ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOCTORAL (PhD) THESIS BOOKLET

ESMERALDA KADËNA

A Threat Avoidance Perspective of Users' Security Behaviours in Smartphones: Albania versus Hungary

Supervisors: Dr. András Keszthelyi and Prof. Dr. Katalin Takács-György

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES

Budapest, 2022

Table of Contents

Summary

The thesis' research was conducted around the idea of giving a better understanding of the factors responsible for the users' security behaviours in smartphones. The study's primary purpose was to assess the influence of smartphone users' cognitive factors and individual differences and determine whether the motivation of using smartphone security technologies leads to better security behaviour in different cultures. The conceptual model was developed based on contextualization of Technology Threat Avoidance Theory (TTAT) as an extension of the Protection Motivation Theory (PMT). The cognitive factors incorporated the TTAT predictors of behaviour in the form of threat appraisal factors (threat perception and its two antecedents: perceived threat susceptibility and severity) and coping appraisal factors (safeguard effectiveness, safeguard cost, and self-efficacy). In addition, three broad constructs, impulsivity, risk, and distrust propensity of users were included.

This study focused on Albanian and Hungarian smartphones users. A web-based survey was used to gather the data, and in total, 588 responses were kept for analysis. Descriptive statistics and the Partial Least Square Structural Modeling (PLS-SEM) were used to analyze the gathered data. To better explain the threat assessment process in different cultures, an alternative approach was proposed by conducting a Multi-Group Analysis that involved two groups of interest. At first, the model was tested with all the valid data. Then, the multigroup analysis between users in Albania and Hungary was performed, and the results were presented in a systematic and detailed way. Path coefficients, t-statistic values, and p-values were generated by emphasizing significant differences and similarities between the two countries. Also, a separate analysis was performed for each group for a better understanding.

The most finding to emerge from this study is that applying the theoretical model across different countries will lead to different results for each of them. These results improve knowledge and understanding of the effect of cultural differences in the smartphone security context. This suggests that cultural differences should be considered in future studies when investigating individuals of different cultures. This dissertation provides a significant opportunity to advance the knowledge regarding human behaviours in smartphone security. It can be regarded as a first step towards understanding Albanian and Hungarian smartphone users.

Summary in Hungarian language – Magyar nyelvű összefoglaló

A disszertáció alapjául szolgáló kutatás célja a mobiltelefonok biztonságával kapcsolatos magatartást meghatározó tényezők feltárása, a mobilhasználók kognitív tényezőinek és az egyéni különbségek kiértékrlése, valamint azon, a mobilbiztonsági technológiák használatakor jellemző motivációk azonosítása, amelyek jobb biztonsági magatartást eredményeznek a különböző kultúrákban.Az elvi modellt a technológiai veszélyek elkerülése elméletének (TTAT) megfelelő kontextusba helyezésével alkottam meg, mint a védelem-motiváció elmélet (PMT) egy kiterjesztését. A kognitív tényezők magukba foglalják a TTAT viselkedés-előjelzőit a fenyegetésértékelési tényezők formájában (fenyegetés érzékelése és ennek két előzménye, az észlelt fenyegetettség és a súlyosság), valamint a megküzdésértékelés tényezőit (biztonsági intézkedések hatékonysága, ára, önhatékonyság). A továbbfejlesztett TTAT-modellben a mobilhasználók három jelentős osztályozási tényezőjét (impulzivitás, kockázati hajlam és bizalmatlanság) is figyelembe vettem.

A vizsgálathoz kérdőíves kutatást folytattam 2021-ben magyar és albán válaszadók körében, 588 értékelhető kitöltéssel. Az adatok kiértékelését varianciaalapú strukturális egyenletek modelljével végeztem (PLS-SEM). Az eltérő kultúrából adódó fenyegetésértékelési folyamatok pontosabb megmagyarázására alternatív megközelítést javasoltam, többcsoportos elemzéssel (MGA), ami két országot, Albániát és Magyarországot foglalja magába. Az összes érvényes adattal teszteltem a modellt, majd az albán és magyar telefonhasználók vonatkozásában a kapott eredményeket részletesen és rendszerbe foglalt módon mutattam be. Az útvonal együtthatók, t-statisztikai értékek és p-értékek a két ország közötti jelentős különbségek és hasonlóságok hangsúlyozásával lettek meghatározva, továbbá minden egyes csoportot külön is elemeztem.

Az elméleti modell a különböző országok esetében különböző eredményeket adott. Ezen eredmények segítik a kulturális különbségek hatásának megismerését és megértését a mobilbiztonság területén. Aa jövőbeli kutatások során a kulturális különbségeket figyelembe kell venni, ha a vizsgálat alanyai különböző kultúrákhoz tartoznak. A dolgozat érdemi lehetőséget ad arra, hogy a mobilbiztonsággal kapcsolatos emberi magatartást illető tudásunkat fejlesszük. Tekinthető úgy is, mint az albán és magyar mobilhasználók megértése felé tett első lépés.

1 Introduction

"Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information." – Kevin Mitnick (2000, p. 8)

Nowadays, mobile technology has become an inevitable part of almost every aspect of our lives. Since smartphones enable users to access many services, they have become essential. People are constantly connected with their mobile devices to the Internet. The world is changing rapidly, and the digital revolution is becoming hardly stoppable. Besides the chances of innovation in society, smartphones present significant risks. Their increasing popularity raises many security concerns. Security breaches on these devices can cause damages to individuals as well as organizations. Users can become victims of many security threats. On the other hand, their unsafe behaviours may create opportunities for hackers to attack the companies' applications and systems they access with their devices.

1.1 Problem Statement

Since the use of smartphones has been increasing, they have become an easy target for hackers [1]. The valuable information they contain poses risks of breaches to information security at the individual and organizational level. Besides addressing and mitigating security threats in smartphones, users' risky behaviours remain the most critical challenges in cybersecurity. Along with technological advancements, there is an increasing concern over the factors contributing to users' intentions and behaviours in security. Consequently, technology alone is not enough to ensure security. A vast number of security incidents and data breaches within organizations are associated with users' behaviour in mobile devices for personal and business reasons. Scholars and professionals continuously recommend awareness practices for users that focus on understanding smartphone security. It is still a challenge to identify if users understand and apply them correctly. We are in a situation where many cyber incidents can be avoided, but they continue to occur.

Naturally, a question arises: Why do people not protect themselves? The human aspect of security has gained many researchers' interest [2], [3]. The lack or minimal exploration in this area may be attributed to the fact that the human factor is complex to understand and manage within the information security context because human behaviour is unpredictable [4].

Researchers in information security has been focused on measuring the actual behaviours based on behavioural intention [5], [6], [7]. However, many issues are present due to other factors that can influence users' intentions. Thus, other researchers have faced difficulties in predicting information security behaviours [8], [9], [10], [11]. Besides, little is known about users' behaviours and their peculiarities from the countries of interest in this research. The lack of literature examining users' (in Albania and Hungary) behaviours in smartphones from the threat avoidance perspective presents an opportunity to add to the body of knowledge on smartphones' security. Thus, this study aims to address a gap and provide more evidence regarding users from Albania and Hungary on the factors that influence users' perceived threats and the factors that affect their intentions to use security technologies, which consequently can behave securely in smartphones.

This dissertation is presented along with the rise in cybercrime moving towards smartphones by emphasizing users' differences and their behaviours in security.

1.2 Research Objectives

This dissertation's key objective was to determine, with empirical data, the factors that influence users' security behaviours in smartphones. The research was classified from the perspectives of inquiry and objectives mode. From the viewpoint of inquiry, the study is conducted based on qualitative and quantitative data. From the objectives point of view, the research methods used were descriptive and explanatory. At first, preliminary research was conducted to accomplish the following objectives:

- O1: To introduce security and threats regarding smartphones.
- O2: To gain insight into user behaviour of smartphone security and their using habits based on related research findings.

