Serbian Journal of Management 19 (1) (2024) xxx - xxx

www.sjm06.com

Serbian Journal of Management

APPLYING ATTITUDE THEORY TO DETERMINE USER SECURITY APPROACHES

Kata Rebeka Szucs[a], Andrea Tick[b*] and Regina Zsuzsanna Reicher[c]

[a]Óbuda University, Doctoral School on Safety and Security Sciences, Népszínház u. 8., Budapest, Hungary
[b]Óbuda University, Keleti Károly Faculty of Business and Management, Tavaszmező u. 15-17., Budapest, 1084, Hungary, tick.andrea@kgk.uni-obuda.hu
[c]Budapest Business School, Faculty of Finance and Accountancy, Buzogány u. 10-12., Budapest, Hungary

(Received 01 July 2023; accepted 31 August 2023)

Abstract

Mobile phones and internet form a crucial part of modern life, which raises important questions, such as security, data protection and privacy. Countless studies examine what influences users' approaches towards security. The attitude theory gives the basic background to the present study through which the topics of cyber safety and security, data protection and privacy are examined. The three components of attitude, which served as the three pillars of the applied survey, are: (1) the cognitive component (belief and knowledge), (2) the affective component (feelings) and (3) the behavioural component (the effect of the attitude on the users' behaviour). Self-reported security knowledge and feelings about security were assessed, out of which three factors were formed using EFA. The security behaviour of each factor was examined to determine the consistency of the responses. Moreover, the three factors helped to identify three separate clusters. As a conclusion it can be stated that the theory of attitudes can help understanding user security behaviour better. Finally, future research directions are suggested.

Keywords: attitude theory, security attitude, mobile device security, information security

1. INTRODUCTION

Mobile phones and internet are a crucial part of present life. In Hungary by the fourth quarter of 2022 there were 141 mobile phone subscriptions per 100 people (KSH, 2022a), while mobile data traffic increased by nearly a third in one year (KSH, 2022b), and mobile

* *Corresponding author: Tick.Andrea@uni-obuda.hu*

DOI: 10.5937/sjm19-45280

broadband internet connection was used in 76.7% of households (KSH, 2022c). Regarding habits, 83.4% of the population used the internet several times a day or continuously and further 12% is reported to use it once a day or almost every day (KSH, 2022d). The share of internet users in the EU-27 countries (as a percentage of the population aged 16–74) was 89% in 2021 equalling the Hungarian average calculated this way (KSH, 2021). The statistics confirm that smart phone and internet usage are essential parts of our everyday lives and studies show how new challenges emerge with new technologies (Szatmáry & Szikora, 2023). Consequently, and simultaneously cyber safety and security, privacy and data protection have also grown to be a highly important aspect of the modern lifestyle (Rahim et al., 2015). Nowadays these trending topics get a lot of attention. Mobile device security can be explored from the devices' point of view (like for example in the following study where mobile hardware and software are examined (Kadena et al., 2022), and also from the users' point of view, which is the topic of this paper. Studies also examine the issue using a combined view of the above, where both the device and the human element is scrutinized (Kadena & Keszthelyi, 2022; Szucs, 2019). Despite the trends, one cannot be sure if smartphone users also feel the pressure to secure their devices and data. The present research aims to discover the factors that affect users' attitude towards cyber safety and security, and privacy, and to determine whether this is an activity users often consider in their routine.

To explore security attitude affecting factors, the logic and theory of attitude studies was used. There are several definitions, but according to the psychologist Katona, "attitudes represent our generalized viewpoints that enable us to evaluate certain situations favourably and others unfavourably" (Rekettye et al., 2016, p. 116). The three components of attitude, that served as a basis for the composition of the present survey as well, are: (1) the cognitive component (belief and knowledge), (2) the affective component (feelings) and (3) the behavioural component (the effect of the attitude on the users' behaviour). It is common for the emotional component of the attitude to influence the general attitude. In order to create harmony between cognitive and affective elements in conscious opinion formation, users adjust the respective components to the emotions even without sufficient information (Rekettye et al., 2016).

Regarding attitude it must have a subject which can either be an abstract concept such as "security", or a tangible thing; it has direction, degree and intensity as well. Although degree and intensity are indeed related, they are not the same, as for instance, a person may feel that applications are unreliable, but their conviction (attitude intensity) that they are right is not very strong. Attitude also has a structure, specifically, the structure of human attitudes is similar to a circular structure, where in the centre an individual's important values and self-image can be found (Hofmeister-Tóth, 2014). Attitudes also interact with each other and thus form a complex entity (Chan, 2008; Tsai, et al., 2022), which assumes that there must be some degree of consistency between them. Since attitudes are related to each other, there is some degree of compatibility between them, otherwise they would be in conflict with each other. In addition, attitude can be learned, however learning prevents the development and change of attitude (Lazareva et al., 2019). Attitudes are formed

on the basis of our own experiences with reality, from our friends, as well as information obtained from mass communication information and advertisements. They can come from both direct and indirect life experiences. Since attitudes can be learned, the longer they persist, the stronger they become, or at least the more resistant to change (Aydin et al., 2007). Consequently, newly formed attitudes change more easily and are less stable than old ones of the same strength (Ashenden, 2018).

