A Self-Report Measure of End-User Security Attitudes (SA-6)

Cori Faklaris, Laura Dabbish and Jason I. Hong

Human-Computer Interaction Institute, School of Computer Science, Carnegie Mellon University
Pittsburgh, PA, USA
{cfaklari, dabbish, jasonh}@cs.cmu.edu

Abstract

We present SA-6, a six-item scale for assessing people's security attitudes that we developed by following standardized processes for scale development. We identify six scale items based on theoretical and empirical research with sufficient response variance, reliability, and validity in a combined sample ($N = 478$) from Amazon Mechanical Turk and a university-based study pool. We validate the resulting measure with a U.S. Census-tailored Qualtrics panel ($N = 209$). SA-6 significantly associates with self-report measures of behavior intention and recent secure behaviors. Our work contributes a lightweight method for (1) quantifying and comparing people's attitudes toward using recommended security tools and practices, and (2) improving predictive modeling of who will adopt security behaviors.

1. Introduction

The human in the loop is often the weakest link in any security system [17,78]. Understanding people's attitudes toward security technology is key to designing systems that are both usable and tough to breach. For this reason, a fair amount of research in usable security and privacy employs in-depth interviews and observation with small samples to understand people's attitudes toward a security practice or technology, e.g. [12,20,29,36,73]. However, we need to seek ways to operationalize such concepts in efforts to better understand the phenomenon and its relation with causes and outcomes in a more robust way e.g., experiments and longitudinal surveys. It is not always feasible or appropriate to utilize a qualitative approach. It is time-consuming to identify and label the concepts underlying people's open-ended responses, and such custom analyses are prone to error. We need a quantitative measure in order to systematically assess and compare users' security attitudes.

The current state of the art for measuring users' thinking about security practices is the Security Behavior Intentions Scale [32,33]. SeBIS' 16 items are grounded in security expert recommendations for user behavior in four areas: device securement, updates, password management, and

proactive awareness. While SeBIS can tell us the degree to which a user intends to comply with these expert recommendations, it cannot tell us people's attitudes about security behaviors.

A measure of security attitudes supports research on differences in security-related intentions and behaviors. Attitudes represent people's evaluation of objects, groups, events, that is, how they orient to the world around them [4]. An extensive body of research in psychology examines attitudes, their antecedents and consequences, and their relationship to intentions and behavior [4,6,18,49]. In fields as disparate as organizational psychology [57] and environmental sustainability e.g. [9,43], researchers measure attitudes to understand behavior and general tendencies. In security, such a measure would be useful to understand what leads to different security attitudes, and the effect of these attitudes on intentions and behavior.

For this purpose, we introduce a 6-item self-report measure of security attitudes: SA-6. Our measure is based on user-centered empirical and theoretical studies of awareness, motivation to use and knowledge of expert-recommended security tools and practices (*security sensitivity*) [20–24]. Using principles of psychological scale development [28,39,46,53], we generate 48 candidate items that on their face corresponded to prior work on security attitudes and that pilot testers found to be unambiguous and easily answered. Through iterative rounds of analysis, we narrow to six items that demonstrated desired response variance, factor loadings, reliability, and validity using data from Amazon Mechanical Turk and a university-based study pool (combined $N = 478$) and from a U.S. Census-tailored panel ($N = 209$).

We find SA-6 to be significantly associated with self-report measures of behavior intention. Using linear regression, we found SA-6 explained 28% of the variance in SeBIS ($p<.01$). This result is consistent with longstanding psychological evidence of the relationship between attitudes and behavior intention [5,7,8,37,69,75]. Our data shows SA-6 also relates with measures of subjective norms, chiefly privacy, and perceived behavior control, such as impulsivity, self-efficacy and internet know-how. Our data also shows SA-6 differs as expected by personal experiences and hearing/seeing reports of security breaches, and by age, gender, education and income level. These results, predicted by the Theory of Reasoned Action Model [37], demonstrate the convergent and discriminant validity of this scale [28,39,46,53].

We also find SA-6 significantly associated with self-reported recent security behavior. Here we go beyond previous work on security behavior intentions, connecting attitudes and intentions to people's recalled security actions in the past week. We find that SA-6 and SeBIS associate with recent security actions and support for SeBIS as a partial mediator of SA-6's influence on reported recent security behavior. Our results suggest that SA-6 may help model who is likely to act on security recommendations and who will benefit most from security awareness training or tutorials.

This paper makes the following contributions:

- The introduction of a six-item validated self-report measure of security attitudes (SA-6) for use by researchers and practitioners to systematically assess and compare user attitudes toward security techniques;

- An analysis of the relationship between security attitudes, security intentions, and recent security actions;

- A discussion of how and why to use SA-6 for measuring security attitudes to explain and predict user adoption of recommended security behaviors.

2. Related Work

Most human behavior is goal-directed [8]. But for most computer users, staying secure and avoiding relevant threats is a secondary goal at best. The need to understand how to nudge adoption of secure behaviors *in spite of this* underpins much prior work integrating psychology with cybersecurity.