- O3: To explore the research methods and theories for users' cyber-security motivations, threat perception, coping ability, and cybernetics.
- O4: To explain the samples used in the research model and define each users' group's cultural characteristics.

After content analysis, the following objectives were specified:

- O5: To examine the Albanian and Hungarian users' perceived threat regarding smartphones.
- O6: To examine the effects of safeguard measures (cost, effectiveness, and self-efficacy) in the Albanian and Hungarian users' motivation to use security technologies.
- O7: To investigate the influence of individual differences (Albania and Hungary) in motivation of using security technologies, and security behaviours in smartphones.
- O8: To investigate the Albanian and Hungarian users' security motivation and behaviour of using smartphones' security technologies.
- O9: To compare research results and highlight differences between Albanian and Hungarian users.

2 Research Methodology, Questions and Hypotheses

The research was carried out in three phases (Figure 2).

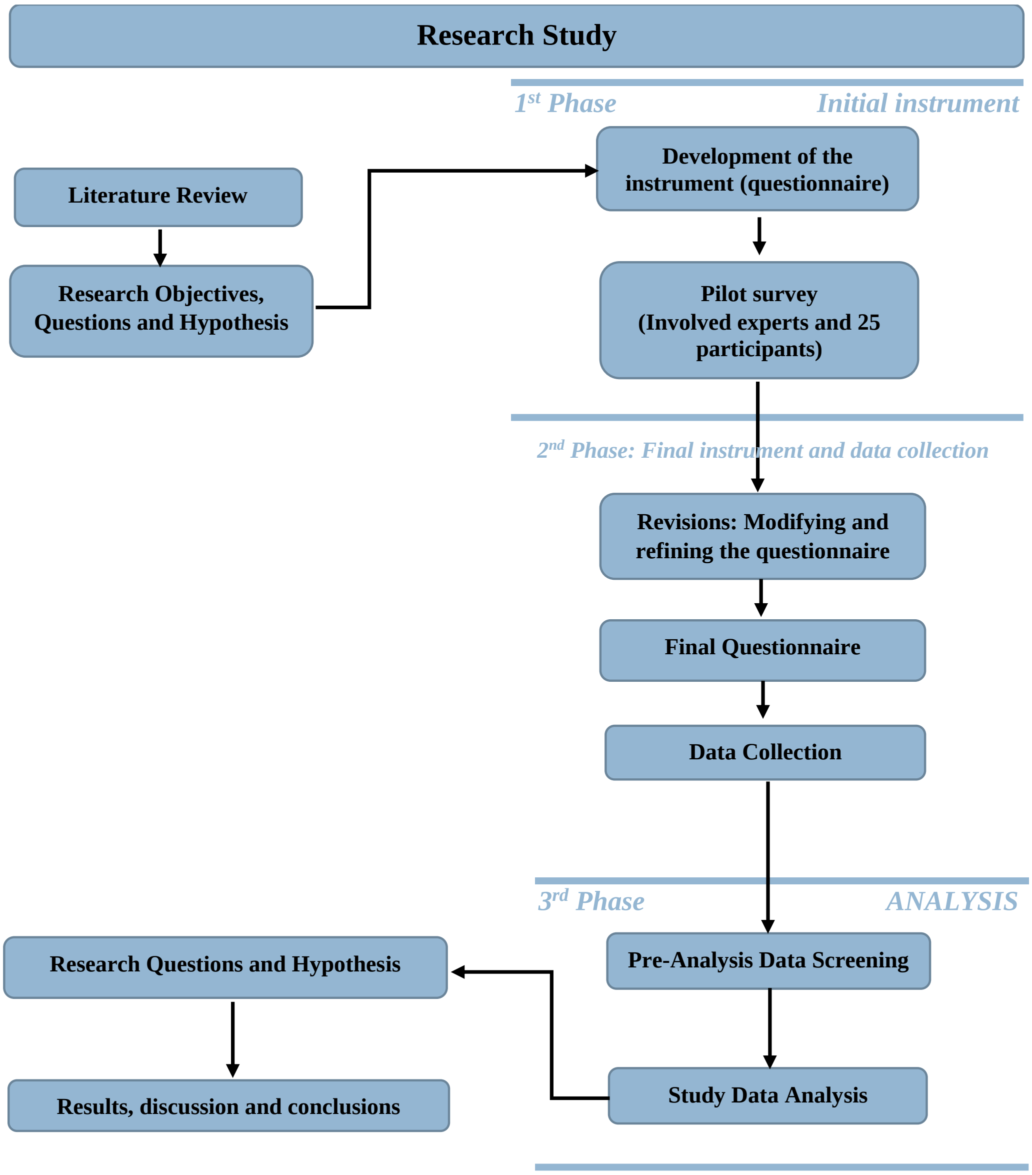
Research Study
1st Phase
Initial instrument
Literature Review
Research Objectives, Questions and Hypothesis
Development of the instrument (questionnaire)
Pilot survey (Involved experts and 25 participants)
2nd Phase: Final instrument and data collection
Revisions: Modifying and refining the questionnaire
Final Questionnaire
Data Collection
3rd Phase
ANALYSIS
Pre-Analysis Data Screening
Study Data Analysis
Research Questions and Hypothesis
Results, discussion and conclusions

Figure 1: Research Methodology

In the first phase, an exploratory study was conducted. The relevant literature review regarding smartphone threats and empirical studies were examined to define the research questions and hypotheses. The questionnaire was developed based on validated measures from the existing TTAT model. The first version of the questionnaire was used to examine the usability and identify possible issues with the instrument.

In the second phase (confirmatory stage), the instrument was improved after conceptualizing constructs in the research model. The final survey instrument was developed, followed by the data collection process that addressed the research questions and hypotheses. In the last phase, the confirmatory study was conducted. The quantitative data were analyzed using descriptive statistics and Structured Equation Modelling (SEM) PLS. A preliminary analysis was performed for data accuracy in the third phase (data analysis). It was examined if the assumptions for conducting path analysis were satisfied, followed by the study data analysis.

2.1 The research questions

The main question that drove this research was: "How do the cognitive factors (copping and threat appraisal) and individual differences influence the Albanian and Hungarian users' security behaviour in smartphones?

Five specific research questions were derived from the main question by applying the research model. The first research question integrated threat appraisal factors (perceived severity and susceptibility) and its outcome (perceived threat) that shape security motivation, leading to security behaviour. The second question aimed to investigate the effect of users' Perceived Threat on their motivation to defend against attacks and use smartphones' security technologies. The third research question has considered the three coping apprasial factors (Safeguard Effectiveness, Safeguard Cost, and Self-Efficacy) that shape Security Motivation, leading to Security Behaviour. The fourth question aimed to examine the influence of Security Motivation on users' behaviour using smartphones' security technologies. Finally, the fifth research question investigated the effect of risk and distrust propensity in users' perceived threat and the impulsivity impact in their motivation to use smartphones' security technologies. Based on these constructs, the research questions in this study are as follows:

- *Research question 1 (RQ1):* Do the Perceived Severity, Perceived Susceptibility, Risk, and Distrust propensity influence the users' Perceived Threats on smartphones?
- *Research Question 2 (RQ2):* Does the users' Perceived Threat influence their motivation to use smartphones' security technologies?
- *Research Questions 3 (RQ3):* Do the Safeguard Effectiveness, Safeguard Cost, Self-Efficacy, and Impulsivity influence users' motivation to use smartphones' security technologies?
- *Research Questions 4 (RQ4):* How do users' Security Motivation influence users' Security Behaviours?
- *Research Question 5 (RQ5):* Do the users' differences (Risk and Distrust Propensity and Impulsivity) influence their Perceived Threat and Motivation in using smartphones' security technologies?

