2024

It Is Not Only About Having Good Attitudes: Factor Exploration of the Attitudes Toward Security Recommendations

Miguel A. Toro-Jarrin
Yachay Tech

Pilar Pazos
Old Dominion University

Miguel A. Padilla
Old Dominion University

Original Publication Citation

Toro-Jarrin, M. A., Pazos, P., & Padilla, M. A. (2024). It is not only about having good attitudes: Factor exploration of the attitudes toward security recommendations. *Journal of Cybersecurity*, *10*(1), 1-10, Article tyae011. https://doi.org/10.1093/cybsec/tyae011

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2024, tyae011
https://doi.org/10.1093/cybsec/tyae011

Research Paper

It is not only about having good attitudes: factor exploration of the attitudes toward security recommendations

Miguel A. Toro-Jarrin [1,*], Pilar Pazos[2], Miguel A. Padilla[3]

[1]Agro-industrial Sciences Department, Yachay Tech, Hacienda San Jose, Urcuqui, 100115, Ecuador
[2]Engineering Management Department, Old Dominion University, Norfolk, VA 23529, United States
[3]Department of Psychology, Old Dominion University, Norfolk, VA 23529, United States

*Corresponding author. Agro-industrial Science Department, Yachay Tech, Hacienda San Jose, Urcuqui, 100115, Ecuador.
E-mail: mtoro@yachaytech.edu.ec, matoro81@hotmail.com

Received 31 August 2023; revised 24 May 2024; accepted 5 June 2024

Abstract

Numerous factors determine information security-related actions (IS-actions) in the workplace. Attitudes toward following security rules and recommendations and attitudes toward specific IS actions determine intentions associated with those actions. IS research has examined the role of the instrumental aspect of attitudes. However, authors argue that attitudes toward a behavioral object are a multidimensional construct. We examined the dimensionality of attitudes toward security recommendations, hypothesized its multidimensional nature, and developed a new scale [attitudes toward security recommendations (ASR scale)]. The results indicated the multidimensional nature of attitudes toward security recommendations supporting our hypothesis. The results revealed two dimensions corresponding to the perceived legitimacy and effectiveness of security recommendations and its perceived rigor. The new ASR scale showed good psychometric properties. This work contributes to the IS research at suggesting that attitudes are a multidimensional construct in the IS context. These findings imply that the employee's evaluation of information security policy can be examined considering their instrumentality (security recommendations are important) and rigor (security recommendations are strict). Different effects of the dimensions of attitudes over IS-action suggest different interventions. Additionally, this study offers the ASR scale as a new instrument to capture employees' evaluation of security recommendations.

Keywords: attitudes toward security recommendations; multidimensional attitudes; scale development; ASR scale

Introduction

Information technology enhances efficiency and performance but also brings new risks. Simple actions such as clicking on an email attachment or responding to a phishing email can compromise an organization's information systems and overall performance. Organizations formulate and communicate recommendations aligned with their information security policy, but employees' lapses relative to those recommendations are prevalent. Several factors at different levels (i.e. individual, group, organizational, and social) influence employee's information security-related action (IS-actions). Among these factors are employees' attitudes toward those actions and attitudes toward following information security policy. Attitudes toward IS-actions are positively associated with the intention to act [1, 2], and attitudes toward following information security policy are precursors of the intention to act in compliance with those policies [3, 4].

Attitudes are an overall evaluation of a stimulus (object, activity, and symbol) [5]. However, authors have argued that attitudes are multidimensional [6, 7]. People come up with an overall evaluation when asked to evaluate an action. Still, when the focus is on different aspects independently, the evaluation of the same action can change, and in turn, the influence of each dimension over people's intention to act. For example, the influence of our overall evaluation of daily exercise is different than the evaluation of how important it is for our health and how hard it would be to perform when it is in our control. Similarly, organization members who regard following security

policy as important and necessary can also think that following security policy is annoying or time-consuming. In this paper, we argue for considering (1) the multidimensionality of attitudes and (2) instead of evaluating following policy provisions or specific IS-actions, evaluating the provisions themselves.

We believe the first element is essential for studying the behavioral aspects of cybersecurity because sufficiently different dimensions of attitudes will affect the intention to perform IS actions differently. Therefore, the training and awareness campaigns would have different elements and emphases depending on the more critical dimensions of a specific organization. For example, in an organization with limited resources to deploy information security technology or in places where monitoring employees is not a common practice, an approach that emphasizes the importance of security policy provisions might be more practical and effective than unpractical and expensive punitive measures. But in other organizations where information security is paramount and have the technical and human systems in place that help hold people accountable for security lapses, the necessity of policy provisions might not be as compelling as letting people know that there are punitive actions due to information security misbehavior.

We also argue that changing the focus from evaluating IS action or following security policy provisions to evaluating those provisions is necessary to reduce the effect of social desirability. Asking organization members if specific policy provisions are necessary or sufficient is less prone to social desirability than asking, for example, whether they think that clicking on suspicious emails is good or whether following organizational policy is necessary.

Finally, aligned with this work's focus, we developed an attitudinal scale [attitudes toward security recommendations (ASR scale)] to capture several dimensions of attitudes. This new scale is necessary for IS research and practice given the approach we took to examine attitudes in IS research. The ASR-scale does not compete with other valuable options (i.e. SeBIS [8]; SA-6 [9]; HAIS-Q [10]), whose focus is on attitudes toward specific actions. We believe that the ASR-scale can supplement the information provided by these and other instruments by assessing different dimensions of the evaluation of security policy provisions.

We implemented a sequential quantitative exploratory–confirmatory research design. In the exploratory portion, we formulated several items to capture ASR and pretested them using a sample. Expert feedback and the results obtained led to a set of revised items. Next, we conducted an exploratory factor analysis (EFA) on the revised items to examine the factor structure of the measurement model. This phase led to a revised set of items that underwent a third phase of confirmatory factor analysis (CFA) to validate the final factor structure using a new sample.