To develop our scale, we identified a concept in the cybersecurity literature that corresponds to the psychological conception of attitude. We then identified concepts that could be expected to relate to and vary with this attitude factor according to theoretical models of how accept and adopt expert-recommended secure tools and practices.

2.1. Attitudes

Attitudes represent people's evaluation of objects, groups, events, that is how they orient to the world around them [4]. Eagly and Chaiken [30] define an attitude as "a psychological tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor." An extensive body of research in psychology examines attitudes, their antecedents and consequences and their relationship to intentions and behavior [4,6]. In fields as disparate as organizational psychology [57] to environmental sustainability e.g. [9,43], researchers measure attitudes to understand behavior.

To develop our measure of security attitudes, we examined the cybersecurity literature for work that documented user attitudes about expert-recommended tools and practices. The focal concept we identified is *security sensitivity*.

2.2. Security Sensitivity

In the field of usable security, end-user *security sensitivity* is defined by Das as "the awareness of, motivation to use, and knowledge of how to use security tools" and practices [20]. Das and collaborators based this construct on empirical findings in interview studies that many people believe themselves in no danger of falling victim to a security breach and are unaware of the existence of tools to protect them against those threats; also, they perceive the inconvenience and cost to their time and attention of using these tools and practices as outweighing the harm of experiencing a security breach; and, they think these measures are too difficult to use or lack the knowledge to use them effectively [20–23].

Das summarized the concept as a series of six questions, which focus in parallel on tools and threats [20]. Restated, these six sub-dimensions are: *awareness of the existence of security threats*; *awareness of the existence of security measures* (tools, behaviors and strategies) that can be used to counteract threats; *motivation to counteract security threats*; *motivation to use security measures* to counteract threats; *knowledge of the relevance of security threats*; and *knowledge of how to use security measures* to counteract relevant threats. This builds in turn on theoretical and empirical work from Davis and others [25,26] on *user perceptions of usefulness and ease of use,* from Egelman et al. [31]'s adaptation of the *Communication-Human Information Processing* model to end-user security, and from Rogers' *Diffusion of Innovations* model [61] of how messages spread in a social network about a new idea.

We used the literature from Das et al. on security sensitivity as a main source of items to test for inclusion in SA-6.

2.3. User Acceptance Theories and Models

Davis et al.'s *Technology Acceptance Model* [25,26] (TAM) was among the first to integrate users' psychology along with design characteristics to explain the degree to which users accept and use a computational technology. In their model, a user's attitude toward using a system (affective response) after encountering its design features (external stimulus) is mediated through their perceptions of the system's usefulness and ease of use (cognitive response) to determine their actual system use (behavioral response).

The TAM in turn builds on a psychological framework originated by Fishbein & Azjen, the *Theory of Reasoned Action* [37] (TRA). The basic theory posits that behavior is preceded by intention, with intention in turn determined by an individual's attitude toward the behavior (positive or negative) along with subjective norms, e.g. whether the behavior is seen as appropriate in context or socially acceptable. Azjen's related *Theory of Planned Behavior* [3] added a third determinant of behavior intention, the individual's perception of behavioral control; he also noted the importance of *actual* behavioral control in moderating intention and perceived control, as no one can act if they are not able to do. Venkatesh incorporated these factors in his
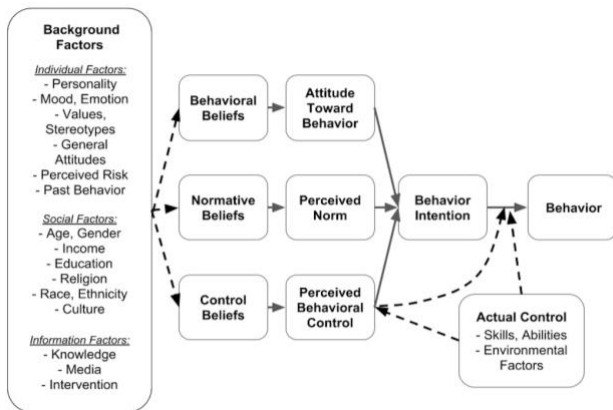
Figure 1: The Theory of Reasoned Action (TRA)

work with Davis and others to update the TAM as the *Unified Theory of the Acceptance and Use of Technology* [71,72].

Based on this literature on user behaviors, we incorporated measures of other concepts beyond attitude that we theorized would relate with it, such as privacy, self-efficacy and internet know-how, and also individual measures by which SA-6 would be expected to vary, such as past experience of security breaches, age, and socioeconomic status.

2.4. Security Behavior Intentions Scale

The current state of the art for quantifying users' thinking about security practices is the Security Behavior Intentions Scale [32,33] (SeBIS). Its asks about intended user behavior in four areas: device securement, updates, password management, and proactive awareness. SeBIS is not worded as a traditional intention survey – instead of "I intend" statements, it measures intention by asking respondents for their frequency from "Never" to "Always" of such active statements as "I use a password/passcode to unlock my laptop or tablet" – but it has been extensively validated [32,64] and cited by other usable security researchers [31,60]. Its short length makes it practical to include in a larger survey or battery of psychological tests, or to administer during a lab experiment.