Considering the relationship between the attitude components, it is the authors' assumption that the third factor (behaviour that aims security) is the result of the first two factors (security knowledge and users' feelings about the topic). Therefore, if users consider security an important topic, have any idea about security, and are aware of the threats and protection methods, their behaviour aiming to secure their data and devices will be more prevalent.

There are countless studies that support or explore similar theories in different methods as well. For example, a study from Behardien and Brown suggests that smart phone user security behaviour is influenced by security awareness, users' IT sophistication and their trust in society in general (Behardien & Brown, 2022). A study, published by Thompson, McGill and Wang, examines the determinants of security behaviour (Thompson et al., 2017). A study by Tick et al. explores how attitudes to cyber risks and security behaviour is changed during the pandemic in different countries (Tick et al., 2021) In another study, from Harris, Brookshire and Chin, the motivations behind installing an application are explored with a model based on perceived risk, trust, perceived benefit, and intent to install (Harris et al., 2016). Although the categories that are mentioned in the above and other studies are similar, in general, attitude as a concept is not cited in them. To create the survey for this paper, however, theories used by other authors with similar topics were also taken into consideration, mapped to the theory of attitude.

2. RESEARCH QUESTIONS AND METHODOLOGY

Researchers are continually trying to explore how users' attitudes towards security can be determined and what are the components that affect their security attitudes. This paper aims to answer the following research questions.

1. How can the concept of attitude be applied to the subject of security?
2. Can the participants be grouped into clusters based on their security knowledge and feelings about security?
3. How the above group affiliation affects behaviour aiming security?

The basis of the study is the assumption of the relationship between the components of security attitude. The logic is that the security knowledge of users and their feelings about security result in their behaviour aiming security. Considering the cognitive and affective components, four types of user groups are expected that can be described in a matrix structure. The rows of the theoretical matrix are whether users are knowledgeable of security (the cognitive component), and the columns are whether users care about security (the affective component). In summary the four expected groups are given below.

- Users who care and know about security,

- Users who care about security but do not know too much about it,
- Users who do not care about security but know about it,
- Users who do not care and do not know about security either.

Based on the group affiliation, the security behavioural component will also be assessed, examining the relationship of the three attitude components. Using this logic can help to understand users' security attitude better which might be useful for users, application providers and regulators as well.

The above is assessed using a quantitative method, namely a questionnaire. A survey was created and then the authors of this paper used an online service to run it online with the help of Ipsos Instant Research Service to make sure the sample is close to being representative to the Hungarian population proportions considering gender, age, region, and size of settlement. (It is important to highlight that the authors did not use the help of the mentioned service for the creation of the survey.)

The questionnaire consists of two main parts. First, different aspects of security are examined, to fit the first two components of the attitude model, including control, knowledge, ability, mindfulness, energy investment, evaluation of the issue of security, perceived risk and trust. This was queried with metric scale questions in order to create factors and clusters. As a type of validation, some of the questions were used from various security related studies as baseline that fit into the attitude model and its components, however the word 'attitude' is not mentioned in these models, different ones are implemented (Balapour et al., 2020; Thompson et al., 2017; Harris et al., 2016).

The aim of the second part of the survey is to confirm the behavioural component of attitudes of the respondents. There are questions regarding security measures taken by the respondent (which are based on our previous studies (Szucs, 2019)). In addition, two more types of multiple-choice questions were included: one that queries the motivation behind approving excessive access permissions upon app installation, the other asks about the important factors when choosing an app. Both latter include security as an aspect as well, but they have other options too, such as functionality or aesthetic of the applications. The results were analysed with the SPSS software (version 29 – free trial version). A filter question (regarding mobile app use) was not included deliberately, as every user has an opinion, regardless of their internet and application usage habits (however, as the survey was filled online, and the sample is representative to the Hungarian population, probably they have some kind of experience already).

3. RESULTS

3.1. Demographic profile

After the survey was run, 525 replies were gathered. The respondents are between the age of 18 and 65 (working age) and their average age is 43.5 years (median is 44 years). Around half of them are female (48%) and the other half are male (52%), which is similar to the Hungarian population proportion (KSH, 2022e). Around third of them, 35% of them live either in Budapest (the capital city) or in country seats, further 33% live in other, smaller cities and the remaining 32% are from villages (also similar to the population of Hungary (KSH, 2022f)). Less than half of them, 42% of them

have college, university diploma or postgraduate training and further 34% have graduated from high school. One fifth of them, that is 20% of the respondents have qualification or occupation that is related to the IT field.

3.2. Factors related to the cognitive and affective components of attitude

The investigation was started with an Exploratory Factor Analysis (EFA) using principal component analysis (PC) for the 15 scale questions which contained questions about the first two attitude factors, namely self-reported security knowledge and users' feelings about the topic. The Principal Component Analysis extraction method was applied with Promax rotation with Kaiser Normalization and the rotation converged in 6 iterations. The EFA proved to be valid since the KMO (Kaiser-Mayer-Olkin Measure of Sampling Adequacy) equalled 0.888, according to which the group of variables used is suitable for factor analysis. The result of the Bartlett test (p=0.000) also supports the usage of EFA with the pre-set parameters (meaning that there is a correlation between the variables). The Communality table listed values greater than 0.5 for all the questions, which implies that each and every question can be included in the model. Therefore, three factors were created. The total variance summed up to 67.32%, that is, the extracted three principal components explain 67.32% of the variances in the original variables.