Literature review

Attitudes constitute evaluations of a behavioral object (i.e. action, object, individual, group, institution, or policy) [11–13]. Attitudes are a precursor of action or intention to act concerning the behavioral object [14, 15], and authors have suggested that those attitudes have a multidimensional structure [7, 11]. Some authors suggest that in evaluating a behavioral object, two dimensions of attitudes can be distinguished: instrumental and experiential. The instrumental (or cognitive) facet refers to the evaluation of behavioral objects, whereas the experiential (or affective) refers to the individual's feelings toward behavior [11]. Other authors suggest that attitudes contain evaluative, strength or rigor, and activity dimensions [7]. It is noticeable that the examination of attitudes in IS research does not differentiate the possible dimensions of attitudes, even though these dimensions can have a different or opposite effect on IS actions. For example, an employee who thinks the security policy in the organization is important and necessary might think that it is incomplete or too punitive in the case of an IS misbehavior. Are there different dimensions of attitudes toward IS-action or security policy? We examined the IS literature considering the behavioral object studied and the dimensions of attitudes suggested by the items used in the studies. In our review, we found that IS researchers focus on three behavioral objects: specific IS actions, compliance with information security policy, and security policy or its provisions. The items used in IS research reveal primarily an instrumental dimension, even though in some cases, the items suggest at least two: instrumental and experiential.

Researchers that consider attitudes as a unidimensional construct operationalized attitudes toward specific actions or more broad concepts (i.e. following security policy) with items that suggest one dimension. Among the IS actions examined are actions toward implementing protective technologies [1], insecure IT behaviors [16], adopting security technologies [17], secure IS actions [2], performing nonmalicious security violations. [18], and IT ethical behaviors [19] and categories of IS actions such as password management, email use, internet use, social network site use, incident reporting, mobile computing, and information handling [10, 20–23]. The items that authors used in this line of research are, for example, "For me, cleaning spyware from my computer would be: Very bad idea—Very good idea." Researchers that consider broader concepts frequently focus on the antecedents of compliance with security policy or its provisions [i.e. 24–26]. An example of item when the focus is on following security policy is, "Following security policy in my organization is *necessary*."

Researchers also investigate attitudes toward specific actions or more general concepts (i.e. following security policy), capturing the attitudinal construct with items that suggest more than one dimension. Examples of IS-actions investigated in this avenue of research include antivirus software implementation [27] or IT ethical behavior [28]. Examples of the evaluation of more broad concepts are Belanger *et al.* [29] study of the antecedents of early conformance with security policy change or Bulgurcu *et al.* [3] and Ifinedo *et al.* [30, 31] studies on the antecedents of compliance with security policy. Researchers capture the attitudinal construct with items that suggest the consideration of the instrumental aspect of it (e.g. "security measures such as implementing antivirus software, firewalls, or system updates on your home computer are a *good* idea" or "mandating this change of password is a *good* idea.") and the experiential aspect of it (e.g. "performing IT actions is *punishable/rewarding*"). It is noticeable that even though the items suggest more than one dimensions of attitudes, researchers do not separate them conceptually or analytically. It is possible that employees positively evaluate a prescribed action, thinking of it as necessary for preserving information security. Still, they might think performing such action is annoying or time-consuming.

In the present work, we examine attitudes as a multidimensional measure because the different dimensions of attitudes can relate to IS action in a different strength or direction. Evidence of different dimensions of attitudes toward security recommendations (SR) will help make more targeted interventions. For example, in an organization where the importance of SR is not related to IS-Action, but the strictness of SR is, a more punitive approach can be more effective. On the other hand, a strong correlation between the evaluation of SR and IS action will suggest a focus appealing to the legitimacy of SR.

Theoretical background and premise

The reasoned action approach

According to Fishbein and Ajzen [11], attitudes toward action predict the intention to perform the same action, and the intention to act is a good predictor of action under the circumstances conducive to its enactment. The relevance of attitudes as a precursor of action and intention is supported across different domains, such as screening programs [32], physical exercise [33], dietary patterns [34], health-related behaviors [35], chronic illness treatment adherence [36], nutrition-related behaviors [37], organic food consumption [38], condom use [39], sun-protective habits [40], cigarette consumption [41], and physical activity in adolescents [42]. Multiple meta-analyses [i.e. 32, 33, 43, 44] reported medium and large predictive validity of attitudes over the intention to act and action.

Multidimensionality of ASR

Authors [7, 11] argue that attitudes are not unidimensional. For example, people could have positive attitudes toward physical exercise to the extent they know the benefits to their health and well-being. Still, they could also evaluate physical activity as challenging [6]. Therefore, variance in a composite measure of attitudes could be wrongly attributed to only interrater variance when this, in reality, is due to the different valence of different dimensions of attitudes toward the same behavioral object. Proponents of the Theory of Reasoned Action [11] suggest that studying attitudes as part of the dynamics of actions requires a preliminary examination of the dimensionality of this construct before testing its predictive or explanatory capability. This preliminary examination is absent in the IS literature. For some authors, attitudes have an inherent cognitive and affective component [45]. Other authors suggest a two-factor solution with instrumental and experiential factors [11]. Relative to IS-Action and IS policy, employees could evaluate the performance of specific IS actions, recommended or included in IS policy, as necessary while considering them restrictive, time-consuming, or annoying. Thus, it would be logical to think that employees' attitudes toward IS-Action or security policy provisions would have two or more dimensions associated with intention and action. Based on this rationale, we hypothesized that:

H1: the structure of ASR presents a multidimensional structure with an instrumental and experiential aspects.

The perceived rigor of SR as an additional dimension of attitudes

Osgood [7], in his work on the study of meaning, found that besides the evaluative dimension of attitudes, other dimensions emerged. In the study of the attitudes toward several objects, Osgood [7] found a third dimension. The author called this dimension "Potency" (from now on, perceived rigor). This dimension concerns the behavioral object's perceived power, strength, rigor, or hardness. The measurement of this dimension involves terms such as *hard–soft or strong–weak*. One possible explanation for its emergence is that this third dimension depends on the behavioral object [11]. The dimension that emerge depends on the object and the adjectives that are used to capture the attitudes. Thus, the attitudes toward an object can be interpreted as evaluative (instrumental and experiential dimensions) and/or perceived rigor of a behavioral object. For example, and in IS research, attitudes toward security policy can be captured with, for example, "the security procedures are necessary (instrumental)" or "the security procedures are confusing (experiential)," whereas the perceived rigor can be captured with, for example, "the security procedures are strict (perceived rigor)." The last statement could be interpreted also as an instrumental aspect if the respondents evaluate the security policy based on its qualities. It could also be interpreted as experiential if respondents evaluate the same policy based on the results of such a policy. Furthermore, it could be interpreted as perceived rigor if participants regard the word "strict" to punishment in the event case of not following SR.

