International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

September 2023 Issue 56 Volume 15 Number 3 Pages 327-333

ADR PROJECT PLANNING TO INCREASE CYBER SECURITY AWARENESS OF MOBILE DEVICE USERS

E. Sala E. Martiri

Department of Statistics and Applied Informatics, Faculty of Economy, University of Tirana, Tirana, Albania
enxhia.sala@unitir.edu.al, edlira.martiri@unitir.edu.al

Abstract- This article explores the significant difficulties related to data security and privacy in the current era characterized by increased use of mobile devices among customers and companies. The increasing reliance on mobile devices highlights the need for people to possess a comprehensive understanding of cybersecurity. In order to effectively tackle this issue, the paper proposes the utilization of the Action Design Research (ADR) methodology as an effective approach for increasing cybersecurity awareness. In today's digital environment, characterized by the prevalence of mobile devices as integral components of people's lives and essential tools for organizations, the significant risks related to data breaches, illegal access, and cyber threats are of paramount concern. The need for increased understanding about cybersecurity has become more evident. The protection of mobile devices from possible security breaches is of the utmost priority due to the storage of sensitive personal and business information on these devices. The paper proposes a mobile application that provides users with educational content, security checklists and threat warnings. Finally, it discusses the design principles that may arise from developing interventions that increase cybersecurity awareness among mobile device users.

Keywords: Mobile Devices, Cybersecurity, Awareness, Action Design Research, Mobile Application.

1. INTRODUCTION

Mobile devices have become a vital tool for both consumers and organizations, thanks to the increasing availability of high-speed wireless networks and an extensive number of mobile applications. This expanded use, however, has created new issues, such as ensuring the security of business data and managing the growing number of mobile devices. It has resulted in an increase in cybersecurity risks, making it critical for users to be aware of potential threats and take precautions to secure their sensitive data. This research investigates the significance of cybersecurity knowledge for mobile device users and makes recommendations for boosting awareness. Planning the Action Design Research (ADR) Project aims to answer three research questions, including the current level of knowledge and practices of mobile device users regarding cybersecurity, effective strategies for promoting cybersecurity awareness, and relevant metrics for evaluating the impact of initiatives to improve cybersecurity awareness. In addition, this paper discusses several theoretical foundations, such as the Technology Acceptance Model (TAM), Health Belief Model (HBM), Protection Motivation Theory (PMT), Diffusion of Innovations (DOI), and Social Cognitive Theory (SCT), that may help in the design and implementation of interventions to improve secure mobile device behavior among users.

This paper explores the use of Action Design Research (ADR) methodology in the development of a mobile application to address cybersecurity challenges. ADR is a practical approach to research that involves collaboration between researchers and practitioners to develop, implement, and assess interventions in real-world settings. This paper highlights the significance of organizational components such as user participation and support for cybersecurity measures in ensuring the project's success. In the end, this paper presents design principles that can guide the development of interventions that focus on promoting cybersecurity awareness among mobile device users.

2. SECURITY ISSUES

The increased use of mobile devices on the one hand, has also increased security concerns about these devices on the other hand. Mobile devices have become an indispensable tool for both individuals and enterprises, with sensitive information and data saved and exchanged via these devices [1]. One of the most significant problems is data protection in mobile devices. However, the use of an Intrusion Detection System (IDS) can help detect malicious activity and prevent further damage [2].

Since mobile devices are vulnerable to data breaches, hacking, and malware attacks that may harm sensitive data, there are being developed many ways to embrace security, like for example a CNN-LSTM based deep learning model that is feasible and adaptable for detecting advanced persistent threats and typical malware [3]. To secure data saved on mobile devices, organizations must deploy security measures such as encryption and two-factor authentication. Furthermore, regular software updates and patches are required to prevent vulnerabilities and keep devices up-to-date with the most recent security protocols.

Concerns about privacy are a major issue regarding mobile devices. Mobile devices capture a large quantity of data on their users, such as their location, browsing history, and personal information. This data is frequently exchanged with third-party applications and services, creating concerns regarding its privacy and security. Organizations must develop privacy rules to protect user data and ensure that it is utilized responsibly and openly. Users should also be informed about how their data is used and given the opportunity to opt out of data sharing [4].