The question "It is very important for me to be aware of the use of my personal data" showed cross-factor loading, that is its factor weight gave a relatively high value for both components (0.544 for the cognitive and 0.474 for the affective component), the analysis was run again without this question. Thus, when run on the 14 scale questions, the outcomes are KMO= 0.873, and Bartlett's test sig is 0.000. The EFA still identified three factors explaining 67.241% of the variances in the original variables. The same parameters were given i.e. Extraction Method: Principal Component Analysis, Rotation Method: Promax with Kaiser Normalization and Rotation converged in 5 iterations. The results for the second run and the factor weights can be seen in Table 1.

In summary, three factors were identified from the selected 14 questions.

1. *Security awareness, confidence in control:* this factor points out whether the user feels that they know how to protect their data; if they feel they are in control and whether they know what to do in case of a security incident. This can be aligned with the concept of self-reported security knowledge if attitude theory is considered.
2. *Perceived risk*: this factor shows whether the users are worried about security and the protection of their data. Considering the attitude components, this could be the affective one.
3. *Perception of the subject of security*: this factor shows whether users think security and personal data protection is overrated or an important topic and whether it takes too much effort to secure and protect their data. Regarding the approach of attitude, this could also be considered part of the affective component, but from a different angle than the previous point.

To verify the internal consistency and internal reliability, further calculations were carried out. The value of Cronbach's alpha increases in parallel with the degree of correlation between the data. That is why the coefficients are also called internal consistency or the internal reliability of the

test (Münnich et al., 2006). Cronbach's Alpha for the first group equalled 0.91, it was 0.79 for the second group of questions, and it totalled 0.65 for the third factor, which signals that these questions stand together as well.

After confirmation that the above identified factors can be aligned with the theory of attitude, the users were divided into groups based on the three recognised factors.

3.3. Clustering – forming groups based on the identified factors

After the factors were found, user groups are formed with the help of clustering based on their answers about the different factors. Ward's method (with squared Euclidean distance) of the hierarchical clustering methods was used to create clusters on the three factors created earlier. The dendrogram excerpt below, in figure 1, illustrates how observation units are merged. In order to make the last steps of the merge more visible, the height of the table was significantly reduced, making its essence clearer.

The results of the agglomeration schedule were also examined, in which the last six values of the coefficients were plotted with a line diagram, so that the "elbow criterion" could also be used. (This option was rejected based on the representation in figure 2 below, where an "elbow" was not observed, further analysis was conducted from the data shown on the dendrogram.)

Considering the grouping process used by the Ward's method, the versions with different number of clusters were calculated at the same time within the same analysis

Table 1. Factor analysis, second attempt

		Component		
		1	**2**	**3**
1	I can use technology well to protect the security of my personal data.	0.913		
2	I have sufficient ability to protect my personal information from theft/disclosure.	0.908		
3	Taking the necessary security measures on mobile devices is completely under my control.	0.840		
4	Due to the privacy statements, I believe that my personal data is treated confidentially by the apps.	0.757		
5	If I become a victim of a security incident (for example, my email account is hacked), I know what to do.	0.743		
6	Before using mobile apps, I consciously set security settings (for example, what an app can access).	0.743		
7	I trust the security of my transactions with mobile applications.	0.643		
8	I am concerned that mobile applications may use my personal data collected about me without my permission.		0.877	
9	In general, it would be risky to provide my personal information to a mobile application.		0.817	
10	It is very important to me to be aware of the use of my health information.		0.625	
11	It would be a serious problem for me if someone had access to confidential information on my phone without my permission or knowledge.		0.617	
12	The issue of security and data protection is overrated.			0.833
13	It is important to me that if the interest of the community so requires, I may even relinquish my control over my personal data (for example during COVID).			0.674
14	It takes too much invested energy to take security measures to protect my mobile device.			0.674