The relevance of the perceived rigor of ASR is particularly interesting due to the frequency at which IS researchers rely on deterrence theory [e.g. 46, 47]. Based on deterrence theory, researchers argues that the perception of being detected committing an insecure act and the severity of the organizational response to that act can deter the action or intention [48, 49]. The organizational response can be evaluated as a strict response to careless behavior in using information technologies at work. Thus, including perceived rigor of security policy provisions as an additional dimension of attitudes toward security policy provision will be relevant in the overall evaluation of attitudes. Employees' perception of SR as strict or demanding will differ from the instrumental and experiential evaluation of security provisions. Based on this rationale, we hypothesized that:

H2: examining ASR will reveal an additional perceived rigor dimension.

Research design and methods

We implemented a sequential preliminary, exploratory, and confirmatory design, each stage using independent samples. Participants prior to the confirmatory part were recruited from Amazon Mechanical Turk (MTurk), whereas participants at the confirmatory part of the design were recruited from Qualtrics online panels. Before providing their written consent, participants read a description of the study and received a monetary incentive after completing the study. All research was approved by the appropriate Institutional Review Board (IRB). All surveys were administered via Qualtrics, and data were analyzed using RStudio software [50]. In the preliminary study, the items were administered to a sample to assess item wording and survey flow. In the exploratory study, the items were administered to a second sample to explore the attitudes' factor structure. In the confirmatory stage, the items were administered to a third sample to confirm the factor structure from the exploratory study. Before participants read the items, they were presented with the following SR:

"Sharing personal information by email is typically not recommended in organizational policy as it could lead to a security incidents. Some organizations have systems in place that allow employees to enter and share personal information. However, due to a lack of resources or privacy concerns, it is difficult for organizations to monitor whether employees email personal information or use secure systems."

Then they read the following scenario:

"John works at a manufacturing company. People at work believe he is a very supportive coworker, always willing to help. John receives an email asking for some personal information from a colleague, and John, out of professional courtesy, decides to email the required information."

Table 1. Initial item adjectives with corresponding dimensions and descriptive statistics.

Dimension	Adjective	M	SD
Experiential	Meaningful	4.26	0.75
	Influential	4.19	0.79
	Complete	4.18	0.78
	Sufficient	4.22	0.72
	Complex	3.93	1.02
	Concise	4.20	0.80
	Positive	4.25	0.78
	Fruitful	4.20	0.76
	Precise	4.15	0.81
	Perfect	4.13	0.96
	Wise	4.27	0.71
Instrumental	Necessary	4.28	0.74
	Beneficial	4.23	0.81
	Important	4.26	0.72
	Useful	4.28	0.67
Stringent	Constrained	3.99	0.95
	Strong	4.20	0.76
	Severe	3.95	1.02
	Hard	3.82	1.16

Note. $N = 183$. Item Stem: "The recommendations my organization has in terms of handling personal information online are [adjective]."

The preliminary and exploratory study used this scenario, whereas, in the confirmatory study, we used four scenarios with the same character performing the same action but in different contexts at work. In the confirmatory study, participants read only one of the four scenarios. For all studies, items and scenarios were administered randomly.

Preliminary study

We initially developed 19 items to capture the degree at which SR are valued. The item format consisted of a common stem with varying adjectives. The common stem was, "The recommendations my organization has for handling personal information online are [adjective]." Table 1 has initial items adjective and corresponding dimensions of attitudes they were intended to capture [6, 7, 11]. Participants saw one item at a time on their screen, so they can consider the entire item text before answering. The items were measured with a Likert scale ranging from *strongly agree* (1) to *strongly disagree* (5). Items were reversed-scored for the analysis. After reversing the score, a high number indicates that participants think SR in their organizations are important, necessary, complete, strict, and so on.

Measures

The survey included the nineteen initial items that captured the ASR Scale.

Data checking

There were no missing data. Data were examined for multivariate normality and outliers. There was no evidence of non-normality. The Mahalanobis distance was calculated for each score and compared with a cutoff corresponding to the chi-square value of 19 degrees of freedom (the number of items) and an alpha = 0.001 as recommended [51]. Scores with Mahalanobis distance bigger than the cutoff were deemed outliers. In total, 19 outliers were removed to retain a total sample size of 183 (130 males and 53 females ages 18–74). Table 1 has the item descriptive statistics. No noticeable issues were observed with the means and standard deviations as they were visually comparable for the items within each dimension. As such, item wording and survey flow appear to be good.

Exploratory study

Here, interest was in exploring the factor structure of the ASR scale from the preliminary study. An EFA and corresponding supporting statistics were estimated.

Measures

The survey included the final items of the ASR scale from the preliminary study, the same SR, and the scenario shown in the preliminary study.

Data checking

There were no missing data. Data were examined for multivariate normality and outliers. There was no strong evidence of nonnormality. Scores with Mahalanobis distance bigger than the cutoff (chi-square of 19 degrees of freedom; alpha = 0.001) were deemed outliers. In total, 42 outliers were removed to retain a total sample of 727 (429 females and 298 males aged 18–75). For this sample, the participant to item ratio was 38:1, higher than the recommended 10:1 ratio [52].

Confirmatory study

Here, interest was in confirming the factor structure of the ASR scale found in the exploratory study. A CFA and corresponding supporting statistics were estimated. Model fit was assessed with the following criteria: the comparative fit index (CFI) $\geq$ 0.95 [53], standardized root mean square residual (SRMR) $\leq$ 0.08 [54], and root mean square error of approximation (RMSEA) $\leq$ 0.06 [55].

Measures

Participants were given the 19-item ASR, 22-item Williams' [56], and the 5-item social desirability [57] scales, along with the security recommendation shown in the description of the preliminary study, and one out of four different scenarios. The Williams' scale was given to provide evidence of convergent validity as it measures the vulnerability and consequences of phishing attacks along with the costs of preventing phishing attacks. The Williams' scale consists of the following six factors:

1. Perceived severity of the consequences of falling victim to a phishing attack (PS, 5 items, alpha = 0.86);
2. Perceived vulnerability of falling victim to a phishing attack (PV, 5 items, alpha = 0.90);
3. Antiphishing techniques self-efficacy as means to prevent falling victim to a phishing attack (RE, 3 items, alpha = 0.85);
4. Antiphishing techniques knowledge acquiring self-efficacy (SE, 3 items, alpha = 0.85);
5. Perceived ability to detect phishing emails (PA, 3 items, alpha = 0.87); and
6. Response cost regarding acquiring antiphishing techniques knowledge (RC, 3 items, alpha = 0.80).