2.2 Research Model and Hypotheses

Hypothesis 1 (H1)

As proposed and explained by Liang and Xue in 2010, threat perception is shaped by two antecedents: perceived severity and perceived susceptibility. Perceived severity stands for users' subjective belief regarding the damage that a malicious IT could affect their devices and systems. Similarly, perceived susceptibility is related to users' subjective belief that malicious IT will probably affect their devices and systems. According to Burns et al., a high threat severity level motivates individuals to protect themselves [12]. This research supports the scholars' arguments and findings, and thus, it was hypothesized:

H1a: Perceived susceptibility of being attacked positively affects perceived threat in smartphones.

H1b: Perceived severity of being attacked positively affects perceived threat in smartphones.

Hypothesis 2 (H2)

Maslow and Mitzen define safety as a basic human need [13], [14]. According to Liang & Xue, individuals' responses to health threats can be similar to their reactions to IT threats[15]. Also, Tu et al., and Posey et al., found out that users that receive "signals" about a possible risk show a higher motivation in engaging in response actions [16], [17]. Supporting the argues of the prior literature, it was hypothesized:

H2: Perceived threat positively affects security motivation in smartphones.

Hypothesis 3 (H3)

Here the safeguard effectiveness is defined in the context of smartphones security; if its application can be effective in using security technologies against the threats. Bandura in 1982 and Janz and Becker in 1984 explained that the outcome of using a safeguard is the user perception that can be noted as similar to outcome expectancy and the health belief model [18], [19]. When individuals feel safe and secure, they do not stress themselves to cope with the threats. Thus, a safeguard would make them feel more confident and adapt the security against the threats. Other authors confirm the relationship between safeguards and threats in the IT field, and they argue that in order to avoid security threats, technical, data and human safeguards must be deployed [20], [21].

H3: Safeguard effectiveness positively affects security motivation in smartphones.

Hypothesis 4 (H4)

Liang and Xue (2009) stress that safeguard cost is related to the physical and cognitive efforts such as money, time, inconvenience, and understanding level. Accordingly, the individuals compare benefits and costs before engaging in a behaviour. So, before taking action, people are usually making a cost-benefit analysis. Albuquerque Junior et al. concluded that some public institutions are not deploying the necessary tools for protection because of the high costs involved [22]. Woon et al. highlighted that people would enable wireless network security if its costs reduce [23]. Consequently, the higher the price/cost of a safeguard, the less motivation for users to use it.

H4: Safeguard cost negatively affects security motivation in smartphones.

Hypothesis 5 (H5)

Self-efficacy is defined as an individual’s confidence to take a safeguard measure. Agarwal et al., Compeau and Higgins, and Compeau et al. studied the relationship of self-efficacy with the IT adoption intent [24], [25],

[26]. Other authors have also explained that if the users' level of self-efficacy increases, they will be more motivated to perform IT security behaviour [3], [2]. As a result, their motivation to avoid IT threats using a measure will be stronger.

H5: Self-efficacy positively affects security motivation in smartphones.

Hypothesis 6 (H6)

In the TTAT model, there is no difference between motivation and intention [27]. In this case, security motivation can be explained by the behavioural intention to use security technologies. Two cognitive theorists concluded that behavioural intention is a significant and strong predictor of actual behaviour [28], [29]. This relationship has been confirmed by other researchers as well [30].

H6: Users' motivation to use smartphones' security technologies positively influences their security behaviour.

Hypothesis 7 (H7)

The effects of personality characteristics on cybersecurity behaviours have been in many IT researchers' attention [6]. In their studies, Giwah and Uffen et al. summarized that factors affecting the actual usage of mobile devices' security technologies are very different. They depend on the effect of other external variables such as individuals' personality differences [5], [7]. Consistent with the analysis and suggestions of Carpenter et al., this research includes the three constructs (Impulsivity, Risk and Distrust Propensity) [31].

Since this study focuses on users' behaviour to use security technologies on smartphones, I found it relevant to examine how these three individuals' differences impact security threats and motivations that shape security behaviour in using smartphones' security technologies. Thus, the seventh hypothesis presumes that individual differences affect users' perceived threat and security motivation that shape smartphone security behaviour.

H7: Individual differences affect users' perceived threat and security motivations that shape their smartphone security behaviours.

The hypotheses incorporated three constructs: impulsivity, risk propensity, and distrust propensity.

H7a: Impulsivity negatively influences motivation to use the smartphone's security technologies.

H7b: Risk propensity negatively influences users' perceived threat in smartphones.

H7c: Distrust propensity positively influences users' perceived threat.

The research model used for this work is presented in Figure 1.

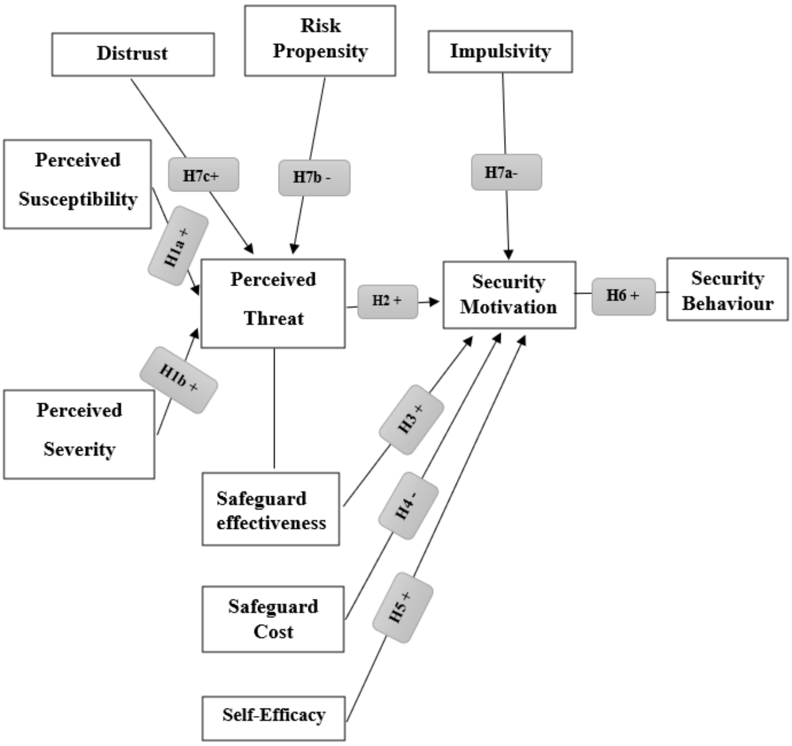

Figure 2: Research Model

2.3 Research Design: Procedure and Strategy

Considering the aim(s) of this research, the direction of this study is behavioural. The insights from the prior literature on IT security behaviour are applied to the smartphone context. The research methodology applied in this study could be in line with the positivist philosophy of research [32]. The authors pointed out that a structured methodology should be applied for the research using quantitative methods, including statistical analysis [180]. The aim was to obtain reliable, consistent, unbiased, and replicable results from other studies to present reality.

To study the chosen groups' security behaviours, it was relevant to be guided by the post-positivism research philosophy, known as post-empiricism and methodological pluralism [33]. And in this work, besides providing descriptive information and statistical analysis concerning the samples, understanding complex actions and contributing to knowledge growth were essentials.

2.3.1 Source of Data and Collection Method

A survey instrument was employed to examine the revised TTAT model and the resulting hypotheses in this study. After consulting with my advisors and for the purposes of this research, we realized that for a better understanding and to ensure validity, some of the items had to be changed and removed following the context of smartphones. The final web-based survey (in Google Forms) was appropriate for the present research. It allows the collection of a large number of responses in different locations and is a very useful method for testing the hypotheses [34].

The original language of it was English, and for better understanding, it was translated into Albanian and Hungarian languages. The survey contained three blocks of sections. The first one included demographic questions. The second section had questions related to users' habits and practices in smartphones and security. The final, and most important section included TTAT constructs and their respective items. The three forms (Albanian, English, and Hungarian) were active from October 26, 2020, until December 14, 2020. The electronic surveys were sent to the participants through email and social media platforms.