However, SeBIS is not a measure of attitudes. Its 16 items are not designed to measure a user's beliefs or emotions about the included behaviors, nor to indicate whether they are attuned to social or situational norms around the behaviors. They do not measure the extent to which the user has the requisite awareness, perceived ability or relevant knowledge to perform the behavior. We see a need for a complementary self-report measure that more directly gets at people's security attitudes underlying their intentions and behavior. We also see a need for a measure that is not tied to technology-specific language, so that the measure retains validity as the security technology changes.

3. Consideration of Broader Impacts [77]

We believe a new psychometric scale for assessing a person's attitudes toward expert-recommended tools and

practices will be a net benefit to the usable security field and to humanity. While the potential for abuse of such technologies has become recently prominent [40], we have also noted the significant impact to world events from human lapses in cybersecurity judgment [55,79]. SA-6 can help researchers and practitioners to design products in good faith that strengthen resilience to attacks.

4. Scale Development and Testing

In developing our self-report attitude measure, we relied on the guidance provided by sources such as Fowler [39], Hinkin et al. [46], Netemeyer et al. [53] and Dillman et al. [28], as well as our own experience and that of our colleagues. Briefly, we sought to measure whether the scale is reliable and valid through analyses of the measures in the literature that we identified that fit with the Theory of Reasoned Action and with security sensitivity literature. We look at the convergence of our scale with these related scales and how the scale varies according to how related measures vary. We iterated in stages to develop a suitable list of candidate items and a survey for testing these items. All pilot work was conducted in accordance with the policies and approval of our Institutional Research Board, as required by U.S. National Science Foundation grant no. CNS-1704087.

4.1. Item Generation

A common best practice in psychometric scale development is to generate a long list of possible statements that could measure the underlying construct, in order to increase the chances of developing a sufficiently reliable and valid scale [28,39,46,53]. We generated 200+ items to be rated on a 5-point Likert-type agreement scale (1=*Strongly disagree*, 5=*Strongly agree*). We based the wordings of these items primarily in empirical research by Das et al., but also borrowed some wordings from SeBIS, from other work in usable security and psychology [1,15,16,27,29,41,45,58,66] and from our experiences. We conducted multiple rounds of review of these items, first with experts in usable security who checked the items for content adequacy, then with several nonexperts in security research, whose feedback was used to ensure the survey protocol was clear, unambiguous and easily understandable, in line with common best practices and [28,39,46,53]. These reviews pared our list of items to 60 for online testing.

4.2. Survey Development

Another best practice for scale development is to collect variables that are thought to relate with or to vary with the construct, to test if they relate with and vary with the scale to a similar extent [28,39,46,53]. We used the Theory of Reasoned Action [37] as our guide to which constructs we should include measures of in our survey instrument so that we could test for our scale's degree of associations and variances with these constructs. We referred to prior work such as [32,33] for identifying measures for *need for cognition* [14], *consideration of future consequences* [68],

risk perception and *risk taking* [11], and *impulsiveness* [67]. We incorporated measures of *internet* and *technical know-how* [48], *computer confidence* [38], and *web-oriented digital literacy* [44], along with general and social *self-efficacy* [66] and the "Big Five" *personality factors* [42]. We included two measures of *privacy concerns* [13,51], a subjective norm strongly related to security beliefs [50,54]. To help test for expected variances in security sensitivity, we asked participants the extent to which *they*, or *someone close to them*, *had been a victim of a security breach*, as well as how much they had *heard or read about security breaches during the past year*. See Section 12.1 for the list of measures included in this report.

Our questionnaire was piloted on Amazon Mechanical Turk with three Masters-qualified workers. Each provided their feedback and suggestions for improving the survey experience via an open-ended text box added at the end. The pilot survey designs ranged between 18 and 24 pages in length as we experimented with how best to break the items among pages and provide clear instructions on each page. The survey was structured to front-load the most important questions, namely the candidate items and the SeBIS questions, because of concern for answers being affected by response fatigue due to the survey length. After the third iteration received entirely positive feedback from a Masters worker, we submitted a formal modification to our Institutional Research Board for review of our survey and research design and exemption from human subjects regulation under U.S. 45 CFR 46.
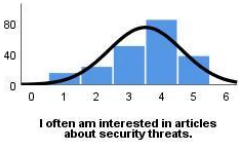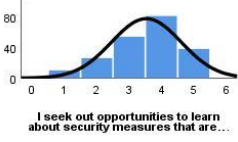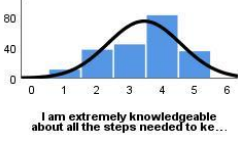
4.3. Finalizing Candidate Items

A third best practice for scale development is to collect an initial batch of data to determine which candidate scale items meet minimum standards for response variance and for factor and reliability statistics [28,39,46,53]. We administered 60 candidate items on five pages of 12 items each, along with 16 pages of measures theorized to relate to our survey, in a first round of MTurk research in November-December 2017. We advertised this as a "Survey on attitudes & behaviors among computer users (~30 minutes)" and requested U.S. residents age 18 or older. Using a base rate of $10/hour and a median pilot duration of 24 minutes, we compensated participants with $5 per survey. The survey used one open-ended item asking participants to either mention other security measures they use or to write "None"; this was partly included as a check on attention (if left blank) and fraudulent responses (if nonsensical). As a precaution against workers taking the survey more than once under different IDs, we removed all but one response from an IP address and/or specific location.