Items were Likert ranging from *strongly agree* (1) to *strongly disagree* (5). Social desirability is a distinct construct from SR. As such, the unidimensional social desirability scale (ScD; average alpha = 0.70) was given to provide evidence of discriminant validity. Items in this scale are Likert ranging from *definitely true* (1) *to definitely false* (5).

Table 2. Response counts per group for valid responses.

Counts	*N*	%
Age		
18–34 years old	179	26
35–44 years old	173	25
45–54 years old	136	20
55 years old and over	200	29
Gender		
Male	317	46
Female	371	54
Education		
High school graduate, no college, and less than a high school diploma	130	19
Some college, no degree, and associate degree	202	29
Bachelor's degree	220	32
Advance degree	136	20
Work experience		
Less than 10 years	195	28
More than 10 years	493	72
Job level		
Entry and mid-levels	550	80
Executive level	138	20
Number of employees		
Between 2 and 100 members	212	31
Between 101 and 500 members	141	20
More than 500	335	49

Note: $N = 688$.

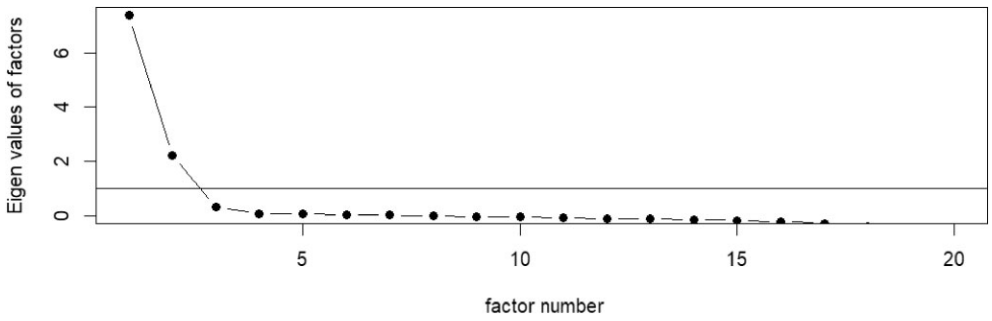

Figure. 1. Scree Plot, ASR scale, N=727.

Sample size requirements and data checking

A power analysis was conducted to establish the sample size requirement for a CFA. An a priori power analysis [58] for the two-factor measurement model ($df = 53$) with RMSEA of 0.06, alpha of 0.05, and 0.8 statistical power resulted in a minimum sample size of 235 cases. There were no missing data. Data were examined for multivariate normality and outliers. There was no strong evidence of non-normality, and 33 outliers were removed with the Mahalanobis distance criteria.

After data checking, we retained 317 males and 371 females aged 18–74 with valid responses ($N = 688$). Data were collected based on demographic quotas of age, gender, and level of education following the US Bureau of Labor Statistics [59]. Table 2 shows response counts per group for valid responses.

Results

Exploratory factor study

An EFA was used to explore the factor structure of the ASR Scale. Factors were extracted using principal axis extraction, and rotated with an Oblimin rotation that allows factors to correlate [51]. The Oblimin rotation used delta = 0 allowing the factor correlations to be determined by the data. The critical consideration in the EFA was an interpretable factor structure (Tabachnick, 2001).

Based on the scree plot in Fig. 1, two factors were extracted. Initially, three factors were extracted, but two factors were highly correlated with $r = 0.72$ indicating that these factors may be redundant. As such, two factors led to a more interpretable factor structure. Of the 19 items, the following seven items were removed due to poor loadings (< 0.3) and/or cross-loading: *perfect*, *meaningful*, *useful*, *influential*, *positive*, *fruitful*, *and concise*. The remaining item loadings were in the range between very good (> 0.63) and excellent (> 0.71) [60]. The final two-factor structure consisted of the following two factors: Legitimacy and effectiveness of Security Recommendations (LESR) and Rigor of security recommendations (RSR). Table 3 presents the exploratory factor structure for the final 12 items with Cronbach's alpha normal theory bootstrap confidence interval (CIs) [61].

Confirmatory factor study

The ASR CFA results for each step of the analyses are in Table 4. The initial 12-item factor loadings indicated a good two-factor structure with fit indices that indicated decent fit. It is common for initial Structural Equation Models (SEMs) to not adequately fit the data [62, 63].

Table 3. ASR exploratory factor structure for the final 12 items.

Adjective	M	SD	LESR	RSR
Beneficial	4.18	0.78	**0.76**	−0.09
Complete	4.02	0.85	**0.63**	0.16
Sufficient	4.09	0.85	**0.68**	0.13
Important	4.26	0.76	**0.67**	−0.19
Wise	4.23	0.79	**0.72**	−0.06
Necessary	4.28	0.78	**0.69**	−0.15
Precise	3.99	0.86	**0.69**	0.15
Hard	3.43	1.24	−0.06	**0.85**
Strong	4.09	0.87	**0.68**	0.17
Severe	3.61	1.15	0.19	**0.70**
Constrained	3.67	1.05	0.02	**0.74**
Complex	3.46	1.20	−0.04	**0.81**

Note: $N = 727$. Principal axis extraction and Oblimin rotation were used. LESR = Legitimacy and effectiveness of security recommendations, Cronbach Alpha [95% CI] = 0.879, [0.864, 0.894]; RSR = Rigor of Security Recommendations, Cronbach Alpha [95% CI] = 0.863, [0.846, 0.881]; LESR and RSR correlation = 0.19. All CIs based on 1000 bootstrap samples. Item Stem: "The recommendations my organization has in terms of handling personal information online are [adjective]."

As such, to maintain a clear factor structure and parsimony, modification indices (MIs) were used to refine the factor structure [64]. In particular, the *severe* item MI suggested that it also loads into LESR. However, items with cross-loadings obscure a facture structure, so the *severe* item was eliminated. Additionally, the MIs for the *important* and *beneficial* items suggested measurement error (residual) correlations with the *necessary* item. Because the *important* and *beneficial* items are conceptually similar, they were eliminated to eliminate redundant information. The results of the final 9-item two-factor structure are in the final step of Table 4. To further determine that a two-factor structure is preferable to a single factor structure, the final 9-item two-factor structure was compared to a 9-item single factor structure, $\chi^2(27, N = 688) = 533.263$, CFI = 0.798, RMSEA [90% CI] = 0.165 [0.153, 0.177], SRMR = 0.116. The chi-square difference test indicated that the two-factor structure had significantly better fit than the single factor structure, $\chi^2(1, N = 688) = 432.78$, $P = 0.000$, Delta CFI = 0.172. Table 5 has the 9-item ASR factor structure with Cronbach alphas. All loading ranged from 0.62 to 0.81 (good to excellent; [65]). The ASR Cronbach alphas were all acceptable (> 0.7).