Another major privacy concern is the potential for unauthorized access to mobile devices. Mobile devices are frequently lost or stolen, exposing people who are not permitted access to important data. To protect their data in the event of a lost or stolen device, organizations must deploy security measures such as remote data wiping [5]. Additionally, users must be educated on the importance of password protection and device security in order to prevent unauthorized access. Since security is and will continue to be one of the biggest challenges of our time, it is critical to understand the most common issues regarding smartphones.

3. CYBERSECURITY AWARENESS

As the security concern grows, so does the necessity for users to be aware of cybersecurity risks. Mobile devices have a large quantity of sensitive data, such as personal information, financial information, and organizational information, making them an ideal target for e-criminals. Understanding potential dangers is one of the most important parts of cybersecurity awareness for mobile device users. Users of mobile devices should be aware of typical dangers such as phishing, malware, and network attacks. Users should also understand how these threats can affect their devices as well as the possible consequences of a security breach. The use of strong passwords and authentication procedures is another critical part of cybersecurity knowledge. Users should avoid using easily guessable passwords and, whenever possible, use two-factor authentication. Biometric identification methods, such as facial recognition and fingerprint scanning, can also offer a layer of protection. Users should also understand the significance of keeping their devices up-to-date with the most recent security patches and software updates. These updates frequently include security enhancements and bug fixes to address known vulnerabilities. Finally, users of mobile devices should exercise caution while downloading apps or clicking on links. Malicious apps and URLs might infect the device with malware or access sensitive data. They should only download apps from trusted sites and double-check the app's legitimacy before downloading [6].

This study aims to address the following research questions utilizing the Action Design Research (ADR) methodology:

1) What's the actual state of cybersecurity understanding and usage among mobile device users, and what causes affect their behavior?
2) What are the most effective strategies for promoting cybersecurity awareness and encouraging secure behaviors among mobile device users, and how can these strategies be implemented in real-world settings?
3) What are the most relevant metrics for evaluating the impact of initiatives designed to improve cybersecurity awareness and promote secure behavior among mobile device users?

These research questions are only the starting point, as the research proceeds, other questions may arise. They do, however, provide a framework for investigating different aspects of cybersecurity knowledge and behavior change among mobile device users.

3.1. Contributing Theoretical Bases

In today's digital environment, increasing cybersecurity awareness among mobile device users is an essential concern. Several theoretical foundations have been offered to help with the design and implementation of interventions focused on promoting secure mobile device behavior among users. The Technology Acceptance Model (TAM) is a commonly used theory in cybersecurity awareness [7]. In accordance with the TAM, the utility and ease of access to a technology are significant factors in determining user acceptance and adoption. TAM has been applied to the domain of cybersecurity, and researchers have discovered that customers' impressions of the utility and simplicity of applying security measures, such as biometric authentication and mobile device management solutions, are important determinants of their adoption and compliance [8].

In the discipline of health psychology, the Health Belief Model (HBM) has been extensively utilized to explain and predict health-related behaviors such as vaccination uptake and cancer screening behaviors. The HBM assumes that people will take action to protect their health if they believe they are vulnerable to a health hazard, that the threat is significant, that the benefits of taking action outweigh the costs, and that they are capable of taking the necessary action. In the context of cybersecurity awareness and behavior modification, the HBM can be used to investigate mobile device users' attitudes and beliefs about the hazards and threats related to mobile device use, as well as the factors that impact their decisions to adopt secure behaviors [9]. Protection Motivation Theory (PMT) is a psychological framework that has been applied to many kinds of study situations, including health behavior, environmental behavior, and cybersecurity behavior. According to the PMT, people are motivated to protect themselves against perceived risks by taking action to lower their chance of damage. In the context of cybersecurity, PMT can be used to uncover the factors that influence mobile device users' motivation to adopt secure behaviors and protect their devices and confidential data.

For example, Lwin and Saw (2007) investigated how the measurement of behavior consequences links them to the recommended behavior and assessed whether individuals perceive these consequences as likely outcomes of the recommended action [10]. Other research has concentrated on the importance of coping evaluations such as self-efficacy and reaction efficacy in influencing users' willingness to engage in secure actions [11].