Source: edited by authors

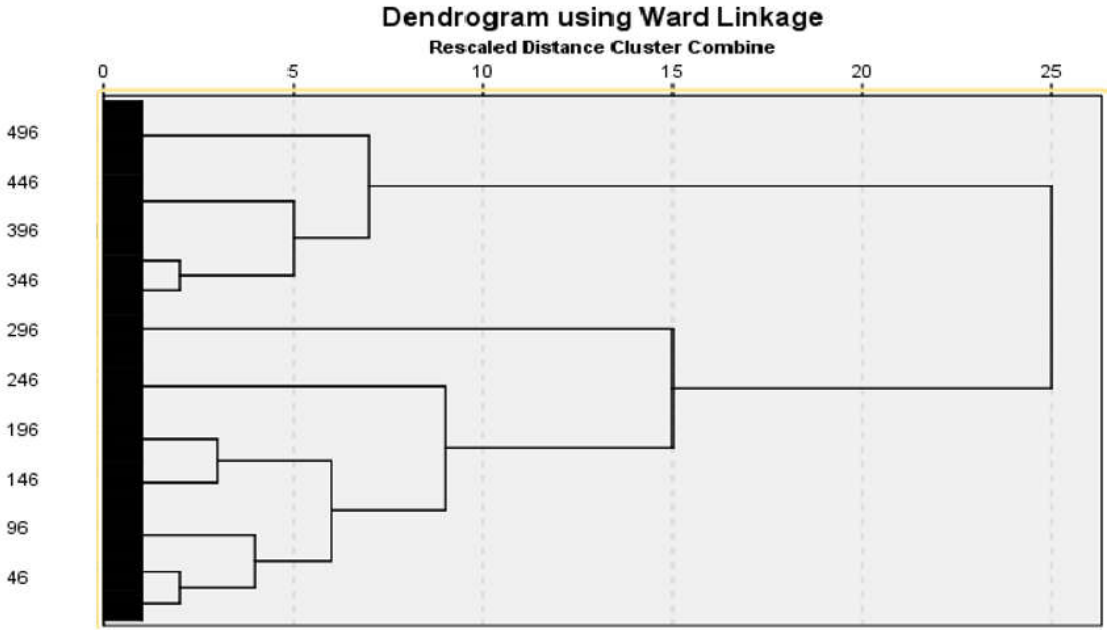

Figure 1. Screenshot from SPSS, dendrogram using Ward Linkage, rescaled

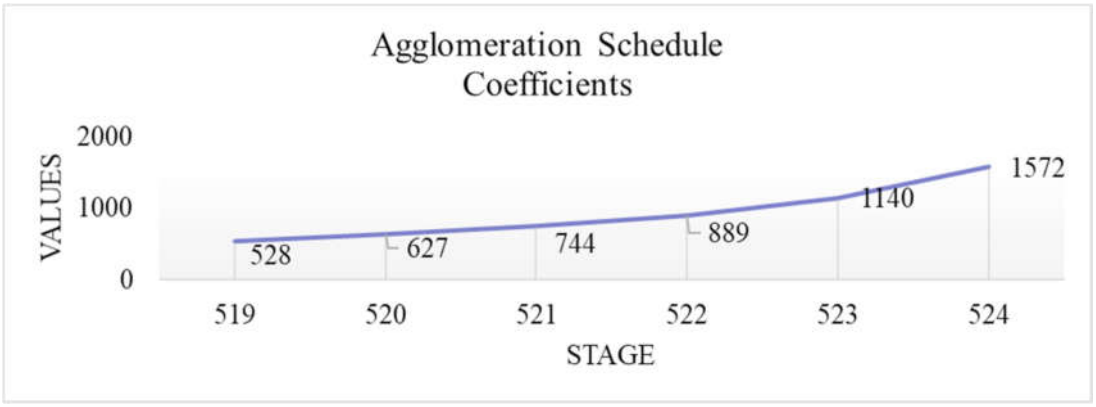

Figure 2. Agglomeration schedule coefficients
Source: edited by authors

(see Figure 1). After reviewing the dendrogram, the cluster numbers 2 and 3 and 4 were saved as new variables and further analyses were carried out with the help of variance analysis to examine the characteristic of each cluster in order to determine the appropriate number of clusters. The two-cluster solution was rejected by the authors because it does not give a detailed enough analysis of the sample and there were no striking differences between the groups.

In the case of the three–cluster solution, the attitude of the respondents to certain factors is divided as described below. Table 2 shows the average and standard deviation per factor characteristic of the clusters, as well as the number of cluster elements.

Table 2. Three-cluster solution – The average and standard deviation per factor characteristic of clusters, and the number of cluster elements

Ward Method		Security awareness	Perceived risk	Security perception
1	Mean	0.31	0.54	-0.43
	N	256	256	256
	SD	0.86	0.70	0.90
2	Mean	-0.60	-0.89	0.07
	N	217	217	217
	SD	0.89	0.63	0.64
3	Mean	0.99	1.07	1.82
	N	52	52	52
	SD	0.46	0.33	0.39
Total	Mean	0.00	0.00	0.00
	N	525	525	525
	SD	1	1	1

Source: edited by authors

Based on these results the three clusters are:

1. *Aware*: The members of the first cluster (N=256, group number 1 in Table 2) claimed to have a degree of security awareness, and they also feel and perceive security risk and they do not perceive security as an overrated topic. Consequently, this group will be called the ‘aware’ ones, since they have a high level of awareness, but they are also quite confident that they know what to do to be safe.

2. *Calm*: The members of this cluster (N=217, group number 2 in Table 2) stated that they do not consider themselves to be security conscious and they have the lowest level of perceived risk compared to the other groups. They also seem to consider security a bit overvalued, this is why they are named the ‘calm’ ones.

3. *Expert*: The third group is a strange one, because all three components got the highest rates from this group, which means that they consider themselves to be very conscious of security, their perception of risk is high and at the same time they are not concerned with security in their day-to-day life at all. This suggests a kind of self-confidence that suggests to label them the group of ‘experts’. Fifty-two respondents were clustered into this group (group number 3 in Table 2).