We performed an exploratory factor analysis (EFA) and reliability analysis on the $N = 196$ completed and valid responses. After finding smaller-than-desired variance in some response distributions and in the alpha and total variance explained by items with high factor loadings, we decided to retain just 18 items without changes. We

Table 1: Sample statistics for scale finalizing, validation

N	Scale finalizing 478	Validity study 209
What is your age range?		
18-29	46.7%	20.6%
30-39	32.2%	18.7%
40-49	10.0%	23.0%
50-59	7.1%	21.5%
60 or older	4.0%	16.3%
What is your gender identity?		
Male	41.6%	41.6%
Female	57.7%	58.4%
Nonbinary or non-conforming	0.6%	0.0%
What is your level of education?		
Some high school	0.6%	0.0%
High school degree/equivalent	7.3%	32.5%
Some college/assoc./tech. deg.	28.7%	37.8%
Bachelor's degree	43.7%	15.3%
Graduate/professional degree	19.7%	14.4%
Are you a U.S. citizen?		
Yes	91.2%	98.1%
No	8.8%	1.9%
What is your yearly household income?		
Up to $25,000	24.5%	22.5%
$25,000 to $49,999	29.1%	24.9%
$50,000 to $74,999	18.8%	33.5%
$75,000 to $99,999	13.2%	9.1%
$100,000 or more	14.4%	10.0%
What is your employment status?		
Employed full time	(Not Asked)	42.1%
Employed part time		8.1%
Unemployed looking for work		9.6%
Unemployed not looking for work		8.6%
Retired		16.7%
Student		5.7%
Disabled		9.1%
How frequently or infrequently have you personally been the victim of a breach of security (e.g. hacking, viruses, theft of personal data)?		
Very infrequently	51.3%	39.7%
Infrequently	27.0%	29.2%
Neither infrequently or frequently	11.7%	18.2%
Frequently	8.2%	10.0%
Very frequently	1.9%	2.9%
How frequently or infrequently has someone close to you (e.g. spouse, family member or close friend) been the victim of a breach of security (e.g. hacking, viruses, theft of personal data)?		
Very infrequently	28.2%	28.7%
Infrequently	40.6%	34.4%
Neither infrequently or frequently	18.4%	23.9%
Frequently	11.7%	9.6%
Very frequently	1.0%	3.3%
How much have you heard or read during the last year about online security breaches?		
None at all	5.0%	7.2%
A little	32.4%	24.9%
A moderate amount	35.4%	38.8%
A lot	19.0%	21.1%
A great deal	8.2%	8.1%

Table 2: Final set of SA-6 items with factor loadings, alpha if item deleted, and histograms. Factor loadings well above .40 indicate strong relationships. Alpha above .70 indicates strong internal consistency of scale responses.

SA-6 scale items *(Principal Components Analysis; Overall alpha: .84)*	*Factor loading*	*Alpha if item deleted*	*Histograms* *(1=Strongly disagree, 5=Strongly agree)*
I seek out opportunities to learn about security measures that are relevant to me.	0.81	0.80	
I am extremely motivated to take all the steps needed to keep my online data and accounts safe.	0.78	0.81	
Generally, I diligently follow a routine about security practices.	0.77	0.81	
I often am interested in articles about security threats.	0.72	0.82	
I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.	0.71	0.83	
I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.	0.71	0.83	

generated 30 new items that used more extreme wordings to encourage a greater response distribution. After reviews similar to those in Section 4.1, a final list of 48 candidate items were deployed in an MTurk survey in February 2018; on these newly gathered N =339 responses, we performed several EFAs and reliability analyses and examined the item response distributions, factor loadings, factor alphas, and total variances explained to ensure that they displayed sufficient psychometric properties for further testing. The 48 candidate items and their sources are listed in Section 12.2.

4.4. Finalizing Scale Items

The next stage of scale development was to collect a sufficient number of responses from which to narrow the list of items to those that most clearly measured the security sensitivity construct [28,39,46,53]. To this end, in July-August 2018, we collected a third dataset on MTurk and a fourth dataset in a university-run online study pool, using very similar recruitment language and the same participant compensation as in Section 4.3. A chi-square analysis found that these datasets did not differ significantly by gender: $X^2(1, N = 475) = 2.95$, p = n.s. We conducted 10 pairwise comparisons of the datasets by age range, first correcting for possible compounded Type I error by conducting a Bonferroni procedure that adjusted alpha to $p < .005$. We did not find any pairwise comparisons by age to be statistically significant: overall $X^2(4, N=478)=11.42$, p = n.s. See Section 12.3 for chi-square statistics for age-level pairwise comparisons and for the pairwise comparisons by levels of education, income and breach-experience measures.