Diffusion of Innovations Theory (DOI) is a commonly used theoretical framework in innovation management research that explains how new ideas and technologies get adopted and shared among a community. DOI have been used in a variety of domains, including information systems, to analyze the adoption and spread of new technology such as smartphones and mobile apps. DOI can be used to understand how new and creative cybersecurity solutions can be adopted and spread among mobile device users in the context of cybersecurity awareness and behavior change. Organizations can improve cybersecurity awareness and behavior change among mobile device users by identifying causes impacting the dissemination of security of smartphones technologies, such as perceived relative advantage, compatibility, complexity, trialability, observability, and by utilizing appropriate strategies to promote their adoption and use has been extended to the domain of cybersecurity awareness to explain how users acquire and utilize security information and skills [12] [13]. According to the Social Cognitive Theory (SCT), people learn through observation, imitation, and reinforcement. Interventions that combine social learning and reinforcement mechanisms, such as peer mentorship and gamification, have been demonstrated to be helpful in promoting secure behaviors among mobile device users [14].

Choosing the best theoretical foundation for developing a game mobile app to increase cybersecurity awareness is highly dependent on the characteristics of the intended user group and the behaviors we wish to improve. However, based on the presented models, a combination of the TAM and the SCT would provide a comprehensive approach to our objective. The TAM, which emphasizes perceived usefulness and usability, can be especially beneficial during the design phase of our mobile application. User adoption and continued utilization can be increased by making the application user-friendly and demonstrating its value in strengthening cybersecurity. Although, SCT can be utilized to make learning more interactive and interesting. Learning occurs in a social context and can be accelerated through observation, imitation, and reinforcement, according to this theory. This can be accomplished through the incorporation of game mechanics such as scoring systems, competition, collaboration, and rewards, which not only make learning enjoyable but also encourage users to adopt secure behaviors. In a game context, the peer-learning aspect inherent to SCT can be an effective instrument.

However, it is important to note that no single theory can cover every aspect. All the theories mentioned above can provide valuable insights into how to positively influence user behavior and increase the effectiveness of our application. Therefore, a multi-theoretical approach that combines elements from each of these models may be the most effective method for developing an effective mobile app for cybersecurity awareness.

4. PLANNING THE ADR PROJECT

The growing reliance on mobile devices and the sophistication of cyberthreats require proactive methods to strengthen user cybersecurity awareness. In this context, the ADR methodology develops as an encouraging path due to its customized qualities that adapt to the dynamic and practical aspects of cybersecurity awareness. ADR is an analytical approach for developing prescribed design expertise via the construction and assessment of combined IT artifacts within an organizational context [15]. It provides a framework for undertaking research with the goal of solving real problems and improving organizational performance. As a result, it is an ideal methodology to use when developing a mobile application to raise cybersecurity awareness. Furthermore, ADR methodology involves the collaboration of both researchers and practitioners [16]. Working closely with stakeholders to understand their needs and requirements, as well as co-designing interventions to satisfy those needs, is required. This method ensures that the study is based on the practical realities of the organization and is more likely to result in relevant and effective actions.

Lastly, the ADR approach includes iterative design, implementation, and evaluation cycles. This technique enables continual intervention, improvement, and refining. The ADR team may guarantee that the intervention is effective and satisfies the needs of users by testing and modifying it in many cycles. When evaluating the suitability of ADR for improving cybersecurity awareness among mobile device users, a comparative examination with other research methodologies, including Experimental Research, Case Study Research, and Ethnographic Research, reveals the distinctive merits of ADR. Experimental research is very valuable for assessing certain variables due to its controlled setting. Nevertheless, the contextual importance of ADR extends beyond purely controlled evaluations. ADR involves the active participation of stakeholders and users throughout the design process, leading to the development of solutions that specifically target practical requirements.