In the case of the four–cluster solution, which also followed the same methodology (Ward's method with squared Euclidean distance based on the factors from above), compared to the previous solution, a fourth group is identified which actually divides the first group of the three–cluster solution, the 'aware’ ones, into two separate groups numbered 1 and additionally 4 as listed in Table 3, consisting of 203 and 53 respondents, respectively (see also Figure 1).

The first group is similar to the first group of the three–cluster solution, to the ‘aware’ ones, where the level of perceived risk is high among the group members, and they admitted to have a relatively high degree of perceived security risk in their life, furthermore, in line with this they feel that security overall is somewhat important. The fourth group, on the other hand, in this division claims to have a high level of security awareness (highest of all groups),

Table 3. Four-cluster solution – The average and standard deviation per factor characteristic of clusters, and the number of cluster elements

Ward Method		Security awareness	Perceived risk	Security perception
1	Mean	0.07	0.77	-0.24
	N	203	203	203
	Std. Deviation	0.76	0.57	0.89
2	Mean	-0.60	-0.89	0.07
	N	217	217	217
	Std. Deviation	0.89	0.63	0.64
3	Mean	0.99	1.07	1.82
	N	52	52	52
	Std. Deviation	0.46	0.33	0.39
4	Mean	1.25	-0.33	-1.17
	N	53	53	53
	Std. Deviation	0.47	0.39	0.5
Total	Mean	0.00	0.00	0.00
	N	525	525	525
	Std. Deviation	1	1	1

Source: edited by authors

which helps them to feel a lower level of risk, and, at the same time, they think that the topic of security is overall an important aspect of their life. This group could be called the 'confident' ones. This means that the only observable difference between the 'aware' and 'confident' groups is their perception of risk.

Considering the size of the additional, fourth group (N=53) and that the four–cluster solution does not add a very different group compared to the three–cluster solution, the three–cluster version was selected and kept for further analysis. It is important to note that although it would be ideal not to have groups with only 52 members ('experts'), that group is left in the clustering because in every version that was processed, these 52 respondents stood together, which implies that they are so special and have so unique opinions about the questions compared to other groups that it is worth keeping them separately.

In summary, based on the above results, the three-cluster solution was chosen to continue the analysis.

4. DISCUSSION – ANALYSING THE CLUSTERS BASED ON THEIR BEHAVIOUR AIMING SECURITY

In the following section the three clusters are going to be examined further to understand them and their attitudes better. The questions selected for the factor and cluster analyses included the first two components of the attitude logic: the self-reported security knowledge and respondents' feelings about the topic. To connect the results to the third component, namely to behaviour aiming security, the different clusters have also been examined regarding their actions to protect their data. In the survey three types of questions were included for behaviour, as explained earlier.

In the second part of the questionnaire, in the first question, fifteen potential measures

Table 4. Security measures taken by each cluster, shown as calculated percentage of row totals

	Aware (%) (N=256)	**Calm (%)** (N=217)	**Experts (%)** (N=52)
I know the regulations and my rights related to personal data management. (e.g. GDPR)	41.41	32.72	40.38
I read the privacy policies of apps.	45.31	33.18	48.08
I carefully review the proposed cookie settings before accepting them.	36.72	23.04	17.31
I only download applications from the official application store. (For example Play Store or App Store)	75.78	64.06	42.31
I regularly review applications' permission requests. (For example, it checks which applications can use your location data and photos.)	42.19	28.57	15.38
I update my applications regularly.	54.69	44.24	32.69
I use antivirus.	60.55	48.39	38.46
I follow the news about Internet scams.	35.16	21.20	11.54
I backup my data. (For example, documents, photos)	45.70	30.88	9.62
Verify the authenticity of the website or application before issuing personal data.	46.88	30.88	11.54
I would recognize a phishing email based on its characteristics.	44.14	26.27	13.46
I choose complex passwords.	49.61	32.72	25.00
I choose a password that cannot be linked to me personally.	41.02	28.11	21.15
I update my passwords regularly.	23.83	17.51	9.62
I use biometric identification. (For example, fingerprint or face recognition)	37.89	31.34	7.69

Source: edited by authors

were listed that can elevate the *level of security* and it was found that on average the first cluster applied 7, the second one applied 5 and the third one applied 3 of them. Table 4 shows what percentage of each cluster selected the respective type of behaviour (percentage of cluster– or row– total).

It is visible that the first two group indeed are consistent of what they stated in the first half of the survey. The group of *aware* ones, in most cases selected the methods in the largest proportion compared to the size of their cluster, and the group of *calm* ones are indeed selected less of these. Interestingly, the third group, identified as '*experts*', because they declared themselves as highly security aware people who perceive a high security risk, have selected the least of these measures. This can be interpreted as a confirmation that as per their perception of security, this is not that important for them. Although this does not rule out the possibility that these people are really experts, it is certainly interesting that they do not use too many protective measures (of our list at least). A possible explanation of this phenomenon is that they see but also accept the risks of using mobile apps, therefore they are not concerned too much about taking measures.