The target samples for this study were individuals from less than 20 years old to more than 50 years old from Albania and Hungary. It was decided to consider also the international students studying and living in Hungary. A prerequisite for participation was that participants own a smartphone and use it for personal, business reasons, or both. The samples were randomly selected within the target countries. The total number of the participants was 593, and after removing the outliers, only 588 responses were kept, of which 329 were from Hungary, 137 were from Albania, and 122 international students living in Hungary.

2.3.2 Methods of Data Analysis

Assumptions for conducting Path Analysis

- The collected data were checked for possible outliers with SPSS software. In addition, it was used Mahalanobis Distance method for each case. According to the calculations in SPSS, five outliers with a p-value less than 0.001 were detected and removed.
- Cook's distance statistics were performed to check if influential points or significant extreme cases can affect the model. The three dependent variables were checked, and from the results, the values were all below 1.0. To define the linearity between dependent and independent variables and to check if this assumption is satisfied, the scatterplots of the standardized residuals versus predicted values were examined for the three dependent variables: Perceived Threat (PTH), Security Motivation (SM), and Security Behaviour (SB). The graphs were assessed after generating Cook's distance statistics and the relationships were close to linear.
- The Durbin-Watson statistic test was used to access the independence of residuals of errors. Durbin-Watson statistic can range from 0 to 4, but the value indicates no correlation between residuals is two or around two. After the test, results showed that the D-W statistic for the three independent variables was around the value of 2.
- To check if the indicators meet the normality assumption, measures of kurtosis and skew were used. Both skew and kurtosis were analyzed through descriptive statistics. Acceptable skewness values should fall between − 3 and + 3, and the kurtosis range is appropriate from − 10 to + 10 when utilizing SEM [35]. The values indicated that they fall into the pre-defined ranges, and we had a normal distribution of the data, and the normality assumption was not violated.
- Another critical assumption is that multicollinearity should not exist. Factor analysis is an interdependency technique, and there should not be multicollinearity between the variables [36]. In this study, multicollinearity was checked with the help of the most widely used indicator, variance

inflation factor (VIF) [37]. The values were examined, and all the variables had a VIF below 10, indicating that this assumption was fulfilled.

- An essential step in PLS-SEM analysis is to evaluate the outer model. This evaluation aims to determine how well the items load on the hypothetical construct [38]. For this purpose, the reliabilities of each item and variables, internal consistency, construct validity, convergent validity, and discriminant validity were assessed [39].

Path Analysis in PLS-SEM

Path analysis in PLS-SEM was applied to address the five research questions and seven hypotheses. The relationships among independent variables and dependent variables were assessed by using SmartPLS 3.0. Path coefficients were used to measure the strength of the relationships between the variables, and they have range values between -1 and 1, and the p-values should be less than 0.05 [39]. Path coefficients closer to +1 indicate strong positive relationships, and closer to -1 indicate strong negative. If these values fall close to 0, the relationships are considered weak. In addition, t-statistics (two-tailed test) for significance testing of both inner and outer models was executed.

A summary of the research objectives, hypotheses, and applied tools is represented in Table 1.

Research objectives	Research Hypothesis	Related Theoretical Model and Applied survey questions	The research tools
O1: To introduce security and threats regarding smartphones.	-	Literature review: Chapter I – "Security and Smartphones"	Background sources.
O2: To gain insight into user behaviour of smartphone security and their using habits based on related research findings.	-	Chapter 2.1: Weakest Link- Human Factors importance Survey: Questions 8-20 related to users' habits and practices in smartphones and security.	-Background sources. -Descriptive statistics.
O3: To explore the research methods and theories for users' cyber-security motivations, threat perception, coping ability, and cybernetics.	-	Theoretical framework: Chapter 2.3 – TTAT Approach	-Background sources.
O4: To explain the samples used in the research model and define each users' group's cultural characteristics.	-	Cultural Differences: (AL-HU) - Chapter 2.2 Survey: Questions 1-7 related to demographics. - Chapter 4.1-4.3	-Hofstede 6-D Model -Descriptive statistics.
O5: To examine the influence of users' perceived threat and its two antecedents (perceived severity and perceived susceptibility) in users' security motivation in smartphones.	H1a: Perceived susceptibility of being attacked positively affects perceived threat in smartphones. H1b: Perceived severity of being attacked positively affects perceived threat in smartphones.	Liang and Xue (2009) TTAT Survey: Question 21 related to Perceived Susceptibility of getting a malicious IT (3 statements). Question 22 related to Perceived Severity of the threat consequences (8 statements).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H2: Perceived threat positively affects motivation to use smartphone's security technologies.	Liang and Xue (2009) TTAT Question 23 related to Perceived Threat (2 statements).	-Durbin-Watson Test -Normal P-P Plot -Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).

O6: To examine the effects of safeguard measures (cost, effectiveness, and self-efficacy) in the users' motivation of using security technologies.	H3: Safeguard effectiveness positively affects motivation to use smartphone security technologies.	Liang and Xue TTAT model (2009) Question 24 related to Perceived Safeguard Effectiveness (3 items).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H4: Safeguard cost negatively affects motivation to use smartphone's security technologies.	Liang and Xue TTAT model (2009) Question 25: 6 statements referring to Perceived Safeguard Cost	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H5: Self-efficacy positively affects motivation to use smartphone security technologies.	Liang and Xue (2009) TTAT Question 26 refers to the Self-Efficacy construct (5 statements).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
O7: To investigate users' security motivation and behaviour of using smartphones' security technologies.	H6: Users' motivation to use smartphones' security technology positively influences their behaviour of using smartphones' security technologies.	Liang and Xue (2009) TTAT Question 27 related to users' motivation in using security technologies (3 statements). Question 28 contains 5 (Yes/No) statements related to users' behaviours in using smartphone security tools/technologies.	-Durbin-Watson Test Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).

O8: To investigate the influence of individual’s differences in motivation and behaviour of using security technologies.	H7a: Impulsivity negatively influences motivations to use the smartphone’s security technologies.	Grasmick et al. (1993) Question 30 refers to impulsivity construct (4 statements).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H7b: Risk propensity negatively influences motivation to use smartphone’s security technologies.	Nicholson et al (2005) Question 29 refers risk propensity construct (8 statements).	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
	H7c: Distrust propensity negatively influences security motivation to use smartphone’s security technologies.	Ashleigh, Higgs, and Dulewicz, (2012) Question 31 refers to Distrust construct (5 statements)	-Kurtosis & Skewness. -VIF values (multicollinearity) -Reliability and Validity indicators. -HTMT values for Discriminant Validity. -Factor and Path Analysis, PLS-SEM (path coefficients, t-value, and p-value).
O9: To compare research results and highlight differences between Albanian and Hungarian users.	-	Research Results	Multigroup Analysis -AL vs. HU differences: β coef., p-values, t-values.

Table 1: The research objectives related to hypotheses, and the applied statistical tools

3 Hypotheses Tests

Before starting the analysis process, the raw data transferred in excel files were converted into a suitable format and coded for decision-making and conclusions.

3.1 Albania

In the case of Albania, only two hypotheses (H3+, H5+) and partially the first one (H1b+) were fully supported. Even though there is a relationship between Security Motivation and Behaviour, and the null hypothesis is rejected, the direction of this result is negative (β=-0322, $p<0.05$) and not positive as it was hypothesized.

Hence, the threat appraisal and coping factors cannot fully explain Albanian users' security motivations and behaviours in smartphone security. Also, the individual differences have not shown a significant effect. Therefore, the main research results for this group are as follows:

- Albanians perceive the threat in smartphones based only on the severity of an attack/threat and not its susceptibility. The more severe the nature of a threat, the more they will realize it. In addition, the study of this group failed to reject the null hypotheses for the influence of risk and distrust propensity. These variables did not show an effect on the way Albanians perceive the threats in smartphones.
- Their intention or motivation to use security technologies against a threat in smartphones is influenced only by the effectiveness of safeguards and their efficacy in intending to use secure technologies. The cost of a safeguard against threats, the users' perceived threat, and their impulsivity do not affect their motivation to use security technologies.
- Albanians' intention and motivation to use technologies to secure smartphones do not lead to better security behaviours.

