) and the female group an improvement of 13.7 percentage points (66.0% to 79.7%). However, for the education level, we can see a more interesting result where those with High School and Primary/Intermediate levels of education have both seen significant improvements of 13.9 and 15.7 percentage points, respectively. However, those with Bachelor's/Graduate degrees had a decrease of 6 percentage points, while those with a master's degree had a dramatic decrease of 20 percentage points. This obviously does not seem to follow the same trend as those with a lower level of education, and the reason is likely either a ceiling effect in P1 or simply that the items were not hard enough for the post-test for higher-educated individuals. Table 1 shows socio-demographic characteristics of participants.

Table 1. Socio-demographic characteristics of participants

Demographic	% Pre-Test	% Post-Test	% Change
Age Group			
Age 60–64	69.0%	77.7%	+8.7%
Age 65–69	62.3%	83.1%	+20.8%
Age 70–75	57.1%	84.3%	+27.1%
Age 75–79	76.0%	80.0%	+4.0%
Age 80–84	100.0%	40.0%	–60.0%
Age 85–89	60.0%	80.0%	+20.0%
Gender			
Female	66.0%	79.7%	+13.7%
Male	67.0%	79.1%	+11.6%
Education Level			
Primary/Intermediate	62.3%	78.0%	+15.7%
High School	67.8%	81.7%	+13.9%
Bachelor/Graduate	84.0%	78.0%	–6.0%
Master's degree	100.0%	80.0%	–20.0%

In conclusion, the intervention led to a large overall effect on cognitive outcomes among the low- and moderate-educated older adults (refer to Table 1). In future studies, the nine questions that did not show any effect and the other eight that had negative values (see Figure 6) should be examined, and strategies for the highly educated subgroup should be considered to provide a positive effect for all subgroups.

5 DISCUSSION

5.1 Study overview

The findings of this study demonstrate that the majority of elderly Brazilian participants exhibited considerable enhancements in cybersecurity awareness following the AI-driven gamified training intervention. For age subgroups below 80, all exhibited statistically significant performance enhancements from P1 (pre-test) to P2 (post-test), with increases ranging from 8.7 percentage points in the 60–64 age group to 27.2 percentage points in the 70–75 age group. These findings are consistent with previous studies indicating that more active and less intensive learning methods are more appropriate for the learning requirements and attention spans of older adults [11, 12].

The 80–84 and 85–89 age groups, on the other hand, did not show the same positive trend. The 80–84 group (n = 2) went from 100% at P1 to 40% at P2, but the 85–89 group (n = 4) only went up by 20 points. These results, although derived from small sample sizes, may indicate challenges in engaging older users with restricted digital competencies and working memory [10]. Both males and females saw similar improvements in terms of gender. Males improved by 11.5 percentage points (from 69.0% at P1 to 79.0% at P2), and females improved by 13.7 percentage points (from 66.0% to 79.7%). These results corroborate the hypothesis that gamified training and personalized learning can advantage a broad spectrum of users, irrespective of gender, as the motivational components in games resonate with various learners [1, 21].

The enhancement among education-level subgroups was more varied. Individuals with Primary/Intermediate and High School education levels exhibited enhancements of 15.7 and 13.9 points, respectively, indicating that those with minimal prior knowledge derive the greatest advantage from the personalization and scaffolding offered by AI-based systems [12]. Conversely, individuals holding Bachelor's/Graduate and master's degrees experienced a reduction of six and 20 percentage points, respectively. This could be due to a ceiling effect, as these groups started with higher baseline knowledge, or because the training wasn't hard enough for them, which could have made them bored or uninterested [13].

In conclusion, the results demonstrate the efficacy of AI-driven gamified training for most subgroups, while indicating the necessity for additional modifications, particularly for the oldest and most educated participants.

5.2 Comparison with previous research

The favorable results identified in this study align with prior research regarding gamification and AI-driven personalization in cybersecurity education, especially for older adults. For example, Balon and Baggili [11] found that gamified training that includes things like points, badges, and feedback in real time is more interesting and helps people remember what they learned better than traditional

lecture-based methods. This study empirically corroborates this finding, demonstrating an average performance enhancement of approximately 11.5 percentage points across all groups.

Boopathi et al. [21] similarly showed that interactive learning tools with adaptive algorithms greatly increase learning motivation and retention among non-technical users. This study's results are in line with those findings, as both male and female participants showed similar improvements. Moreover, Bada et al. [12] emphasized that AI-driven adaptive learning systems can proficiently cater to various learner profiles by delivering content customized to specific requirements, a conclusion corroborated by the notable enhancements noted in the 60–75 age demographic in this study. But the fact that the most educated groups did worse shows that the adaptive gamification part may not work well for very skilled learners. Alnajim et al. [13] also said that gamified training that isn't complicated enough could make more advanced learners lose interest, which could make them do worse on post-tests.