It is visible that the top three measures are the same for the clusters '*Aware*' and '*Calm*', which include downloading apps only from reliable sources, using antivirus and installing application updates regularly. For the '*Expert*' cluster, only the official app stores are mentioned in the top three measures from the previous selection, the other two of their top three measures are reading the terms of applications and

Table 5. Possible reasons for accepting the motivation behind approving excessive access permissions upon app installation per cluster, shown as calculated percentage of row totals

If an application requests too many access permissions after installation, I approve them if:	**Aware (%)** (N=256)	**Calm (%)** (N=217)	**Experts (%)** (N=52)
I trust the app store from which I download the app.	55.08	54.84	38.46
I have not experienced any problems due to a similar case before.	36.33	35.02	38.46
I do not understand why you ask.	11.72	12.90	21.15
they take too long to read.	7.81	12.90	13.46
I feel that these are legitimate requests.	33.20	25.81	13.46
I would really like to use the features provided by the application.	17.58	17.05	13.46

Source: edited by authors

knowing their data protection rights (such as knowing GDPR). This may suggest that cluster 1 and 2 may be more reliant on technology provided security and that cluster 3 may trust themselves more when it comes to security.

The next part of the questionnaire explored the *possible motivation behind* approving excessive access permissions upon app installation. The question 'if an application asks for too many access permissions after installation, I will approve them if...' used the conditional mode, and participants could select statements that applied to them.

As Table 5 shows, the first and second cluster agree on their top three choices, which are trust in official app stores, lack of previous bad experience, and they also agree to the permission requests of apps if they think these are reasonable requests and make sense.

On the other hand, the third choice of third cluster is that they approve these permission requests even if they do not understand what they are asked for. This could suggest that they do not care about the topic of security and they agree to whatever is suggested by the service/app providers. After these two sections it is visible that behaviour–wise the first and second clusters are not too different. Upon creating the clusters, the first group seemed to be almost the opposite of the second group considering their degree of security awareness and perception of risk and security, so it is quite conspicuous that at eventually they think alike when it comes to security behaviour. It is important to note that since the whole questionnaire was about security and its aspect, respondents might have felt that they have to admit being concerned with security more than they actually are, which might have led to other aspects, such as the actual function of an app, being reported as less significant for them. This concern is supported by another question which queries the reasons behind selecting an app. For lack of space, not all of the options will be analysed for this question. The available response options were good reviews, place among the search results, star rating, number of downloads, scientific research the app is based on, aesthetics, security, reputation, motivation it can raise, joy it can cause, recommendation, availability in Hungarian, personal data handling. Overall, 74% of all respondents reported that security is an important aspect when selecting an application, but this is not necessarily reflected in their behaviour, as shown above. The other more widely chosen responses included star ratings and reviews of the applications. This can also be caused by the

aforementioned need to create harmony between the elements of one's attitude.

As a limitation of this study, it is important to mention that these questions assess the average regular behaviour of users that they report about themselves, actual behaviour was not assessed in this questionnaire, to avoid being too specific about the usage of one particular application, reducing the possible sample size. In the future, however, this could be a potential continuation of the logic of this study.

5. CONCLUSIONS

In summary, the research question posed, whether the theory of attitude can be applied to user security, is justified. It makes sense to examine all three aspects, namely security related knowledge, feelings about security and actual security behaviour of a user, and, at the same time, to understand them better. As a result, self-reported security knowledge and feelings about security were assessed, and three factors were identified. Considering these factors, three clusters of the respondents were created, which can be considered as an answer to the second research question. After that, the third research question was also examined. The security behaviour of each factor was investigated to determine the consistency of answers. Table 6 summarizes what was concluded in the previous chapters, showing the final security attitude of each group.

The plus sign means that the participants in the particular group responded the factor related questions positively, and the minus sign means the opposite. For the Experts, since they perceive a higher degree of security risk but they feel that security is not an important topic, they got a mixed sign of plus and minus. Regarding the behaviour column, the signs were determined in comparison to the other groups. Since the first two groups' replies were quite similar, they got the positive signs, and since the rates were lowest for the third group they got the minus sign.

Table 6. Summary of the elements of attitude for each group (basis: relative comparison to each other)

	Knowledge	Feeling	Behaviour
Aware	+	+	+
Calm	–	–	+
Expert	+	+/–	+

Source: edited by authors

In summary the group of 'aware' users showed that they have a high security awareness which is also visible in their security behaviour. The 'calm' ones seem to show a lower level of security awareness but their behaviour aiming security is also observable. The group of 'experts' have the highest level of security while thinking that security overall is an overrated issue, however their behaviour aiming security is also evident.

The initial assumption of forming four groups based on the cognitive and affective components of the attitude was partly successful. The groups that were created can fit three of the four expected groups. Namely the 'aware' ones are the users who care and know about security, the 'calm' ones are users who do not care and do not know about security either, and the 'expert' ones are users who do not care about security but know about it. The fourth group would have been the group of users who care about security but do not know too much about it, but identification of this group based on the survey was not possible with more clusters either.