Based on the lack of significant differences by age or gender, we merged these to form one sample of $N=479$. This ensured a 5:1-to-10:1 ratio of observations to items for finalizing the scale, as recommended by [39,46,53]. See Table 1 for descriptive statistics for this sample.

We conducted a series of factor analyses and reliability assessment to identify the number of possible factors from scree plots and factor loadings; which factors explained at least 40% total variance in the sample and eigenvalues over 1.0; and which of these factors met a threshold Cronbach's alpha of .70. Finally, we tested the goodness-of-fit of each candidate factor structure by conducting a confirmatory factor analysis (CFA) to calculate fit statistics that are appropriate for a large sample [47]: the Comparative Fit Index (CFI), for which an acceptable fit is above .90 and a superior fit above .95, and the Standardized Root Mean Square Residual (SRMR), which should be below .08. We chose the first factor, which explained 64% of the sample variance with 6 items loading over 0.71 on this factor. These six items had a Cronbach's alpha equal to .88, demonstrating excellent internal reliability (well above the threshold of .70); and a CFI of 0.96 and SRMR of 0.03, demonstrating superior model fit. Section 12.4 displays the six item histograms, factor loadings and alpha if item deleted.

5. Validity Study in Census-tailored Panel

To test the reliability and validity of SA-6 outside of the MTurk and university study populations, we repeated our study in September 2018 with a U.S. Census-tailored panel filled by Qualtrics ($N=209$). We again targeted compensation at $5 per response, however this was not handled by us directly; Qualtrics worked with its third-party providers to provide sufficient payment in forms such as reward points.

We dropped survey measures that were less central to this report, reordered items so that the demographics questions were asked first to fill the survey quotas, added a question about employment status, and (beyond the open-ended item noted in Section 4.3) added a second attention check: "*We use this question to discard the answers of people who are not reading the questions. Please select "51% to 75% of the*

time" (option 4) to preserve your answers." The panel received a sufficient number of responses in all variable categories to complete the statistical picture for this report. See Table 1 for descriptive statistics for this sample.

As before, we examined the items' statistical properties and confirmed the factor structure in this smaller sample. SA-6 was found to explain 56% of total sample variance, with a Cronbach's alpha of .84, a CFI of 0.91, and an SRMR of 0.05. Table 2 displays the six item histograms, factor loadings and statistics for Cronbach's alpha if item deleted for SA-6. These demonstrate SA-6's solid factor structure, internal consistency and goodness of fit.

6. Convergent and Discriminant Validity

In the Census-tailored sample (*n*=209), we conducted a series of correlations and independent-samples t-tests to assess the degree to which security attitudes as measured by SA-6 converged with measures thought to relate with it (*convergent validity*) and varied as expected by categorical measures (*discriminant validity*), consistent with the Theory of Reasoned Action [37]. These tests support that the scale is measuring the concept that it claims to measure. We excluded some collected variables from validity tests because they did not meet a Cronbach's alpha of .70, which indicates they may include higher-than-acceptable random measurement error. Section 12.5 reports the Cronbach's alpha values for each observed measure.

6.1. Correlation with SeBIS

To examine convergent validity of SA-6, we first tested its statistical association with SeBIS, the field's standard self-report measure of security behavior intention. We did this because attitude is a direct antecedent of behavior intention in the Theory of Reasoned Action [37]. Using a Spearman correlation, we found SA-6 to be significantly positively associated with SeBIS (*r* =.54, *p* < .01). Using linear regression, we found that SA-6 explained 28% of the variance in SeBIS (*p*<.01). This result is consistent with longstanding psychological evidence of the relationship between attitudes and behavior intention [5,7,8,37,69,75] and demonstrates SA-6's convergent validity.

6.2. Correlations with Other Interval Variables

To further examine the convergent validity of SA-6, we looked at its statistical association with measures of perceived behavioral control, perceived norms (chiefly privacy) and individual cognitive and risk styles. We collected and tested these measures because these were used in validity testing for SeBIS [32–34] since they represent closely associated concepts. These concepts are also components of the Theory of Reasoned Action [37].

We found expected significant associations among SA-6 and psychological indicators of perceived behavioral control (Barratt Impulsiveness Scale *r*= -.180, *p*<.01; General Self-Efficacy, *r*=.208, *p*<.01; Social Self-Efficacy, *r*=.363, *p*<.01); indicators of privacy concerns (Internet Users'

Informational Privacy Concerns *r*=.390, *p*<.01; Privacy Concerns Scale (*r*=.382, *p*<.01); and two indicators of cognition and risk styles (Need for Cognition *r*=.258, *p*<.01, and the Domain-Specific Risk Taking Health/Safety subscale for risk perception: *r*=.175, *p*<.05). We did not find a significant association for SA-6 with the Consideration of Future Consequences scale, with the General Decision-Making Styles subscales for dependence and avoidance, or with the Domain-Specific Risk-Taking Health/Safety subscale for risk-taking propensity.