The use of this collaborative method helps to reconcile the disparity that exists between controlled trials and the complex dynamics inherent in the cybersecurity field. Case Study Research examines specific situations deeply, providing valuable insights. However, the iterative improvement method of ADR continues to preserve its competitive advantage. The constant evolution of cyber dangers necessitates the ongoing modification of solutions. The dynamic nature of

ADR enables it to adapt in real-time to constantly evolving cyber environments, thereby increasing its application and efficacy. Ethnographic research provides comprehensive insights into user behavior inside their authentic environments. Nevertheless, the primary advantage of ADR is its prompt practicality. The direct contribution of ADR to behavioral change is achieved through its emphasis on the development of practical treatments. The partnership between academics and practitioners facilitates the development of treatments that are both intellectually rigorous and operationally feasible, resulting in concrete outcomes.

Acknowledging the qualities of ADR does not exclude the possibility of enhancing its effectiveness by integrating it synergistically with components from other research approaches. The inclusion of controlled experiments derived from the principles of Experimental Research may provide a valuable source of quantitative data that can enhance the qualitative insights provided by ADR. A more thorough knowledge of the success of treatments created using ADR may be attained by measuring their effects. The integration of case studies in conjunction with ADR has the potential to provide comprehensive perspectives on distinct user settings. ADR's iterative structure enables real-time alignment, while case studies provide comprehensive analyses of user experiences, preferences, and issues. By incorporating these observations into the iterative stages of ADR, a more accurate and thorough refining process may be achieved, resulting in improved practicality and applicability of the interventions. The integration of ethnographic methodologies has the potential to enhance ADR by providing a more comprehensive understanding of user behavior. The use of ethnography, with its immersive observations and data that is rich in context, offers valuable and nuanced insights that may inform the design of interventions. By incorporating qualitative viewpoints into the user-centered approach of ADR, approaches may be developed with a deeper comprehension of the behavioral elements involved.

Overall, the effectiveness of ADR in promoting cybersecurity awareness among mobile device users becomes apparent when compared to other research methodologies. The collaborative, iterative, and user-focused method of ADR has intrinsic benefits. However, the potential of ADR is further enhanced when it incorporates aspects of Experimental Research, Case Study Research, and Ethnographic Research in a synergistic manner. The use of this complete approach guarantees the development of interventions that are grounded in academic frameworks and demonstrate practical efficacy within the constantly changing landscape of cybersecurity awareness.

4.1. Organizational Commitment

In today's technologically advanced world, cybersecurity has become a crucial concern for both individuals and businesses. With the increasing reliance on mobile devices, it is critical to protect sensitive data and personal information. The purpose of this article is to investigate the development of a technological solution, specifically a mobile game application, to address cybersecurity problems. The project is an IT-driven initiative, and its ultimate success is dependent on users' willingness and capacity to properly adopt and use technology. As a result, this article emphasizes the significance of organizational elements such as user involvement and organizational support for cybersecurity measures, which may affect project success.

The success of every project is strongly dependent on the team members involved. The ADR team for this project should include a Project Manager, a Tech-Lead, a UX Designer, a Cybersecurity Expert, and a Communications Specialist. The Project Manager oversees the complete project coordination, including the monitoring of timelines, budgets, and deliverables. The Technical Lead is in charge of all technical aspects of the project, such as software development, data management, and security. The User Experience Designer creates user interfaces, conducts user research, and ensures that the program is logical and interactive. The Cybersecurity Expert is in charge of offering subject matter expertise on cybersecurity risks and best practices, as well as assessing the application's content and functionality's accuracy and efficacy.

Finally, the Communications Specialist creates and implements a communication strategy to launch the application and encourage user engagement. It is critical to obtain organizational commitment from stakeholders at all levels, including management, IT workers, and end-users, to ensure the project's success. This could be accomplished by outlining the project's objectives, benefits, and potential hazards, as well as emphasizing the potential impact. To involve stakeholders and assure their commitment to the project, regular communication, feedback meetings, and training sessions could be used.

4.2. Building the Artifact

An initial artifact has been offered, such as a mobile game application, which might give users the essential information and tools to improve their cybersecurity policies. In this paper, we explore the fundamental elements of such an application as well as a strategy for releasing alpha and beta versions of the application. The proposed gaming mobile application would have a number of essential components that would help users improve their cybersecurity procedures.