3.2 Hungary

In the case of Hungary, only H2 and partially H7 were not supported. How Hungarian users perceive smartphone threats does not affect their intention to use smartphone security technologies. Also, the impulsivity of users is not related to their motivation to use secure technologies in smartphones. This study's research questions and hypotheses show that the threat appraisal factors cannot fully explain Hungarian users' security motivation and behaviour. In contrast, the coping appraisal factors can fully explain their security motivation and behaviour. Furthermore, as it was hypothesized, Risk and Distrust Propensity influence how they perceive the threats in smartphones. The following highlights the main results for the Hungarian group:

- Hungarian users perceived threats based on perceived susceptibility and severity factors by showing a positive relationship (H1a+ H1b+). But their perceived threat does not shape motivation on using security technologies in smartphones.
- Risk and distrust propensity influence the Hungarian users' perceived threat. The more risks they take, the less chance they will perceive the threats in their smartphones. The more they distrust, the more they will perceive threats in their smartphones. Therefore, the null hypotheses were rejected, and both sub- hypotheses (H7b- and H7c+) were fully supported for this group.
- The three factors of copping appraisal (safeguard effectiveness, cost, and self-efficacy) explain their security motivation in smartphones, and the three hypotheses (H3+, H4-, and H5+) were fully supported.
- Lastly, the intention/motivation of Hungarian users to use smartphone security technologies positively shapes their security behaviour. Thus, the hypothesis (H6+) was supported.

3.3 Multigroup Analysis

The multi-group analysis allows to test if pre-defined data groups have significant differences in their group-specific parameter estimates (e.g., outer weights, outer loadings, and path coefficients) [40]. SmartPLS provides outcomes of three different approaches (path coefficients, t-value, and p-value) based on every group's bootstrapping results. The groups have a significant difference for a p-value less than 0.05 and greater than 0.95 [41]. The significant differences were generated after the parametric test, assuming equal variances across the groups (Table 2).

Hypotheses	Paths	(β) -diff (AL vs. HU)	t-Value (|AL vs HU|)	p-Value (AL vs _HU)
H1a+	Perceived Susceptibility (PSU) -> Perceived Threat (PTH)	-0.075	0.891	0.374
H1b+	Perceived Severity (PSE) -> Perceived Threat (PTH)	-0.229	2.027	0.043
H2+	Perceived Threat (PTH) -> Security Motivation (SM)	0.128	1.229	0.220
H3+	Safeguard Effectiveness (SE) -> Security Motivation (SM)	-0.154	1.647	0.100
H4-	Safeguard Cost (SCO) -> Security Motivation (SM)	-0.174	2.057	0.040
H5+	Self-Efficacy (SEF) -> Security Motivation (SM)	0.196	1.783	0.075
H6+	Security Motivation (SM) -> Security Behaviour (SB)	0.175	2.020	0.044
H7a-	Impulsivity (IMP) -> Security Motivation (SM)	0.045	0.369	0.712
H7b-	Risk Propensity (RP) -> Perceived Threat (PTH)	-0.099	1.092	0.275
H7c+	Distrust (DIST) -> Perceived Threat (PTH)	0.067	0.710	0.478

Table 2: Parametric Test (PLS Multi-Group Analysis)

Hypothesis 1a: Perceived susceptibility of being attacked positively affects perceived threat in smartphones.

Hypothesis 1b: Perceived severity of being attacked positively affects perceived threat in smartphones.

Thesis 1a: There is a positive relationship between users' perceived threat susceptibility and perceived threat in smartphones, and this association is significant only in Hungary and not in Albania.

Thesis 1b: Users' perceived severity of being attacked positively affects smartphone perceived threat, and this association is stronger in Hungary than in Albania.

Published in: Kadena, 2017 [42]*; Kadena 2018* [43].

Hypothesis 2: Perceived threat positively affects security motivation in smartphones.

Thesis 2: Users who receive "signals" regarding possible threats will be more motivated to use smartphones' security technologies, and this association was demonstrated significantly in Hungary and not in Albania.

Published in: Kadena, 2017 [44]*; Kadena 2018* [43]*; Kadena et al. 2022* [45].

Hypothesis 3: Safeguard effectiveness positively affects security motivation in smartphones.

Thesis 3: Smartphones' safeguard effectiveness positively affects users' motivation to use security technologies, and the association is stronger in Hungary than in Albania.

Published in: Kadena, Kovács, 2017 [46]*; Kadena, Ruiz 2017* [47], *Kadena, 2018* [48].

Hypothesis 4: Safeguard cost negatively affects security motivation in smartphones.

Thesis 4: The cost of safeguards regarding smartphone security negatively influences users' motivation to use security technologies in Hungary and not Albania.

Published in: Keszthelyi, Kadena, 2016 [49]*; Kadena 2017* [42]*; Kadena 2018* [50]*; Holicza, Kadena, 2018* [51].

Hypothesis 5: Self-efficacy positively affects security motivation in smartphones.

Thesis 5: Users' confidence to take a safeguard measure in smartphones contributes to better motivation in using smartphones' security technologies, which is more significant in Hungary than in Albania.

Published in: Kadena, 2018 [52]*; Kadena, 2019* [53]*; Kadena, 2020* [54].

Hypothesis 6: Users' motivation to use smartphones' security technologies positively influences their security behaviour.

Thesis 6: Users' intention to avoid threats and use smartphones' security technologies contributes to better security behaviours in Hungary but not Albania Thesis 7a: Users' impulsivity in both countries does not contribute to their motivation in using smartphones' security technologies.

Published in: Kadena, 2018 [50]*; Kadena, 2019* [55]*; Kadena, Gupi 2021* [56].

Hypothesis 7: Individual differences affect users' perceived threat and security motivations that shape their smartphone security behaviours.

Thesis 7a: Users' impulsivity in both countries does not contribute to their motivation in using smartphones' security technologies.

Thesis 7b: Users with high-risk tendencies in Hungary will feel more concerned with smartphone threats. While in Albania, there is no significant association between users' risk propensity and perceived threat.

Thesis 7c: Users' distrust tendencies contribute to a better understanding of smartphone security threats in Hungary and not Albania.

Published in: Kadena, 2017 [42]*; Holicza, Kadena, 2018* [51]*; Kadena, 2018* [57]*; Kadena, Holicza, 2018* [58]*; Kadena, 2019* [59]*; Kadena, Pokorádi, 2020* [60].

4 The Use of New Scientific Achievements

Results indicated that copping appraisal factors influenced the users' motivation and consequently their security behaviours in smartphones more than threat appraisal factors. Users' perceived threat will not always lead to better motivation in using smartphones' security technologies. This implies that more attention should be paid to increasing users' beliefs in the effectiveness of measures against smartphone threats and their confidence in performing these behaviours. Moreover, more effort should be made to reduce the costs of performing security behaviours, contributing to users' motivation to behave securely.

Translate awareness into action

Human error remains the weakest link in the security chain. Besides the antiviruses and other protective layers on computers and infrastructure, studies have shown that they do not mitigate the security threats [3], [4], [5] completely. Therefore, organizations have already recognized that users' behaviours are responsible for security flaws and may pose significant risks to information security. For instance, in the case of Albania, lastly, data leakage has been a considerable concern. Over 600.000 personal data, including salaries, leaked because of internal infiltration and not an outside cyber-attack [61]. Albanian data protection legislation should put more effort into Information and Data Protection, following the best practices of its homologs in EU countries. Human factor knowledge and user-centered design principles would be helpful for security designers to produce more practical security solutions [62].