Table 6 has the correlations of the ASR, Williams', and social desirability measures to assess the validity of the ASR. In terms of convergent validity, the ASR had the expected correlations with the dimensions of the Williams' measure. For LESR, there were moderate to strong correlations with RC ($r = 0.38$), PS ($r = 0.42$), RE ($r = 0.37$), and SE ($r = 0.33$). This indicates that individuals value SR as legitimate and effective if they are aware of the consequences of phishing attacks and feel prepared to acquire knowledge to detect and prevent falling victim to phishing attacks. For RSR, there were moderate to strong correlations with PV ($r = 0.34$) and PA ($r = 0.52$). This indicates that individuals, aware of the vulnerability of falling victim to a phishing attack, value the severity of SR but can also see those recommendations as costly for time and attention. In terms of discriminant validity, the ASR dimensions had the expected correlations with ScD. Specifically, the LESR ($r = 0.018$) and RSR ($r = -0.03$) correlated weakly with social desirability, providing evidence of discriminant validity for the ASR.

Table 5. ASR final factor structure with cronbach alphas.

Adjective	LESR	RSR
Complete	0.810	
Sufficient	0.751	
Wise	0.733	
Necessary	0.653	
Precise	0.779	
Strong	0.777	
Hard		0.772
Constrained		0.622
Complex		0.695

Model: $\chi 2\ (26, N = 688) = 100.487$, $P = 0.000$, CFI = 0.970, RMSEA [90% CI] = 0.065 [0.051, 0.078], SRMR = 0.043. LESR = Legitimacy and effectiveness of Security Recommendation, Cronbach Alpha [95% CI] = 0.885, [0.871, 0.899]; RSR = Rigor of Security Recommendations, Cronbach Alpha [95% CI] = 0.737, [0.695, 0.778]. LESR and RSR correlation = 0.142; All CIs based on 1000 bootstrap samples. Item Stem: "The recommendations my organization has in terms of handling personal information online are [adjective]."

In addition, we examined factorial validity. We compared the average variance extracted (AVE) with each factor's composite reliability (CR). An AVE value greater than 0.5 and lower than CR for each factor was deemed as evidence of convergent validity. Discriminate validity was established if the square root of AVE by each factor was greater than the correlation between the construct in question and the other factors [66]. The AVE of the two factors was equal to or greater than 0.5 and lower than the CR, suggesting convergent validity. The square root of AVE of the two factors was greater than the correlation between them, suggesting discriminate validity. Table 7 shows the factorial validity results of the two-factor solution.

Discussion

We found that a two-factor, uncorrelated measurement model best describe the ASR. The two factors reflect two dimension of attitudes,

Table 4. ASR fit and MIs.

Step	MI
Initial: $\chi 2(53) = 318.841$, CFI = 0.927, RMSEA [90% CI] = 0.085 [0.076, 0.095], SRMR = 0.076	
severe to load on LESR; *severe* removed	64.461
Step 1:	
Residual correlation between important and necessary; *important* removed	38.130
Step 2:	
beneficial to correlate with *necessary*; *beneficial* removed	36.945
Final: $\chi 2(26) = 100.487$, CFI = 0.970, RMSEA [90% CI] = 0.065 [0.051, 0.078], SRMR = 0.043	

Note: $N = 688$.

Table 6. ASR factor correlations with other measures.

Factor	LESR	RSR	Williams's dimension
RC	**0.378**	− 0.082	Response cost regarding acquiring antiphishing techniques knowledge.
PV	0.003	**0.343**	Perceived vulnerability of falling victim to a phishing attack.
PS	**0.422**	− 0.066	Perceived severity of the consequences of falling victim to a phishing attack.
RE	**0.370**	− 0.057	Antiphishing techniques self-efficacy as means to prevent falling victim to a phishing attack.
SE	**0.333**	− 0.066	Antiphishing techniques knowledge acquiring self-efficacy.
PA	− 0.034	**0.519**	Perceived ability to detect phishing emails.
ScD	0.018	− 0.032	Social desirability composite score

Note: LESR = legitimacy and efficacy of security recommendations; RSR = rigor of security recommendations. Bolded indicate moderate to strong correlation.

Table 7. Factorial validity results of the two-factor solution.

Factor	CR	AVE	LESR	RSR
LESR	0.885	0.576	(0.758)	
RSR	0.736	0.496	0.148	(0.704)

Note: The element in the matrix is the correlation coefficient between LESR and RSR. In parenthesis are the square root of the AVE for LESR and RSR. AVE: average variance extracted; CR: composite reliability; LESR: legitimacy and effectiveness of security recommendations; and RSR: Rigor of securty recomendations.

the perceived legitimacy and effectiveness, and the perceived rigor of securty recomendations. The emergence of the first dimension partially align with the extant IS literature that capture attitudes toward IS action with terms that suggest the evaluation of IS-Action or policy compliance [i.e. 1, 3, 24, 25, 27, 29]. Noticeable, the attitudinal object in the present work is not an IS action or following security policy, but policy provisions itself. We argue that the operationalization of attitudes toward a broader construct reflecting organizational systems, offers several advantages over the operationalization toward IS action or policy compliance. First, it gives the opportunity to practitioners to examine how policy provisions are perceived and to organization members to express their perspective about the efforts made in terms of cybersecurity. Second, employees' evaluation of what their organization is doing in term of cybersecurity is likely less bias than evaluating their own actions or whether is good to follow or comply with security policy. Future work is necessary to confirm this hypothesis. Finally, evaluating a broader concept such as SR can act as precursor of several IS actions instead of specific ones. In the Fishbein's tradition of operationalization of the antecedents of action, the antecedents correlate stronger with the intention to act if those are relative to the same action, target, context, and time [11]. But this operationalization has received criticism due to the lack of generalizability of findings from the study of single actions and the possibility that this approach would inflate the model's predictive capability [67]. At the conclusion of this work, we offer the ASR scale, which is relative to a broader concept that will assist practitioners capture how important, effective, and stringent SR are perceived and aim to help research with a new approach to capture attitudes as precursor of several categories of IS action at work.