Taking the group affiliation into account, practical advice can be formulated either for app developers or, for example, for employers. Depending on which factor has a negative sign, the more critical areas that should be focused on can be identified, if more specific questions about certain situations or systems were included.

In future studies it is possible to analyse this data further to examine other aspects of the concept of attitude such as prior experience (with security incidents for example). Further possibilities also include examining the actual behaviour of the users (not only their self-confessed behaviour), or broadening the topics of questionnaire, so they do not influence the respondents to consider security as their primary concern.

References

Ashenden, D. (2018). In their own words: employee attitudes towards information security. Information and Computer Security, 26 (3), 327-337.

Aydin, K., Say, A. T., Ustaahmetoglu, E., & Yamamoto, G. T. (2007). Attitudes of Potential Consumers toward Country-of-Origin and Auto Brand Images. Serbian Journal of Management, 2 (2), 205 - 216.

Balapour, A., Nikkhah, R. H., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. International Journal of Information Management, 52, 102063.

Behardien, R., & Brown, I. (2022). Factors Influencing Smartphone End-User Security Behaviour – The Case of Young Adults in South Africa. 2022 IST-Africa Conference (IST-Africa), (pp. 1-10). Retrieved from https://ieeexplore.ieee.org/document/9845602

Chan, J. K. (2008). Understanding the Tourists' Attitudes toward Participating Nature-Based Tourism. Proceedings for Euro-Asia conference on environment and corporate social responsibility: tourism and management session, 156-168. Retrieved from https://www.webofscience.com/wos/woscc/full-record/WOS:000263364600018

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & Security, 77, 226-261.

Harris, M. A., Brookshire, R., & Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. International Journal of Information Management, 36 (3), 441-450.

Hofmeister-Tóth, Á. (2014). The Fundamentals of Consumer behavior. Budapest, Hungary: Akadémiai Kiadó (AK), (in Hungarian)

Kadena, E., & Keszthelyi, A. (2022). Identifying Failures in Mobile Devices. Interdisciplinary Description of Complex Systems, 20 (3), 222-229.

Kadena, E., Koçak, S., Takács-György, K., & Keszthelyi, A. (2022). FMEA in Smartphones: A Fuzzy Approach. MATHEMATICS, 10(3), 513.

KSH. (2021). 12.1.3.4. Internet users [as a percentage of the population aged 16-74]. Budapest, Hungary: KSH (Hungarian Central Statistical Office). Retrieved from https://www.ksh.hu/stadat_files/ikt/hu/ikt0029.html. (in Hungarian)

KSH. (2022a). 12.1.1.1. Main indicators of information and communication. Budapest, Hungary: KSH (Hungarian Central Statistical Office). Retrieved from

ПРИМЕНА ТЕОРИЈЕ СТАВОВА ЗА ОДРЕЂИВАЊЕ ПРИСТУПА БЕЗБЕДНОСТИ КОРИСНИКА

Kata Rebeka Szucs, Andrea Tick, Regina Zsuzsanna Reicher

Извод

Мобилни телефони и интернет представљају битан део модерног живота, што поставља важна питања, као што су безбедност, заштита података и приватност. Бескрајна истраживања испитују шта утиче на приступе корисника безбедности. Теорија става даје основу за ово истраживање кроз које се испитују теме сајбер безбедности и сигурности, заштите података и приватности. Три компоненте става, које служе као три стуба примењеног истраживања, су: (1) когнитивна компонента (веровање и знање), (2) афективна компонента (осећања) и (3) понашајна компонента (утицај става на понашање корисника). Самопријављено знање о безбедности и осећања о безбедности су процењена, из чега су формирани три фактора користећи ЕФА. Безбедносно понашање сваког фактора испитано је да се утврди конзистентност одговора. Поред тога, три фактора помогла су у идентификацији три посебне групе. Као закључак може се рећи да теорија ставова може помоћи да се боље разуме понашање корисника у вези са безбедношћу. Напослетку, предложени су смерови за будућа истраживања.

Кључне речи: теорија ставова, став о безбедности, сигурност мобилних уређаја, информатичка безбедност

https://www.ksh.hu/stadat_files/ikt/hu/ikt0001.html. (in Hungarian)

KSH. (2022b). Faster internet with a stable wireless net data processing form - Internet usage, 2022. Quarter II. Budapest, Hungary: KSH (Hungarian Central Statistical Office). Retrieved from https://www.ksh.hu/infografika/2022/internet_infografika_20222.pdf. (in Hungarian)

KSH. (2022c). 12.1.1.14. Percentage of households connected to the internet. Budapest, Hungary: KSH (Hungarian Central Statistical Office). Retrieved from https://www.ksh.hu/stadat_files/ikt/hu/ikt0016.html. (in Hungarian)

KSH. (2022d). 12.1.1.16. Frequency distribution of internet use. Budapest, Hungary: KSH (Hungarian Central Statistical Office). Retrieved from https://www.ksh.hu/stadat_files/ikt/hu/ikt0018.html. (In Hungarian)

KSH. (2022e). 22.1.1.2. Number and average age of the population by sex. Budapest, Hungary: KSH (Hungarian Central Statistical Office). Retrieved from https://www.ksh.hu/stadat_files/nep/hu/nep0002.html. (in Hungarian)

KSH. (2022f). 22.1.2.1. Population by sex, county and region, 1 January. Budapest, Hungary: KSH (Hungarian Central Statistical Office). Retrieved from https://www.ksh.hu/stadat_files/nep/hu/nep0034.html. (in Hungarian)

Lazareva, E., Zakharova, A., Nikolaev, E., & Emelianova, M. (2019). Professional culture and attitude to personality security in future specialists. Professional culture of the specialists of the future- Book

SeriesEuropean Proceedings of Social and Behavioural Sciences, 73, 785-793.