Increasing users' awareness through training materials and sufficient resources related to smartphone threats is recommended. Materials regarding security tools can be offered and explained with ease for better access and adoption. The information provided to the users against smartphone threats is suggested to highlight the costs of taking protective behaviours. Including proper behaviours and practices in accordance with users' culture can both be perceived to be effective. Consequently, the user can feel more confident in performing securely. Moreover, providing detailed information about how to implement smartphones' security technologies would make the security technologies more adaptive to the users. This can potentially increase their motivation and performance on security.

Understanding users' behaviour in smartphone security can better serve in designing cybersecurity solutions. Understanding the factors related to users' mobile security behaviours may contribute to technologies, policies, and procedures that effectively motivate people to behave more securely. Private and public organizations should encourage users to adopt smartphone security behaviours that promote safety against threats.

Applying computational cognitive methods

Applying cognitive training methods can be helpful to improve behavioural traits and enhance users' security behaviours. Companies should know the characteristics of their employees and customers and develop strategies to help users' security uncertainties and promote security behaviours.. Leaders and decision-makers should consider planning strategies and apply them in accordance with the users' behaviours. Also, developers and manufacturers should consider factors influencing human behaviours and form unique strategies to ensure that systems have maximum security [59], [45].

Computational cognitive methods can be used to predict the behaviour of attackers or systems users' [63], [64]. For instance, social engineering attacks on conversation data like phone calls (call locations and conversations' details) can be detected by using network models [65]. Moreover, special attention should be paid to the reliance on recency and frequency of cyberattacks [66].

Multi-disciplinary research for better cybersecurity strategies

When developing strategies that promote protective behaviours, individual differences and other factors hidden in national differences can be utilized. A fundamental requirement to address cyber threats, should be considered the increase of countries' capacities. This work highlights cybersecurity needs structure, approach, and technical capacities improvements. Future systems, especially those belonging to the critical infrastructure, are suggested to follow European strategic priorities in cybersecurity [67].

Research should focus on understanding how individuals adopt and use new technology and how risk is perceived. A strong collaboration of economics, social disciplines, and technology experts is needed. Such multi-disciplinary research can serve in modeling and designing better future solutions in the digital world.

Moreover, simulation experiments (i.e., artificial intelligence) can create more awareness and a greater understanding of the unconscious and intuitive reactions to threats.

5 Conclusions

Information security involves protection and prevention, which implies users' interventions and behaviours. Hence, this work examined the role of behavioural science theories in understanding users' security intentions and behaviours in smartphones, how these theories can contribute to expanding research, and how the security risks can be reduced. This study can be of value and better serve to understand how users' smartphone security behaviours can be explained by cognitive factors and individual differences in different countries. The research has highlighted the importance of human behaviour in smartphone security. It can be considered a first step towards enhancing the understanding of two main groups: Albanian and Hungarian users.

The findings of this study make several noteworthy contributions to the TTAT original model of Liang and Xue and the original results that Carpenter et al. report in the TTAT revised model. An alternative approach was proposed by conducting a multi-group analysis to explain the threat assessment process better. Therefore, it can be it assists in understanding the different and mixed yielded results among different cultures. This work is relevant to the information security field and can be extended to the behavioural sciences. It contributes to the emerging behavioural field of cultural differences and information security sciences.

6 References

[1] N. Leavitt, “Mobile Security: Finally a Serious Problem?,” *Computer (Long. Beach. Calif).*, vol. 44, no. 6, pp. 11–14, 2011, doi: 10.1109/MC.2011.184.

[2] M. Workman, W. H. Bommer, and D. Straub, “Security lapses and the omission of information security measures: A threat control model and empirical test,” *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, 2008, doi: https://doi.org/10.1016/j.chb.2008.04.005.

[3] B.-Y. Ng, A. Kankanhalli, and Y. Xu, “Studying users’ computer security behavior: A health belief perspective,” *Decis. Support Syst.*, vol. 46, pp. 815–825, 2009.

[4] A. Alhogail, A. Mirza, and S. Bakry, “A comprehensive human factor framework for information security in organizations,” *J. Theor. Appl. Inf. Technol.*, vol. 78, pp. 201–211, Aug. 2015.

[5] A. D. Giwah, “User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory,” in *SoutheastCon 2018,* 2018, pp. 1–5, doi: 10.1109/SECON.2018.8479178.

[6] J. Shropshire, M. Warkentin, A. Johnston, and M. Schmidt, *Personality and IT security: An application of the five-factor model*, vol. 6. 2006.

[7] J. Uffen, N. Kaemmerer, and M. Breitner, “Personality Traits and Cognitive Determinants—An Empirical Investigation of the Use of Smartphone Security Measures,” *J. Inf. Secur.*, vol. 04, pp. 203–212, Jan. 2013, doi: 10.4236/jis.2013.44023.

[8] R. Crossler and F. Bélanger, “An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument,” *SIGMIS Database*, vol. 45, no. 4, pp. 51–71, Nov. 2014, doi: 10.1145/2691517.2691521.

[9] F. Belanger and R. E. Crossler, “Dealing with digital traces: Understanding protective behaviors on mobile devices,” *J. Strateg. Inf. Syst.*, vol. 28, no. 1, pp. 34–49, 2019, doi: https://doi.org/10.1016/j.jsis.2018.11.002.

[10] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, “Gender difference and employees’ cybersecurity behaviors,” *Comput. Human Behav.*, vol. 69, pp. 437–443, Apr. 2017, doi: 10.1016/j.chb.2016.12.040.

[11] R. Xu, R. M. Frey, E. Fleisch, and A. Ilic, “Understanding the impact of personality traits on mobile app adoption – Insights from a large-scale field study,” *Comput. Human Behav.*, vol. 62, pp. 244–256, 2016, doi: https://doi.org/10.1016/j.chb.2016.04.011.

[12] A. J. Burns, C. Posey, T. L. Roberts, and P. Benjamin Lowry, “Examining the relationship of organizational insiders’ psychological capital with information security threat and coping appraisals,” *Comput. Human Behav.*, vol. 68, pp. 190–209, 2017, doi: https://doi.org/10.1016/j.chb.2016.11.018.

[13] A. H. Maslow, “A theory of human motivation.,” *Psychol. Rev.*, vol. 50, no. 4, pp. 370–396, 1943, doi: 10.1037/h0054346.

[14] J. Mitzen, “Ontological Security in World Politics: State Identity and the Security Dilemma,” *Eur. J. Int. Relations*, vol. 12, no. 3, pp. 341–370, Sep. 2006, doi: 10.1177/1354066106067346.

[15] H. Liang and Y. Xue, “Avoidance of information technology threats: A theoretical perspective,” *MIS Q. Manag. Inf. Syst.*, vol. 33, no. 1, pp. 71–90, 2009, doi: 10.2307/20650279.

[16] Z. Tu, O. Turel, Y. Yuan, and N. Archer, “Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination,” *Inf. Manag.*, vol. 52, Mar. 2015, doi: 10.1016/j.im.2015.03.002.

[17] C. Posey, T. Roberts, and P. Lowry, “The impact of organizational commitment on insiders’ motivation to protect organizational information assets,” *J. Manag. Inf. Syst.*, vol. 32, pp. 179–214, Aug. 2015.

[18] A. Bandura, “Self-efficacy mechanism in human agency.,” *Am. Psychol.*, vol. 37, no. 2, pp. 122–147, 1982, doi: 10.1037/0003-066X.37.2.122.

[19] N. K. Janz and M. H. Becker, “The Health Belief Model: A Decade Later,” *Health Educ. Q.*, vol. 11, no. 1, pp. 1–47, Mar. 1984, doi: 10.1177/109019818401100101.

[20] D. Kroenke, *MIS Essentials*, 4th ed. Pearson, 2014.

[21] B. Robertson, “Technical, data, and human safeguards against security threats,” 2020. https://sites.google.com/site/bus141benrobertson/technical-data-and-human-safeguards-against-security-threats (accessed Aug. 28, 2020).