We found a significant association of SA-6 with the "Big Five" personality factor of Extraversion (*r*=.175, *p*<.05). We included the Big 5 because personality is a background component of the Theory of Reasoned Action [37].

We found an expected significant positive correlation with the Kang Internet Know-How scale (*r*=.542, *p*<.01) and with two related scales, one for confidence in using computers (*r*=.280, *p*<.01) and the other for web-oriented digital literacy (*r*=.503, *p*<.01). We included these measures because information, skill and ability are key components of the Theory of Reasoned Action [37].

6.3. Variances by Categorical or Ordinal Variables

To examine discriminant validity, we tested whether SA-6 varied significantly as a function of personal experiences of and media exposure to security breaches, and by age, gender and socioeconomic status. We included these measures because social and informational measures are antecedents of attitude in the Theory of Reasoned Action [37] and previous work has found a connection between demographics and security concern [50,54].

For each type of experience with security breaches, we recoded the 5-level variable responses into 2 levels (low experience (1-2) vs. high experience (3-5)) and conducted independent-samples *t*-tests on the census-weighted sample. This analysis let us look at how SA-6 varied for people with low versus high levels of experience with security breaches (see Table 3 for a summary). SA-6 was significantly higher for participants with higher self-reported frequency of participants falling victim to a security breach, higher self-reported frequency of their close friends or relatives falling victim. and by the amount they had heard or seen about security breaches in the past year.

For demographics, we found a statistically significant difference in SA-6 by age group and gender, with a higher score for older participants and men. SA-6 scores were also higher for participants who attended college and those whose yearly household income exceeded the 2018 U.S. poverty level of $25,100 for a family of four [80]. These differences correspond with differences observed in other studies on cybersecurity opinions and knowledge [50,54]. We did not find a significant difference in SA-6 by citizenship or employment status, with the exception of "Employed full-time" (*M*=3.85, *SD*=.75) vs. "Unemployed looking for work" (*M*=3.24, *SD*=.76, *F*(6,202)=2.59, *p*<.05).

Table 3: SA-6 Mean, standard deviation, and test of difference for security breach experience and demographic variables

	SA-6 Mean (SD)		t(df), p
Security breach experience frequency			
	Low	*High*	
Themselves falling victim to a security breach	3.56 (.78)	4.13 (.58)	t(41.46) = -4.54, p<.001
Close friends or relatives falling victim to a breach	3.57 (.76)	4.10 (.74)	t(207)= -3.40, p<.005
Heard about security breaches in the past year	3.35 (.80)	3.77 (.74)	t(207)=-3.77, p<.001).
Demographic differences			
	18-39	*40 +*	
Age group	3.40 (.81)	3.69 (.76)	t(207)= -2.172, p<.05
	Male	*Female*	
Gender	3.77 (.71)	3.53 (.81)	t(198.38)= 2.19, p<.05
	No college	*Attend. college*	
College attendance	3.42 (.79)	3.73 (.76)	t(207)=-2.76, p<.01
	Below $25K	*Above $25K*	
Income level	3.30 (.71)	3.73 (.77)	t(207)=-3.42, p<.005

6.4. Variances by Participants' Recall of Security Actions

We were able to go one step further than the authors of SeBIS and ask respondents whether, in the past week, they had at least once taken an expert-recommended action for device securement, updating, password management or proactive awareness. The item wordings were drawn from those of SeBIS in those areas, with a response set of "Yes/No/Not Sure/NA" and these instructions: "*For the following statements, please select the response that best represents your recall of what actions you have taken in the past week. Please select "I'm not sure" if you don't know the answer. Please select "NA" if the statement does not apply to you*." We excluded NA responses from the item-level analysis. We recoded the remaining 3-level variable responses into 2 levels (Yes (1) vs. No or Not Sure (2-3)) and conducted independent-samples *t*-tests on the census-weighted sample. This analysis let us look at how SA-6 varied for people who did vs. did not recall performing these certain SeBIS-derived security actions. We found SA-6 to vary significantly by the answers to all but one item. This further demonstrates discriminant validity. See Table 4 for item statistics.

We then conducted a series of binary logistic regressions to compare predicted outcomes by (a) models that combined SA-6 with SeBIS as predictors, (b) models using SeBIS without SA-6 as a predictor, and (c) models using only a constant as a predictor (to indicate baseline performance

without SeBIS). Results indicated that there was a significant association among SA-6, SeBIS and item responses. This improved the performance of models for three items: "*In the past week, I have downloaded and installed at least one available update for my computer's operating system within 24 hours of receiving a notification that it was available*" ($X^2(2) = 42.49$, $p < .001$), boosting the model's percentage of correctly classified responses to (a) 68.1% vs. (b) 67.5% for SeBIS without SA-6 and (c) 58.6% for the constant alone; "*In the past week, I have verified at least once that I am running antivirus software that is fully updated*" ($X^2(2) = 43.06$, $p < .001$), boosting the model's percentage of correctly classified responses to (a) 65.9% vs. (b) 64.9% for SeBIS without SA-6 and (c) 52.7% for the constant alone; and "*In the past week, I have used a password/passcode at least once to unlock my tablet*" ($X^2(2) = 39.65$, $p < .001$), boosting the model's percentage of correctly classified responses to (a) 77.2% vs. (b) 76.7% for SeBIS without SA-6 and (c) 70.5% for the constant alone. See Section 12.5 for the classification tables for each item's logistic regressions.