Münnich, Á., Nagy , Á., & Abari , K. (2006). Multivariate statistics for psychology students. Debrecen, Hungary: Bölcsész Konzorcium. Retrieved from http://gepeskonyv.btk.elte.hu/adatok/Pszichologia/8M%FCnnich/pages/p_2_9.xml. (in Hungarian)

Rahim, N., Hamid, S., Mat Kiah, M., Shamshirband, S., & Furnell , S. (2015). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44, 606-622.

Rekettye , G., Tóth , T., & Malota , E. (2016). International Marketing - Online version. Budapest, Hungary: Akadémiai Publisher. Retrieved from https://mersz.hu/hivatkozas/dj76nm_116. (in Hungarian)

Szatmáry, R., & Szikora, P. (2023). Factors influencing technostress. In A. Szakál (Ed.), 2023 IEEE 21st World Symposium on Applied Machine Intelligence and Informatics (SAMI) (pp. 299-306). Herlany,: Slovakia. doi:10.1109/SAMI58000.2023.10044527

Szucs, K. (2019). Mobile security basics to improve personal and corporate safety. National security review : periodical of the military national security service, (2), 56-72.

Thompson, N., McGill, T., & Wang, X. (2017). “Security begins at home”: Determinants of home computer and mobile device security behavior. Computers & Security, 70, 376-391.

Tick, A., Cranfield, D. J., Venter, I. M., Renaud, K. V., & Blignaut, R. J. (2021). Comparing Three Countries’ Higher Education Students’ Cyber Related Perceptions and Behaviours during COVID-19. Electronics , 10 (22), 2865.

Tsai, C.-Y., Shih, W.-L., Hsieh, F.-P., Chen , Y.-A., Lin, C.-L., & Wu, H.-J. (2022). Using the ARCS model to improve undergraduates’ perceived information security protection motivation and behavior. Computers & Education, 181. 104449

APPENDIX

List of questions in our survey

Demographic questions

- Age
- Gender
- Region
- Size of settlement
- Education

Please rate the following statements on a scale of 1 to 10. (1= I do not agree at all, 10= I completely agree)

- I can make use of technology well to protect the security of my personal data.
- I have sufficient ability to protect my personal information from theft/disclosure.
- Taking the necessary security measures on mobile devices is completely under my control.
- Due to the privacy statements, I believe that my personal data is treated confidentially by the apps.
- If I become a victim of a security incident (for example, my email account is hacked), I know what to do.
- Before using mobile apps, I consciously adjust security settings (for example, what an app can access).
- I trust the security of my transactions with mobile applications.
- It is very important for me to be aware of the use of my personal data.
- I am concerned that mobile applications may use my personal data collected about me without my permission.
- In general, it would be risky to share my personal information in a mobile application.
- It is very important to me to be aware of the use of my health information.
- It would be a serious problem for me if someone had access to confidential information on my phone without my permission or knowledge.
- The issue of security and data protection is overrated.
- It is important to me that if the interest of the community so requires, I may even relinquish my control over my personal data (for example during COVID).
- It takes too much invested energy to take security measures to protect my mobile device.

Please indicate which of the following security measures you generally use.

- I know the regulations and my rights related to personal data management. (For example GDPR)
- I read the privacy policies of apps.
- I carefully review the proposed cookie settings before accepting them.
- I only download applications from the official application store. (For example Play Store or App Store)
- I regularly review applications' permission requests. (For example, it checks which applications can use your location data and photos.)
- I update my applications regularly.
- I use antivirus.
- I follow the news about internet scams.
- I backup my data. (For example, documents, photos)
- Verify the authenticity of the website or application before issuing personal data.
- I would recognize a phishing email based on its characteristics.
- I choose complex passwords.
- I choose a password that cannot be linked to me personally.
- I update my passwords regularly.
- I use biometric identification. (For example, fingerprint or face recognition)

If an application requests too many access permissions after installation, I approve them if:

- I trust the app store from which I download the app.
- I have not experienced any problems due to a similar case before.
- I do not understand why you ask.
- they take too long to read.
- I feel that these are legitimate requests.
- I would really like to use the features provided by the application.

When choosing an application, it is important to me that the app:

- good reviews
- place among the search results
- star rating, number of downloads
- scientific research the app is based on
- aesthetics
- security
- reputation
- motivation it can raise
- joy it can cause
- recommendation
- availability in Hungarian
- personal data handling