The decline in performance among the 80–84 age group, despite being derived from a limited sample size, corroborates the findings of Sivagumaran [20], who identified cognitive load and interface complexity as obstacles for older users. Huda et al. [10] posited that interactive tasks ought to be simplified for older adults to prevent disengagement. This study, along with earlier research, shows that gamified and AI-driven learning is better than traditional methods in many ways. However, it needs to be improved even more, especially for certain groups like the very old and the very educated, to make sure that everyone can use it and stay interested.

5.3 Study impact and effectiveness

The main research question (RQ1) asked if personalized training with an AI-driven app could help older people in Brazil become more aware of cybersecurity. The findings of this study validated the efficacy of the intervention, as demonstrated by statistically significant enhancements in pre- to post-test scores, especially in the areas of cyber risk and prevention, with an emphasis on social engineering.

The study's secondary objectives, such as empowering users to identify and mitigate potential cyber threats, were successfully accomplished. Participants exhibited an enhanced capacity to identify and evade cyber fraud through tailored, scenario-driven assessments and immediate feedback mechanisms. These tools helped with active recall and memory retention, which is different from passive, lecture-based learning [1, 11]. Better ability to spot phishing and malware links after the quiz also showed that the risk of falling for cyber fraud was lower. The app's cloud-based structure made it scalable, accessible, and reliable, so it could train a lot of older people all over Brazil with enough coverage and throughput. As Fakhouri et al. [3] and Camilleri et al. [13] discussed, the AI-driven adaptive learning system made the content more personal by changing the order and difficulty of modules based on how well each student did. The intervention's beneficial effects, attained at a minimal marginal cost per capita, indicate its applicability to a wider demographic, especially for vulnerable populations, including individuals with disabilities or economically disadvantaged communities. This study shows how well AI can provide personalized education and cybersecurity training [9]. In conclusion, the AI-driven gamified app showed that it could help older people in Brazil become more aware of cybersecurity issues. This supports its use as a scalable and cost-effective way to help at-risk groups.

5.4 Limitations

The research revealed several limitations that are crucial for comprehending the study's scope and findings.

- **Geographic Scope:** The research was executed in a minor Brazilian city, indicating that the findings may not comprehensively reflect the wider Brazilian populace, especially regarding cultural differences.
- **Language Barriers:** Most of the cybersecurity terms and ideas were explained in English, which is not a language that most Brazilians speak. This may have impacted understanding and the efficacy of training.

Subsequent research must rectify these deficiencies by augmenting the sample size, incorporating a control group, and broadening the range of inquiries and geographical areas to guarantee more substantial results.

5.5 Future work

Future research should concentrate on broadening the study's scope by integrating demographic data from a more extensive and varied user population. It is also important to make the survey longer and add a human support system to see how emotional well-being affects learning. Some possible directions for future research are:

- Expanding the study to encompass elderly participants from diverse regions, demographics, and cultural backgrounds to guarantee the solution's wider applicability.
- Adding more questions to the survey and demographic data points to make it possible to do more detailed analysis and segmentation.

6 CONCLUSION

This paper looked at how AI-powered solutions can make learning more personal to help older people in Brazil become more aware of cybersecurity. The study showed that combining advanced AI technologies with fun and interesting ways to learn, like gamification, can effectively lower the number of cyber victims in this vulnerable group. AI's ability to spot patterns, adjust to each person's learning style, and add game-like elements to training makes it much better than traditional, one-size-fits-all methods. As cyber threats keep getting worse, it's more important than ever to make sure that older people and other vulnerable groups know how to stay safe online.

The study uncovered numerous important results. First, using AI for adaptive learning made it possible to customize the training content for each person based on their own skill level, which made it easier to use and more effective. Second, using gamification in every part of the training process not only made it more fun to learn, but it also increased user engagement, motivation, and knowledge retention. The training method followed Brazil's LGPD law, which showed that it was ethical because it protected users' personal information and kept their privacy during the study. The solution was also clearly scalable and cost-effective because the mobile

app was able to reach a lot of older people in Brazil, making it an affordable and widely available way to learn about cybersecurity.

The results of this study confirm that AI-driven, gamified training is a good way to raise awareness of cybersecurity among older people. By combining adaptive learning with game mechanics, the training was able to keep participants interested, especially those with less formal education, which helped them understand and remember cybersecurity concepts better. The study also found that the older and more educated groups did worse, which suggests that the training design may have been too complicated for some learners. These results show that the program needs to be improved so that it is both challenging and fun for all types of users. To make the program better, it needs to be redesigned over and over again based on the needs of the target audience, and it needs to have more customizable learning paths. This study helps create effective cybersecurity education methods that can be used by a lot of people and changed to fit different needs, making sure that vulnerable groups are digitally literate.