Initially, we hypothesized that the evaluation of SR would reveal two dimensions, instrumental, and experiential. In the exploratory study the dimensions emerged. We named the emergent dimensions perceived legitimacy (instrumental) and perceived effectiveness (experience). However, we found that the two subdimensions strongly correlated ($r = 0.72$). These results aligns with others in attitudes research [68, 69]. The IS literature in general does not consider a multidimensional measure of attitudes. In the present work, we could not stablish that instrumentality and the experience dimensions of attitudes relative to SR as independent measures. This disconfirm our first hypothesis. However, a significantly different relation between these two subdimension of attitudes and the intention to perform IS action, can still justify the independent consideration of the two evaluative dimensions. Interventions that focus on only the legitimacy of the efforts made by the organization in terms of cybersecurity would omit the positive and negatives experiences that organization members have had with them. An intervention can be more effective if the two aspect of the evaluation of cybersecurity efforts are considered.

Furthermore, and expanding the literature on attitudes toward a behavioral object and the IS literature, the perceived rigor emerged as another dimension of ASR. This evidence corroborates our second hypothesis. These findings are significant because if the relation between this additional dimension of attitudes and IS action is found, more nuanced training sessions and awareness campaigns can give different emphasis to the legitimacy or strictness of the SR depending on the organizational culture. Therefore, a more complete information of the organization members perceptions including the strictness of policy provisions will help to develop robust interventions that target both the evaluations of legitimacy and effectiveness and the perceived rigor of SR.

The improved two-factor measurement model of the ASR scale demonstrated convergent and discriminant validity when compared with other validated scales. For this specific analysis we used the William's scale to measure the self-efficacy relative to the used of antiphishing techniques, their perceived cost, and the perceived vulnerability of phishing attacks [56]. We deemed this scale relevant for our analysis because the present study centered on the attitudes relative to security recommendation that will prevent, among other, phishing attacks. The perceived LESR correlated moderately with the perceived severity of falling victim to a phishing attack. This evidence suggests that employees in the USA regard SR as important to the extent that they perceive severe consequences of falling victim to a phishing attack. It is also worth noticing that the perceived severity of the consequences of falling victim to a phishing attack (PS in Williams' scale) uncorrelated with the perceived RSR and correlate strongly with LESR. This evidence implies that when employees perceive the severity of the consequences of falling for a phishing attack, they do not evaluate those recommendations as restricted or severe but as necessary and sufficient. The perception of RSR was positively associated with perceived vulnerability (PV in William's scale). This evidence suggests that employees see a constrained set of instructions as evidence of the vulnerability of falling for phishing attacks. Finally, the correlation between RSR and perceived ability (RC in William's scale) was moderate as we expected, providing evidence of convergent validity of the ASR scale. But it also suggests that the more complex and severe SRs are perceived, the higher the perceived ability to detect phishing emails.

The sample size was adequate for a significant population and appropriate for the analysis strategy (SEM). The samples came from two online panels and were appropriate for the target population.

Conclusions

We determined appropriate psychometric properties of nine indicators of two dimensions of attitudes. The analyses revealed that an improved two-factor solution has a better model fit than other alternative models and showed internal consistency and convergent and discriminant validity. The items, or modifications of them, can be used to examine the dimensions of attitudes toward SR recommendations or other policy provisions as determinants of IS action or intention.

We found that the attitudes toward SR present a multidimensional structure with two factors: perceived legitimacy and effectiveness of SR and perceive rigor of SR. Considering the complex structure of ASR brings the opportunity to improve security policy addressing each aspect of attitudes. An intervention that focuses on influencing the perceived legitimacy aspect of ASR can also focus on the perceived rigor by setting the right tone and creating realistic expectation regarding the subsequent corrective measures in the event of a security breach result from an unsafe behavior in the cyberspace. Equally relevant, capturing the multidimensional nature of attitudes will allow a comprehensive evaluation of security programs so that policymakers can assess the overall effect of those programs and discriminate the effect of interventions over each dimension of attitudes. The findings in this study contribute to theory expanding the consideration of attitudes as a concept with at least two separate dimensions that can differently affect the intention of IS actions in the workplace. This work provides the ASR-Scale, a 9-item scale, unbiased by social desirability, that can be used to gather employees' evaluations of relevant security policy provisions in addition to scales that capture attitudes toward specific IS-Actions.

This study has limitations. We only examined the attitudes toward security recommendations. A broader concept, such as *evaluating the overall efforts made by organizations in terms of cybersecurity*, could be examined as a focus-concept in future research. Researchers can examine its relationship with the criterion variable (IS-actions, policy compliance) by modifying the ASR scale. Another limitation and subject of future research is further examine the convergent validity examination of the ASR scale with other attitudinal measures such as the SeBIS [8] or the SA-13 attitudinal scale [70]. Even though the Williams and Joinson's [56] scale we used in the present work used the SeBIS and Privacy scales in their analysis of convergent and discriminant validity, future validation of the ASR scale with the SA-13 or the attitudinal dimension of the Human Aspects of Information Security Questionnaire (HAIS-Q) [10, 22] will add further robustness to the new ASR scale.

Authors' contributions

Miguel A. Toro-Jarrin (Conceptualization [Equal], Data curation [Lead], Formal analysis [Lead], Funding acquisition [Equal], Investigation [Equal], Methodology [Equal], Project administration [Lead], Software [Lead], Writing – original draft [Lead]), Pilar Pazos (Conceptualization [Equal], Funding acquisition [Supporting], Investigation [Supporting], Methodology [Equal], Project administration [Supporting], Resources [Equal], Software [Supporting], Supervision [Lead], Writing – review & editing [Lead]), and Miguel A. Padilla (Data curation [Supporting], Formal analysis [Supporting], Methodology [Equal], Software [Supporting], Supervision [Equal], Writing – review & editing [Equal])

Conflict of interest: We have no known conflict of interest to disclose.

Funding

This work was supported by the Coastal Virginia Center for Cyber Innovation and the Commonwealth Cyber Initiative (USA); the Fulbright program (USA); and the Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Ecuador).