The pseudo R-squared value generated with logistic regressions cannot be said, as with a linear regression R-squared value, to show the variance accounted for by the model. In order to use a linear regression model to calculate this variance explained, we transformed the recalled security action items into one interval variable by computing an average of the scores of the nine items that were found to vary significantly by their SA-6 score. The Cronbach's alpha for this compound measure was .77, comfortably above the threshold of .70 we used to exclude measures from validity tests. When we combined SA-6 with SeBIS as a predictor in this model, SA-6 lifted its ability to explain the variance in this compound measure from 23.5% to 24.3% ($p<.001$, $r=.493$). A Spearman correlation also found significant associations (SA-6 with recalled security actions: $r=.398$, $p<.001$; SeBIS with recalled security actions: $r=.541$, $p<.001$). These statistics suggest that SeBIS is a partial mediator of SA-6's influence on the recalled security actions measure, as predicted by the Theory of Reasoned Action's model of attitude helping to determine behavior through the mediation of intention [37].

7. Discussion and Future Work

Our careful scale development process gives us confidence that SA-6 has demonstrated construct validity, internal consistency and reliability, goodness-of-fit, and convergent and discriminative validity. We conducted several tests of our generated items to determine which were most suitable for our scale, then visually inspected the response distributions and conducted factor and reliability analyses to determine which mix of items are the best fit for a short self-report measure of security attitudes. We found SA-6 to correlate as expected with privacy and other theorized concepts such as self-efficacy, and to vary by factors such as exposure to breaches and demographics.

Table 4: Means, standard deviations, and T statistics for participants' answers to recalled security action statements

Participant's recalled security action	*Yes*		*No or Not Sure*				*NA*
	M	*SD*	*M*	*SD*	*t*	*df*	*%*
In the past week, I have changed a password for at least one of my online accounts.	3.84	0.77	3.39	0.74	4.20****	200	3.3
In the past week, I have downloaded and installed at least one available update for my computer's operating system within 24 hours of receiving a notification that it was available.	3.95	0.73	3.40	0.75	5.11****	189	8.6
In the past week, I have left my laptop or desktop computer unlocked at least once when I walked away from it.	3.49	0.81	3.84	0.70	2.95***	184	11.0
In the past week, I have submitted information to a website at least once without first verifying that it would be sent securely.	3.64	0.76	3.68	0.78	(n.s.)	194	6.2
In the past week, I have used a password/passcode at least once to unlock my tablet.	3.71	0.80	3.40	0.68	2.56*	191	7.7
In the past week, I have used at least one password that contains 10 or more characters.	3.77	0.75	3.39	0.77	3.43***	203	1.9
In the past week, I have used the exact same password for at least two online accounts.	3.49	0.82	3.82	0.69	2.95***	200	3.3
In the past week, I have verified at least once that I am running antivirus software that is fully updated.	3.82	0.69	3.49	0.82	3.03***	184	1.9
In the past week, I have verified that at least one app or software program that I use is fully updated.	3.80	0.76	3.38	0.75	3.84****	200	3.3
In the past week, I have verified the URL of at least one internet link that I received in email before deciding whether to click on it.	3.94	0.64	3.45	0.77	4.71****	189	8.6

*Sig. at .05 level ** Sig. at .01 level ***Sig. at .005 level ****Sig. at .001 level

7.1. Using SA-6 to Measure Security Attitudes

SA-6 will be useful to researchers and practitioners who need a reliable and valid method to systematically assess and compare user attitudes about the use and adoption of expert-recommended security tools and practices. SA-6 is easily administered via an online questionnaire in a web browser or on paper, and it also is shorter than measures such as the 31-item Personal Data Attitude measure for adaptive cybersecurity [2] or 63-item Human Aspects of Information Security Questionnaire [56]. SA-6 and its individual subscales will help to answer research questions such as: *To what degree does a user report the awareness, motivation or knowledge to perform recommended security actions? How positive or negative is her or his attitude? To what degree is she or he likely to consider adopting more-secure tools? How does her or his score compare with a group average?*

SA-6's usefulness is not constrained to research motivated by the Theory of Reasoned Action/Theory of Planned Behavior or the Technology Acceptance Models. Our measure could contribute a valuable tool to research motivated by *Self-Determination Theory* [63], helping to assess intrinsic motivation to use recommended security tools and practices. It also could be used for approximating threat appraisal in adaptions to usable security of *Protection Motivation Theory* [52,62] and for pre- and post-study evaluations in cybersecurity education research [19].