First, it would include educational content such as informative articles, films, or infographics that highlight typical cybersecurity risks and how to avoid them. Second, the app would include security checklists that would give users a list of cybersecurity best practices, such as enabling device encryption, routinely updating software, and utilizing strong passwords. Third, the program would deliver threat alerts, which would inform users of potential cybersecurity hazards such as phishing scams or data breaches and advise them on how to avoid them. Furthermore, the application could include a built-in browser that provides additional security features, such as ad blocking, anti-tracking, and VPN connectivity.

Finally, the program, by having a user-centered approach, would encourage user feedback and engagement by requesting comments, offering prizes for accomplishing cybersecurity activities, and enabling social sharing tools to raise cybersecurity awareness. This initial artifact could be developed using an agile software development methodology with frequent iterations and user testing to refine and improve the application's features and functionality. The artifact's ultimate purpose would be to provide mobile device users with an accessible and engaging platform to raise cybersecurity awareness and encourage the adoption of secure behaviors.

4.3. Intervening

Before launching the alpha version, the ADR team would share the application with a restricted set of internal stakeholders, such as ADR team members, IT experts, or other cybersecurity specialists, to gather input and uncover bugs or other issues. Internal testing should also be undertaken to ensure that the application satisfies technical criteria, is user-friendly, and addresses any safety concerns that have been found. The ADR team might choose a group of beta testers, or individuals who have proven an interest in cybersecurity, to roll out the beta version after working on the program based on input from the alpha version. The ADR team would provide the beta version to the assigned group of testers, along with instructions on how to use the application, and report any problems or feedback. The team would then gather input from the beta testers, including their impressions of the application, any problems they encountered, and suggestions for improvement.

Finally, before publishing the final version, the team would review the input and improve the application. It is critical for the ADR team to communicate clearly with stakeholders and users during both the alpha and beta testing phases, to provide clear instructions on how to use the application, and to respond to feedback and concerns that arise. This can help guarantee that the application's final version fits the needs of users while also effectively addressing the identified cybersecurity threats.

The mobile app could be deployed on various platforms, such as the Google Play Store for Android devices or the App Store for iOS devices. The app could also be distributed through other channels, such as the official website of the university or through collaborations with other organizations or companies. Once the mobile app is released, it might evolve based on users' feedback, for example. Thus, users may submit comments on the app's usability and features as they begin to use it. This feedback could be used to make improvements and update the app accordingly.

4.4. Evaluating

The ADR team could utilize the following assessment methodologies to assess the success of a mobile application meant to raise mobile device users' cybersecurity awareness:

- User testing: The ADR team could undertake user testing to gain input on the application's features, usability, and efficacy. This could entail watching users interact with the program and asking them for feedback on their experience.
- Pre- and post-intervention surveys: The ADR team might administer questionnaires to users before and after using the program to analyze changes in their cybersecurity awareness and behavior. This could include questions about their understanding of typical cybersecurity risks, their use of secure procedures, and their confidence in their capacity to protect their mobile devices.
- Usage analytics: The ADR team might collect and analyze data on how users interact with the program, such as how frequently they use it, which features they use the most, and which content is most effective at raising cybersecurity awareness.
- Security issues: The ADR team might track incidences of cybersecurity breaches or attacks among app users and compare this data to previous trends to see if the app is effectively reducing the frequency or severity of such incidents.

The ADR team can measure the efficacy of the mobile application in raising cybersecurity awareness among mobile device users and encouraging the adoption of secure behaviors by combining these evaluation approaches. This may help in the identification of areas for improvement and the development of future versions of the application.

4.5. Analyzing the Intervention Results

The ADR team must employ suitable data analysis methodologies to assess the effectiveness of the intervention. We propose a data analysis approach to analyze the intervention results of a mobile application designed to increase cybersecurity awareness among mobile device users. Thus, the ADR team might analyze the mobile application intervention results using a combination of quantitative and qualitative data analysis methodologies. The team could use descriptive statistics to describe data on user interaction with the app, such as frequency of usage, duration of use, and number of sessions, to start. They could also review data on the application's features and content that users interact with the most.