References

1. Dinev T, Hu Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *JAIS* 2007;**8**:386–408. https://doi.org/10.17705/1jais.00133.
2. Jansen J. Comparing three models to explain precautionary online behavioural intentions. *Inf Comput Secur* 2017;**25**:165–80. https://doi.org/10.1108/ICS-03-2017-0018.
3. Bulgurcu B, Cavusoglu H, Benbasat I. Information Security Policy compliance: an empirical study of rationality-based beliefs and Information security awareness. *MIS Quart* 2010;**34**:523–48. https://doi.org/10.2307/25750690.
4. Rajab M, Eydgahi A. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Comput Secur* 2019;**80**:211–23.
5. Fiske ST, Gilbert DT, Lindzey G. *Handbook of Social Psychology*. 5th edn. Hoboken: John Wiley, 2010.
6. Ajzen I, Driver BL. Application of the theory of planned behavior to leisure choice. *J Leisure Res* 1992;**24**:207–24.
7. Osgood CE. *The Measurement of Meaning*. Urbana: University of Illinois Press, 1957.
8. Egelman S, Peer E. Scaling the security wall: developing a security behavior intentions scale (SEBIS). In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Vol. **2015**, New York: ACM, 2015, 2873–82.
9. Faklaris C, Dabbish LA, Hong JI. A self-report measure of end-user security attitudes (SA-6). In: *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. Vol. **2019**. Santa Clara: ACM, 2019, 61–77.
10. Parsons K, Calic D, Pattinson M. *et al*., The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Comput Secur* 2017;**66**:40–51.
11. Fishbein M, Ajzen I. *Predicting and Changing Behavior the Reasoned Action Approach*. New York: Psychology Press, 2010.
12. Eagly AH. *The Psychology of Attitudes*. Fort Worth: Harcourt Brace Jovanovich College Publishers, 1993.
13. Maio GR, Haddock G, Verplanken B. *The Psychology of Attitudes and Attitude Change*. Thousand Oaks: Sage, 2018.
14. Fishbein M. *Belief, Attitude, Intention, and Behavior an Introduction to Theory and Research*. Reading: Addison-Wesley Pub. Co., 1975.
15. Ajzen I. The theory of planned behavior. *Organ Behav Hum Decis Process* 1991;**50**:179–211. https://doi.org/10.1016/0749-5978(91)90020-T.
16. Djajadikerta HG, Roni SM, Trireksani T. Dysfunctional information system behaviors are not all created the same: challenges to the generalizability of security-based research. *Inf Manag* 2015;**52**:1012–24. https://doi.org/10.1016/j.im.2015.07.008.
17. Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. *Eur J Inf Syst* 2009;**18**:106–25. https://doi.org/10.1057/ejis.2009.6.
18. Guo KH, Yuan Y, Archer NP. *et al*. Understanding nonmalicious security violations in the workplace: a composite behavior model. *J Manag Inf Syst* 2011;**28**:203–36. https://doi.org/10.2753/MIS0742-1222280208.
19. Leonard LNK, Cronan TP, Kreie J. What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics?. *Inf Manag* 2004;**42**:143–58. https://doi.org/10.1016/j.im.2003.12.008.
20. McCormac A, Zwaans T, Parsons K. *et al*. Individual differences and information security awareness. *Comput Hum Behav* 2017;**69**:151–6. https://doi.org/https://doi.org/10.1016/j.chb.2016.11.065.