7 REFERENCES

[1] L. von Ahn and L. Dabbish, "Designing games with a purpose," *Communications of the ACM*, vol. 51, no. 8, pp. 58–67, 2008. https://doi.org/10.1145/1378704.1378719

[2] X. Li, "Impact assessment of cybersecurity awareness training: Moderating effects of age, gender, and education level," 2025. https://doi.org/10.2139/ssrn.5097059

[3] H. N. Fakhouri, B. Alhadidi, K. Omar, S. N. Makhadmeh, F. Hamad, and N. Z. Halalsheh, "AI-driven solutions for social engineering attacks: Detection, prevention, and response," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, IEEE, 2024, pp. 1–8. https://doi.org/10.1109/iccr61006.2024.10533010

[4] H. Tamut and I. K. Dutta, "Understanding and mitigating social engineering attacks to elderly people: A comprehensive survey of methods, impacts, and future solutions," in *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, 2024, pp. 0461–0470. https://doi.org/10.1109/uemcon62879.2024.10754693

[5] J. Camilleri, A. Sheil, M. O'Keeffe, M. Cronin, M. Gruben, and H. Murray, "Cybersafety card game: Empowering digital educators to teach cybersafety to older adults," in *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, ACM, 2025, pp. 1–12. https://doi.org/10.1145/3706599.3719806

[6] R. Salama, F. Al-Turjman, S. Bhatla, and S. P. Yadav, "Social engineering attack types and prevention techniques- A survey," in *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, IEEE, 2023, pp. 817–820. https://doi.org/10.1109/cictn57981.2023.10140957

[7] A. S. V. Nair and R. Achary, "Social engineering defender (SE. Def): Human emotion factor based classification and defense against social engineering attacks," in *2023 International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1)*, IEEE, 2023, pp. 1–5. https://doi.org/10.1109/icaia57370.2023.10169678

[8] G. Tempestini, E. Rovira, A. Pyke, and F. Di Nocera, "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*, vol. 3, no. 1, pp. 61–75, 2023. https://doi.org/10.3390/jcp3010005

[9] S. Jawhar, J. Miller, and Z. Bitar, "AI-driven customized cyber security training and awareness," in *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, IEEE, 2024, pp. 1–5. https://doi.org/10.1109/icaic60265.2024.10433829

[10] N. H. N. Zulkipli, N. A. M. Rashid, A. F. Zolkeplay, and A. G. Buja, "Synthesizing cybersecurity issues and challenges for the elderly," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 5, pp. 1775–1782, 2021. https://doi.org/10.17762/turcomat.v12i5.2180

[11] T. Balon and I. Baggili, "Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education," *Education and Information Technologies*, vol. 28, no. 9, pp. 11759–11791, 2023. https://doi.org/10.1007/s10639-022-11451-4

[12] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" *arXiv*, 2019.

[13] A. M. Alnajim, S. Habib, M. Islam, H. S. AlRawashdeh, and M. Wasim, "Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches," *Symmetry*, vol. 15, no. 12, p. 2175, 2023. https://doi.org/10.3390/sym15122175

[14] C. Shelke and R. Achary, "Social engineering attack and scam detection using advanced natural langugae processing algorithm," in *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2022, pp. 1749–1754. https://doi.org/10.1109/icoei53556.2022.9776697

[15] Gladden, Malik A. "Research aiming to understand baseline cybersecurity awareness for senior citizens and their training needs." (2025).

[16] B. A. Morrison, J. Nicholson, L. Coventry, and P. Briggs, "Recognising diversity in older adults' cybersecurity needs," in *Proceedings of the 2023 ACM Conference on Information Technology for Social Good*, ACM, 2023, pp. 437–445. https://doi.org/10.1145/3582515.3609565

[17] S. E. Hosseini, S. Charters, and P. Anthony, "Effects of smartphone social applications on elderly people's quality of life," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 2, pp. 137–152, 2023. https://doi.org/10.3991/ijim.v17i02.35457

[18] S. E. Hosseini and S. Pervez, "Effects of smartphone applications on elderly people's quality of life," *International Journal of Technology Management and Information System*, vol. 4, no. 4, pp. 28–38, 2022.

[19] S. E. Hosseini, "The effect of technology upskilling on the quality of life of elderly people in Iran," Ph.D. thesis, Lincoln University, 2023.

[20] Sivagumaran, Sinthujan. "Challenges of online security for senior citizens." (2023).

[21] K. Boopathi, S. Sreejith, and A. Bithin, "Learning cyber security through gamification," *Indian Journal of Science and Technology*, vol. 8, no. 7, pp. 642–649, 2015. https://doi.org/10.17485/ijst/2015/v8i7/67760

8 AUTHORS

Sidnei Sales is with the School of Applied IT, Whitecliffe, New Zealand.

Shahbaz Pervez is with the School of Applied IT, Whitecliffe, New Zealand (E-mail: shahbazp@whitecliffe.ac.nz).

Muhammad Nadeem is with the College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait.

Seyed Ebrahim Hosseini is with the School of Applied IT, Whitecliffe, New Zealand.

Muhammad Kashif Siddhu is with the Department of computer sciences, Faculty of Computer Sciences, Lahore Garrison University, Pakistan.