Secondly, the team might apply inferential statistics to evaluate the application's influence on users' cybersecurity awareness and behavior [17]. This could entail comparing survey responses from before and after the intervention to see if users' knowledge and behavior changed significantly as a result of using the program. Furthermore, the team could do a content analysis of the user input obtained throughout the evaluation phase, looking for common themes or concerns relating to the app's usability, functionality, and efficacy.

Finally, to acquire a better knowledge of users' experiences and impressions of the application, the team could conduct qualitative analyses of user feedback, such as interviews or focus groups. Regarding the feasibility of

Building, Intervention and Evaluation (BIE) cycles it has been determined the number of BIE cycles by the scope and complexity of the intervention as well as ADR teams resources. In general, many BIE cycles are recommended to refine the intervention and ensure that it is effectively serving the needs of users. The number of cycles, however, should be evaluated against the costs and resources needed to accomplish each cycle, as well as the duration required for obtaining the intended results.

5. CONCLUSIONS

Increased reliance on mobile devices demands innovative approaches to cybersecurity. In response, this paper proposes the development of a mobile game application aimed at increasing user cybersecurity awareness and encouraging secure behavior. Some design principles that may arise from this research aimed at raising mobile device users' cybersecurity awareness include:

A user-centered approach, which is crucial to the intervention's effectiveness because the goal is to engage and educate users in a way that is relevant and meaningful to them. Understanding users' requirements, preferences, and habits, as well as creating the intervention to fulfill those needs, is required.

– Gamification: Because it taps into users' innate drive for achievement, recognition, and competitiveness, gamification may be a strong tool for enhancing engagement and motivation. Incorporating aspects such as points, badges, and leaderboards into the application's design can help make learning more pleasurable and rewarding for users.

– Personalization: Making the learning experience more relevant and meaningful to individual users can help. This could include adapting the application's content to users' interests or job tasks as well as offering individualized feedback on their progress.

– Simplicity: The application should be designed to be simple and intuitive, with straightforward navigation and brief, easy-to-understand material. This is especially true in the context of cybersecurity awareness, where complicated technical concepts might be difficult to understand for non-experts.

Therefore, by adopting a user-centered approach, including gamification and personalization components, and emphasizing simplicity, designers can create interventions that are more engaging, effective, and long-lasting. A strong organizational commitment, a devoted and diverse ADR team, and a well-structured intervention plan are essential for the success of this project. This paper presents a framework for developing an effective cybersecurity game app by using appropriate methods for constructing the artifact, intervening, evaluating, and analyzing. The iterative nature of BIE cycles further assures the application's continual improvement and adaptability to user feedback and emerging cybersecurity threats. In conclusion, the proposed project has the potential to contribute to a safer and more secure digital environment for all mobile device users by significantly advancing cybersecurity awareness.

ACKNOWLEDGEMENTS

The authors would like to express their gratitude to the related courses lecturers at Lund University, Lund, Sweden. Their exceptional guidance, expertise, and dedication have been instrumental in shaping and understanding of design science research and its application in information systems.

REFERENCES

[1] B. Markelj, I. Bernik, "Mobile Devices and Effective Information Security", Innovative Issues and Approaches in Social Sciences, Vol. 6, No. 2, pp. 40-52, 2013.

[2] Y.H. Alagrash, H.S. Mehdy, R.H. Mahdi, "A Review of Intrusion Detection System Methods and Techniques: Past, Present and Future", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 54, Vol. 15, No. 1, pp. 11-17, March 2023.

[3] E.J. Khalefa, D.A.A. Salman, "Attribution Classification Method of Advanced Persistent Threat (APT) Malware Using AI Learning", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 54, Vol. 15, No. 1, pp. 1-10, March 2023.

[4] A. Altalbe, "Do New Mobile Devices in Enterprises Pose a Serious Security Threat?", Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, pp. 53-57, 2013.

[5] R. Kinage, J. Kumari, P. Zalke, M. Kulkarni, "Mobile Tracking Application", International Journal of Innovative Research in Science, Engineering and Technology. Vol. 2, No. 3, pp. 617-623, 2013.