21. Parsons K, Agata M, , Pattinson M. *et al.* A study of information security awareness in Australian government organisations. *Inf Manag Comput Secur* 2014 **22**:334. https://doi.org/10.1108/IMCS-10-2013-0078.
22. Parsons K, McCormac A, Butavicius M. *et al.* Determining employee awareness using the Human aspects of information security questionnaire (HAIS-Q). *Comput Secur* 2014;**42**. https://doi.org/10.1016/j.cose.2013.12.003.
23. Parsons K, McCormac A, Pattinson M. *et al.* The design of phishing studies: challenges for researchers. *Comput Secur* 2015;**52**:194–206. https://doi.org/10.1016/j.cose.2015.02.008.
24. Siponen M, Mahmood MA, Pahnila S. Employees' adherence to information security policies: an exploratory field study. *Inf Manag* 2014;**51**:217–24.
25. Safa NS, Von Solms R, Furnell S. Information security policy compliance model in organizations. *Comput Secur* 2016;**56**:70–82.
26. Aurigemma S, Mattson T. Generally speaking, context matters: making the case for a change from universal to particular ISP research. *JAIS* 2019;**20**:1700–42. https://doi.org/10.17705/1jais.00583.
27. Anderson CL, Agarwal R. Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quart* 2010;**34**:613–43. https://doi.org/10.2307/25750694.
28. Banerjee D, Cronan TP, Jones TW. Modeling IT ethics: a study in situational ethics. *MIS Quart* 1998;**22**:31–60. https://doi.org/10.2307/249677.
29. Bélanger F, Collignon S, Enget K,. *et al.* Determinants of early conformance with information security policies. *Inf Manag* 2017;**54**:887–901.
30. Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Comput Secur* 2012;**31**:83–95. https://doi.org/https://doi.org/10.1016/j.cose.2011.10.007.
31. Ifinedo P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. *Inf Manag* 2014;**51**:69–79. https://doi.org/https://doi.org/10.1016/j.im.2013.10.001.
32. Cooke R, French DP. How well do the theory of reasoned action and theory of planned behaviour predict intentions and attendance at screening programmes? A meta-analysis. *Psychol Health* 2008;**23**:745–65. https://doi.org/10.1080/08870440701544437.
33. Hagger MS, Chatzisarantis N, Biddle S. A meta-analytic review of the theories of reasoned action and planned behavior in physical activity: predictive validity and the contribution of additional variables. *J Sport Exer Psychol* 2002;**24**:3–32. https://doi.org/10.1123/jsep.24.1.3.
34. McDermott MS, Oliver M, Simnadis T. *et al.* The Theory of Planned Behaviour and dietary patterns: a systematic review and meta-analysis. *Prev Med* 2015;**81**:150–6. https://doi.org/10.1016/j.ypmed.2015.08.020.
35. McEachan RRC, Conner M, Taylor NJ. *et al.* Prospective prediction of health-related behaviours with the Theory of Planned Behaviour: a meta-analysis. *Health Psychol Rev* 2011;**5**:97–144. https://doi.org/10.1080/17437199.2010.521684.
36. Rich A, Brandes K, Mullan B. *et al.* Theory of Planned Behavior and adherence in chronic illness: a meta-analysis. *J Behav Med* 2015;**38**:673–88. https://doi.org/10.1007/s10865-015-9644-3.
37. Riebl SK, Estabrooks PA, Dunsmore JC. *et al.* A systematic literature review and meta-analysis: the Theory of Planned Behavior's application to understand and predict nutrition-related behaviors in youth. *Eat Behav* 2015;**18**:160–78. https://doi.org/10.1016/j.eatbeh.2015.05.016.
38. Scalco A, Noventa S, Sartori R. *et al.*. Predicting organic food consumption: a meta-analytic structural equation model based on the theory of planned behavior. *Appetite* 2017;**112**:235–48. https://doi.org/10.1016/j.appet.2017.02.007.
39. Sheeran P, Taylor S. Predicting intentions to use condoms: a meta-analysis and comparison of the theories of reasoned action and planned behavior 1. *J Appl Soc Pyschol* 1999;**29**:1624–75. https://doi.org/10.1111/j.1559-1816.1999.tb02045.x.
40. Starfelt Sutton LC, White KM. Predicting sun-protective intentions and behaviours using the theory of planned behaviour: a systematic review and meta-analysis. *Psychol Health* 2016;**31**:1272–92. https://doi.org/10.1080/08870446.2016.1204449.
41. Topa G, Moriano JA. Theory of planned behavior and smoking: meta-analysis and SEM model. *SAR* 2010;**1**:23–33. https://doi.org/10.2147/SAR.S15168.
42. Plotnikoff RC, Costigan SA, Karunamuni N. *et al.* Social cognitive theories used to explain physical activity behavior in adolescents: a systematic review and meta-analysis. *Prev Med* 2013;**56**:245–53. https://doi.org/10.1016/j.ypmed.2013.01.013.
43. Tyson M, Covey J, Rosenthal HES. Theory of Planned Behavior interventions for reducing heterosexual risk behaviors: a meta-analysis. *Health Psychol* 2014;**33**:1454–67. https://doi.org/10.1037/hea0000047.
44. Cooke R, Dahdah M, Norman P. *et al.* How well does the theory of planned behaviour predict alcohol consumption? A systematic review and meta-analysis. *Health Psychol Rev* 2016;**10**:148–67. https://doi.org/10.1080/17437199.2014.947547.
45. Conner M, Norman P, Bell R. The theory of planned behavior and healthy eating. *Health Psychol* 2002 **21**, 194–201 11950110
46. Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. *MIS Quart* 2010;**34**:549–66. https://doi.org/10.2307/25750691.
47. Willison R, Warkentin M, Johnston AC. Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives: examining the influence of disgruntlement on computer abuse intentions. *Inf Syst J* 2018;**28**:266–93. https://doi.org/10.1111/isj.12129.
48. Lowry PB, Moody GD. Explaining opposing compliance motivations towards organizational information security policies. In: *Proceedings of the Annual Hawaii International Conference on System Sciences*. Piscataway: IEEE, 2013, 2998–3007.
49. Willison R, Lowry PB, Paternoster R. A tale of two deterrents: considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research. *JAIS* 2018;**19**:1187–216. https://doi.org/10.17705/1jais.00524.
50. RStudio Team. *RStudio: Integrated Development for R*. Boston: PBC, 2020.
51. Tabachnick BG. *Using Multivariate Statistics*. 4th edn. Boston: Allyn and Bacon, 2001.
52. Nunnally JC. *Psychometric Theory*. 3rd edn. New York: McGraw-Hill, 1994.
53. Bentler PM. Comparative fit indexes in structural models. *Psychol Bull* 1990;**107**:238.
54. Bentler PM, Wu EJC. EQS 6.1 for Windows – structural equations program manual. Encino: Multivariate Software, 2005.
55. Steiger JH, Lind JC. Statistically based tests for the number of common factors. I n: *Annual Meeting of the Psychometric Sociality*. Iowa City: University of Iowa, 1980.
56. Williams EJ, Joinson AN. Developing a measure of information seeking about phishing. *J Cybersecur* 2020;**6**:tyaa001.
57. Hays RD, Hayashi T, Stewart AL. A five-item measure of socially desirable response set. *Educ Psychol Measur* 1989;**49**:629–36. https://doi.org/10.1177/001316448904900315.
58. Moshagen M. Power analysis for structural equation models: semPower Manual. CRAN, 2021.
59. U.S. Bureau of Labor Statistics. Employment status of the civilian population. Washington, 2021.
60. Comrey AL, Lee HB. *A First Course in Factor Analysis*. London: Psychology Press, 2013.
61. Padilla MA, Divers J, Newton M. Coefficient alpha bootstrap confidence interval under nonnormality. *Appl Psychol Measur* 2012;**36**:331–48.
62. Kline RB. *Principles and Practice of Structural Equation Modeling*. New York: Guilford Publications, 2023.
63. Loehlin JC, Beaujean AA. *Latent Variable Models: An Introduction to Factor, Path, and Structural Equation Analysis*. New York: Routledge, 2017.
64. Doane AN, Kelley ML, Chiang ES. *et al.* Development of the cyberbullying experiences survey. *Emerg Adulthood* 2013;**1**:207–18.
65. Osborne JW, Costello AB, Kellow JT.Best Practices in Exploratory Factor Analysis *Best Practices in Quantitative Methods* , California: Sage, 2008, 86–99.

66. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. *J Market Res* 1981;**18**:39–50. https://doi.org/10.2307/3151312.
67. Ogden J. Some problems with social cognition models: a pragmatic and conceptual analysis. *Health Psychol* 2003;**22**:424.
68. Ajzen I, Driver BL. Prediction of leisure participation from behavioral, normative, and control beliefs: an application of the theory of planned behavior. *Leisure Sci* 1991;**13**:185–204. https://doi.org/10.1080/01490409109513137.
69. La Barbera F, Ajzen I. Instrumental vs. experiential attitudes in the theory of planned behaviour: two studies on intention to perform a recommended amount of physical activity. *Int J Sport Exer Psychol* 2022;**22**:1–13.
70. Faklaris C, Dabbish L, Hong JI. Do they accept or resist cybersecurity measures? Development and validation of the 13-item security attitude inventory (SA-13). *arXiv* arXiv:2204.03114. 2022.