[22] A. E. de Albuquerque Junior, E. M. dos Santos, A. E. de Albuquerque Junior, and E. M. dos Santos, “ADOPTION OF INFORMATION SECURITY MEASURES IN PUBLIC RESEARCH INSTITUTES,” *J. Inf. Syst. Technol. Manag.*, vol. 12, no. 2, pp. 289–315, May 2015, doi: 10.4301/S1807-17752015000200006.

[23] I. Woon, G. Tan, and R. T. Low, *A Protection Motivation Theory Approach to Home Wireless Security*. 2005.

[24] R. Agarwal, V. Sambamurthy, and R. M. Stair, “Research Report: The Evolving Relationship Between General and Specific Computer Self-Efficacy—An Empirical Assessment,” *Inf. Syst. Res.*, vol. 11, no. 4, pp. 418–430, Aug. 2000, [Online]. Available: http://www.jstor.org/stable/23011046.

[25] D. R. Compeau and C. A. Higgins, “Computer Self-Efficacy: Development of a Measure and Initial Test,” *MIS Q.*, vol. 19, no. 2, pp. 189–211, Aug. 1995, doi: 10.2307/249688.

[26] D. Compeau, C. A. Higgins, and S. Huff, “Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study,” *MIS Q.*, vol. 23, no. 2, pp. 145–158, Aug. 1999, doi: 10.2307/249749.

[27] H. Liang and Y. Xue, “Understanding security behaviors in personal computer usage: A threat avoidance perspective,” *J. Assoc. Inf. Syst.*, vol. 11, no. 7, pp. 394–413, 2010, doi: 10.17705/1jais.00232.

[28] I. Ajzen, “The theory of planned behavior,” *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, 1991, doi: https://doi.org/10.1016/0749-5978(91)90020-T.

[29] I. Ajzen and M. Fishbein, “Understanding Attitudes and Predicting Social Behavior,” 1980.

[30] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, “User Acceptance of Information Technology: Toward a Unified View,” *MIS Q.*, vol. 27, no. 3, pp. 425–478, Aug. 2003, doi: 10.2307/30036540.

[31] D. Carpenter, D. Young, P. Barrett, and A. Mcleod, “Refining Technology Threat Avoidance Theory,” *Commun. Assoc. Inf. Syst.*, vol. 44, pp. 380–407, Jan. 2019, doi: 10.17705/1CAIS.04422.

[32] M. R. De Villiers, “Models for Interpretive Information Systems Research, Part 1: IS Research, Action Research, Grounded Theory - A Meta-Study and Examples,” in *Mora, M., Gelman, O., Steenkamp, A. L., & Raisinghani, M. (Eds.). Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems,* IGI Global, 2012, pp. 222–237.

[33] F. Waismann, *Causality and Logical Positivism*. Springer, 2011.

[34] S. A. Samani, “Steps in Research Process (Partial Least Square of Structural Equation Modeling (PLS-SEM)),” *Int. J. Soc. Sci. Bus.*, vol. 1, no. 2, pp. 55–66, Oct. 2016, Accessed: Jan. 24, 2021. [Online]. Available: www.ijssb.com.

[35] S. Brown, “Measures of Shape: Skewness and Kurtosis,” Oct. 26, 2020. https://brownmath.com/stat/shape.htm (accessed Mar. 16, 2021).

[36] E. S. Vasu and P. B. Elmore, “The Effect of Multicollinearity and the Violation of the Assumption of Normality on the Testing of Hypotheses in Regression Analysis,” Washington, D.C., Mar. 1975.

[37] W. Yoo, R. Mayberry, S. Bae, K. Singh, Q. Peter He, and J. W. Lillard, “A Study of Effects of MultiCollinearity in the Multivariable Analysis.,” *Int. J. Appl. Sci. Technol.*, vol. 4, no. 5, pp. 9–19, Oct. 2014, Accessed: Mar. 11, 2021. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/25664257.

[38] J.-M. Becker, K. Klein, and M. Wetzels, “Hierarchical Latent Variable Models in PLS-SEM: Guidelines for Using Reflective-Formative Type Models,” *Long Range Plann.*, vol. 45, no. 5, pp. 359–394, 2012, doi: https://doi.org/10.1016/j.lrp.2012.10.001.

[39] J. Hair, G. T. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 1st ed. Thousand Oaks, CA: Sage, 2014.

[40] M. Sarstedt, J. Henseler, and C. Ringle, “Multi-Group Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results,” *Adv. Int. Mark.*, vol. 22, pp. 195–218, Jan. 2011, doi: 10.1108/S1474-7979(2011)0000022012.

[41] J. Hair, M. Sarstedt, C. M. Ringle, and S. P. Gudergan, *Advanced Issues in Partial Least Squares Structural Equation Modeling (PLS-SEM)* , 1st ed. SAGE Publications, Inc, 2017.

[42] E. Kadëna, “Smartphone Security Threats,” in *Management, Enterprise and Benchmarking in the 21st Century*, Jan. 2017, pp. 141–160.

[43] E. Kadena, “Smartphone Security Awareness and Practices of Users in Albania,” *J. Aware.*, vol. 3, no. Special, pp. 14–81, 2018, doi: 10.26809/joa.2018548618.

[44] E. Kadena, “Necessity of BYOD Security Strategy,” in *LIX. Georgikon Napok. A múlt mérföldkövei és a jövő*

kihívásai: 220 éves a Georgikon, Z. B. Nagy, Ed. Keszthely, Hungary: Pannon Egyetem Georgikon Mezőgazdaságtudományi Kar, 2017, pp. 198–204.

[45] E. Kadena, S. Kocak, K. Takácsné György, and A. Keszthelyi, “FMEA in Smartphones: A Fuzzy Approach,” *MATHEMATICS*, vol. 10, no. 3, p. 513, 2022, doi: 10.3390/math10030513.

[46] E. Kadëna and T. Kovács, “The need for BYOD security strategy,” *Hadmérnök (XII)*, vol. XIII, no. 4, pp. 138–145, 2017.

[47] E. Kadëna and L. Ruiz, “Adoption of biometrics in mobile devices,” in *Proceedings of FIKUSZ Symposium for Young Researchers*, 2017, pp. 140–148.

[48] E. Kadena, “The adoption of Blockchain in Mobile Devices: Challenges and Opportunities,” in *2. International Conference on Awareness*, Canakkale: Rating Academy, 2018, pp. 421–426.

[49] A. Keszthelyi and E. Kadëna, “Misunderstanding how Passwords Work,” in *11th International Conference on Mangement, Enterprise and Benchmarking (MEB 2016)*, 2016, pp. 83–92.

[50] E. Kadena, “Lack of cybersecurity education,” in *Współczesne problemy zarządzania, obronności i bezpieczeństwa. T. 2*, Z. Tadeusz and I. Horzela, Eds. Warsaw, Poland: Akademia Sztuki Wojennej, 2018, pp. 83–90.

[51] P. Holicza and E. Kadëna, “Smart and Secure? Millennials on Mobile Devices,” *Interdiscip. Descr. Complex Syst.*, vol. 16, no. 3-A, pp. 376–383, Sep. 2018, doi: 10.7906/indecs.16.3.10.

[52] E. Kadena, “Security in Home Automation,” *BÁNKI KÖZLEMÉNYEK*, vol. 1, no. 1, pp. 5–25, 2018.

[53] E. Kadena, “Password Selecting Habits,” in *RAJNAI ZOLTÁN KIBERBIZTONSÁG – CYBERSECURITY 2.*, Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 161–175.

[54] E. Kadena, “Password Selecting Habits,” in *Eight International Scientific Web-conference of Scientists and PhD. students or candidates*, Z. Rajnai, P. Schmidt, and P. Jurik, Eds. Budapest, Hungary: Óbuda University, 2020, pp. 164–176.