[6] Y. Elsantil, "User Perceptions of the Security of Mobile Applications", International Journal of E-Services and Mobile Applications, Vol. 12. No. 4, pp. 24-41, 2020.

[7] F.D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", MIS Quarterly, Vol. 13, No. 3, pp. 319-340, 1989.

[8] F.D. Davis, "User acceptance of information technology: system characteristics, user perceptions and behavioral impacts", International Journal of Man-Machine Studies, Vol. 38, No. 3, pp. 475-487, 1993.

[9] C.J. Carpenter, "A Meta-Analysis of the Effectiveness of Health Belief Model Variables in Predicting Behavior", Health Communication, Vol. 25, No. 8, pp. 661-669, 2010.

[10] M.O. Lwin, S.M. Saw, "Protecting children from myopia: A PMT perspective for improving health marketing communications", Journal of Health Communication, Vol. 12, No. 3, pp. 251-268, 2007.

[11] D.L. Floyd, S. Prentice-Dunn, R.W. Rogers, "A meta-analysis of research on protection motivation theory", Journal of Applied Social Psychology, Vol. 30, No. 2, pp. 407–429, 2000.

[12] E.M. Rogers, "Diffusion of Innovations", Free Press, 4th ed., New York, USA, 1995.

[13] A. Bandura, "Social Foundations of thought and Action: A Social Cognitive Theory", Prentice-Hall, Inc., Englewood Cliffs. New Jersey, USA, 1986.

[14] Q. Xu, Z. Su, R. Lu, "Game theory and reinforcement learning based secure edge caching in mobile social networks," IEEE Transactions on Information Forensics and Security, Vol. 15, pp. 3415–3429, 2020.

[15] M.K. Sein, O. Henfridsson, S. Purao, M. Rossi, R. Lindgren, "Action Design Research", MIS Quarterly, Vol. 35, No. 1, pp. 37-56, 2011.

[16] M.T. Mullarkey, A.R. Hevner, "Entering Action Design Research", New Horizons in Design Science: Broadening the Research Agenda, LNCS 9073, pp. 121-134, 2015.

[17] D. Avison, F. Lau, M. Myers, P.A. Nielsen, "Action Research", Communications of the ACM, Vol. 42, No. 1, pp. 94-97, 1999.

BIOGRAPHIES

Name: **Enxhia**
Surname: **Sala**
Birthday: 18.08.1993
Birth Place: Tirana, Albania
Bachelor: Mathematics and Informatics Engineering, Department of Applied Mathematics, Faculty of Natural Sciences, University of Tirana, Tirana, Albania, 2014
Master: Mathematics and Informatics Engineering, Department of Applied Mathematics, Faculty of Natural Sciences, University of Tirana, Tirana, Albania, 2016
Doctorate: Student, Information Systems in Economy, Department of Statistics and Applied Informatics, Faculty of Economy, University of Tirana, Tirana, Albania, Since 2022
The Last Scientific Position: Lecturer, Department of Statistics and Applied Informatics, Faculty of Economy, University of Tirana, Tirana, Albania, Since 2019
Research Interests: Information Systems, Information Security
Scientific Publications: 14 Papers

Name: **Edlira**
Surname: **Martiri**
Birthday: 06.04.1980
Birth Place: Shkoder, Albania
Bachelor: Informatics, Department of Informatics, Faculty of Natural Sciences, University of Tirana, Tirana, Albania, 2007
Master: Advanced Informatics, Department of Informatics, Faculty of Natural Sciences, University of Tirana, Tirana, Albania, 2009
Doctorate 1: Information Systems, Department of Statistics and Applied Informatics, Faculty of Economy, University of Tirana, Tirana, Albania, 2016
Doctorate 2: Information Security, Department of Information and Communication Technology, Faculty of Engineering, Norwegian University of Science and Technology, Gjovik, Norway, 2022
The Last Scientific Position: Assoc. Prof., Department of Statistics and Applied Informatics, Faculty of Economy, University of Tirana, Tirana, Albania, 2019
Research Interests: Information Security, Biometric Systems, Data Management
Scientific Publications: 63 Papers, 6 Books, 8 Projects, 2 Theses
Scientific Memberships: European Association of Biometrics