[55] E. Kadena, “Blockchain integration into mobile devices,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed. Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 195–201.

[56] E. Kadena and M. Gupi, “HUMAN FACTORS IN CYBERSECURITY: RISKS AND IMPACTS,” *Secur. Sci. J.*, vol. 2, no. 2, pp. 51–64, 2021, doi: 10.37458/ssj.2.2.3.

[57] E. Kadena, “Human error and latent conditions in mobile devices. Reducing risks through FMEA,” in *III.International Rating Academy Congress on Applied Sciences*, Lviv: Rating Academy, 2018, pp. 8–13.

[58] E. Kadena and P. Holicza, “Security Issues in the Blockchain(ed) World,” in *2018 IEEE 18th International*

Symposium on Computational Intelligence and Informatics (CINTI), Nov. 2018, pp. 211–216, doi: 10.1109/CINTI.2018.8928212.

[59] E. Kadena, “Security of mobile devices in the view of Swiss Cheese Model,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed. Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 176–183.

[60] E. Kadena and L. Pokorádi, “HUMAN ERRORS IN MOBILE DEVICES,” in *European Smart, Sustainable and Safe Cities Conference 2020 : Abstract Book*, D. Tokody and Z. Nyikes, Eds. Budapest, Hungary: Óbudai Egyetem, 2020, p. 18.

[61] S. Coble, “Albania’s Prime Minister Issues Data Leak Apology - Infosecurity Magazine,” Dec. 24, 2021. https://www.infosecurity-magazine.com/news/albanias-prime-minister-issues/ (accessed Mar. 22, 2022).

[62] M. Sasse and I. Flechais, “Usable Security Why Do We Need It? How Do We Get It?,” in *Security and Usability: Designing secure systems that people can use*, Sebastopol, US: O’Reilly, 2005, pp. 13–30.

[63] V. D. Veksler, N. Buchler, B. E. Hoffman, D. N. Cassenti, C. Sample, and S. Sugrim, “Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users,” *Front. Psychol.*, vol. 9, 2018, doi: 10.3389/fpsyg.2018.00691.

[64] V. D. Veksler, N. Buchler, C. G. LaFleur, M. S. Yu, C. Lebiere, and C. Gonzalez, “Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior,” *Front. Psychol.*, vol. 11, 2020, doi: 10.3389/fpsyg.2020.01049.

[65] H. Sandouka, A. J. Cullen, and I. Mann, “Social engineering detection using neural networks,” in *2009 International Conference on CyberWorlds*, 2009, pp. 273–278.

[66] Z. Maqbool, P. Aggarwal, V. S. C. Pammi, and V. Dutt, “Cyber Security: Effects of Penalizing Defenders in Cyber-Security Games via Experimentation and Computational Modeling,” *Front. Psychol.*, vol. 11, 2020, doi: 10.3389/fpsyg.2020.00011.

[67] ENISA, “Analysis of the European R&D Priorities in Cybersecurity,” 2018.

7 Own Publications Related to the Dissertation

1. E. Kadena, S. Kocak, K. Takácsné György, and A. Keszthelyi, “FMEA in Smartphones: A Fuzzy Approach,” *MATHEMATICS*, vol. 10, no. 3, p. 513, 2022, doi: 10.3390/math10030513.
2. E. Kadena, H. P. D. Nguyen, and L. Ruiz, “Mobile Robots: An Overview of Data and Security,” in *Proceedings of the 7th International Conference on Information Systems Security and Privacy - ICISSP*, 2021, pp. 291–299.
3. E. Kadena and M. Gupi, “HUMAN FACTORS IN CYBERSECURITY: RISKS AND IMPACTS,” *Secur. Sci. J.*, vol. 2, no. 2, pp. 51–64, 2021, doi: 10.37458/ssj.2.2.3.
4. E. Kadena, “Password Selecting Habits,” in *Eight International Scientific Web-conference of Scientists and PhD. students or candidates*, Z. Rajnai, P. Schmidt, and P. Jurik, Eds. Budapest, Hungary: Óbuda University, 2020, pp. 164–176.
5. E. Kadena and L. Pokorádi, “HUMAN ERRORS IN MOBILE DEVICES,” in *European Smart, Sustainable and Safe Cities Conference 2020 : Abstract Book*, D. Tokody and Z. Nyikes, Eds. Budapest, Hungary: Óbudai Egyetem, 2020, p. 18.
6. E. Kadena, “Security of mobile devices in the view of Swiss Cheese Model,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed. Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 176–183.
7. E. Kadena, “Blockchain integration into mobile devices,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed. Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 195–201.
8. E. Kadena, “Assessing risks in mobile devices by using fmea,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed. Budapest, Hungary: Óbudai Egyetem, Biztonságtudományi Doktori iskola, 2019, pp. 184–194.
9. E. Kadena, “The adoption of Blockchain in Mobile Devices: Challenges and Opportunities,” in *2. International Conference on Awareness,* Canakkale: Rating Academy, 2018, pp. 421–426.
10. E. Kadena, “Human error and latent conditions in mobile devices. Reducing risks through FMEA,” in *III.International Rating Academy Congress on Applied Sciences*, Lviv: Rating Academy, 2018, pp. 8–13.
11. E. Kadena, “Security in Home Automation,” *BÁNKI KÖZLEMÉNYEK*, vol. 1, no. 1, pp. 5–25, 2018.

12. E. Kadena and P. Holicza, “Security Issues in the Blockchain(ed) World,” in *2018 IEEE 18th International Symposium on Computational Intelligence and Informatics (CINTI)*, Nov. 2018, pp. 211–216, doi: 10.1109/CINTI.2018.8928212.
13. E. Kaděna, “The use of smartphones in surveillance,” in *Management, Enterprise and Benchmarking in the 21st Century*, 2018, pp. 170–179.
14. E. Kadena, “Lack of cybersecurity education,” in *Współczesne problemy zarządzania, obronności i bezpieczeństwa. T. 2*, Z. Tadeusz and I. Horzela, Eds. Warsaw, Poland: Akademia Sztuki Wojennej, 2018, pp. 83–90.
15. E. Kadena, “Smartphone Security Awareness and Practices of Users in Albania,” *J. Aware.*, vol. 3, no. Special, pp. 14–81, 2018, doi: 10.26809/joa.2018548618.
16. P. Holicza and E. Kadëna, “Smart and Secure? Millennials on Mobile Devices,” *Interdiscip. Descr. Complex Syst.*, vol. 16, no. 3-A, pp. 376–383, Sep. 2018, doi: 10.7906/indecs.16.3.10.
17. E. Kadëna and L. Ruiz, “Adoption of biometrics in mobile devices,” in *Proceedings of FIKUSZ Symposium for Young Researchers*, 2017, pp. 140–148.
18. E. Kadëna and T. Kovács, “The need for BYOD security strategy,” *Hadmérnök (XII)*, vol. XIII, no. 4, pp. 138–145, 2017.
19. E. Kadëna and A. Kerti, “Security Risks of Machine-to-Machine Communications,” *HÍRVILLÁM = SIGNAL BADGE*, vol. 8, no. 1, pp. 95–115, 2017.
20. E. Kadena, “Necessity of BYOD Security Strategy,” in *LIX. Georgikon Napok. A múlt mérföldkövei és a jövő kihívásai: 220 éves a Georgikon*, Z. B. Nagy, Ed. Keszthely, Hungary: Pannon Egyetem Georgikon Mezőgazdaságtudományi Kar, 2017, pp. 198–204.
21. E. Kadëna, “Smartphone Security Threats,” in *Management, Enterprise and Benchmarking in the 21st Century*, Jan. 2017, pp. 141–160.
22. Keszthelyi and E. Kadëna, “Misunderstanding how Passwords Work,” in *11th International Conference on Mangement, Enterprise and Benchmarking (MEB 2016)*, 2016, pp. 83–92.