7.2. Using SA-6 to Predict Security Behaviors

An open question in psychology is the degree to which attitude, intention and other factors directly determine behavior. Sutton's 1998 meta-analyses [69] showed that TRA and TPB explain on average between 40% and 50% of intention variance, with the rest accounted for by changes in factors such as volitional control and random variance. And Webb and Sheeran's 2006 meta-analyses [75] showed that across 47 experiments, a medium-to-large change in intention (d=0.66) led to a small-to-medium change in behavior (d=0.36). They conclude that "intentional control of behavior is a great deal more limited than previous meta-analyses of correlational studies have indicated."

Sutton notes a relevant distinction in this context between explanation and prediction. In his framing, explanation is a process of identifying what determines intentions and behavior and seeking how such factors combine, while prediction enables the targeting of interventions in spite of not understanding the full degree and nature of a behavior's determinants. An example Sutton gives of the latter is identification of people at high risk of developing a drinking problem, arguing that, despite not having a clear model of which factors combine to influence alcohol addiction, it is still a benefit to create predictive models of alcoholism risk in order to target an early intervention. Nevertheless, he writes, a causal model that sheds light on what factors influence drinking in certain individuals may make it possible to extend the predictive model to similar problems and to avoid a "one size fits all" solution that can better target interventions by differing nature and content.

Similarly, our results suggest to us that even given the moderate *r* values shown in our correlation analyses, SA-6 is likely to add valuable predictive weight with SeBIS in computational modeling of who is likely to act on security recommendations and who is open to changing their security behavior. We see both scales as useful for future research into the degree to which security sensitivity along with security behavior intention can explain which architecture choices or "nudges", as suggested by Egelman & Peer

[34,35], and Redmiles et al. [59] might best improve security choices by users with specific attitude and intention profiles, thus helping the field move beyond a blanket approach to interventions. We also are pursuing work to compare SA-6 with two other scales we are developing to measure users' concernedness with and resistance to changing their security behaviors, as part of a new causal model and framework.

7.3. Using SA-6 vs. SeBIS to Identify Target Interventions

We see utility for SA-6 in measuring a user's readiness for educational interventions. Broadly, SA-6 identifies whether the user is a good candidate for interventions of two types: (1) to raise awareness of the general need for using expert-recommended tools and practices (*low SA-6*) or (2) to add to users' knowledge of how to use recommended tools and practices (*high SA-6*). An example of the first type of intervention might be playing a security awareness game, while an example of the second type would be taking part in a tutorial on creating strong but memorable passwords.

Conversely, we see SeBIS as offering specific utility in measuring a user's readiness for motivational interventions that (3) move them into the intention stage (*low SeBIS*) or (4) move them from intention into action and reinforce action (*high SeBIS*). An example of this third type of intervention would be a positive incentive program, such as rewards for 3, 15 and 30 days of consecutive use of a third-party password manager. An example of the fourth type would be reminders to act, such as context-aware notifications of a newly available software update, or negative incentives for nonaction, such as progressively annoying or persistent notifications for a software update that a user fails to install.

8. Limitations and Next Steps

Our project was conducted with U.S.-based populations age 18 or older using a lengthy, English-language, online questionnaire. More research will be needed to find support for SA-6's reliability and validity in populations of computer users outside the U.S. and/or when translated into other languages. The ability to generalize our results inside the U.S. is limited by our use of purposive, nonrandom sampling of the subpopulation of online survey-takers. Our use of online surveys as the only method of questionnaire administration may also have introduced common method bias, suggesting the need also to test the survey in other modes such as written and telephone versions.

All correlational research is inherently unable to prove causation. This work is only the first step toward finding support for a relationship among the variables in our study. Experimental research will be needed to investigate the hypothesis that changes in security sensitivity will lead to changes in security behavior intention and, ultimately, to changes in actual security behavior by end users. Additionally, we did not test for measurement noninvariance, which limits SA-6's usefulness for comparing groups. Finally, some items in SeBIS and in the

SeBIS-derived items in Table 4 are out of step with current security recommendations (*e.g.,* many experts now advise against forcing users to periodically change their passwords) and features in consumer systems (*e.g.,* many updates can now be downloaded and installed automatically). This limits the usefulness of SeBIS and these SeBIS-derived items for accurately measuring security intention and recalled actions.

However, we believe that SA-6 is a valid way to measure security attitudes for future studies and experiments relevant to cybersecurity. We are pursuing a second work that will allow for a side-by-side discussion of this scale with two others in development and provide support for a causal model and framework for targeting security interventions.

9. Conclusion

In this paper, we introduce and validate SA-6, a self-report measure of end-user security attitudes. Using principles of psychological scale development, we generated and finalized six items that (a) correspond to prior work on their face; that (b) pilot testers found to be unambiguous and easily answered; that (c) demonstrated sufficient response variance, and that (d) were found in factor and reliability analyses to demonstrate desired psychometric properties.

Via analyses of data from a U.S. Census-tailored survey panel, we found SA-6 to be significantly associated with a self-report measure of behavior intention and to exhibit expected variances by participants' recollections of recent security actions. We found SA-6 significantly associated with other measures of cognition and with measures of subjective norms, chiefly privacy, and perceived behavioral control, such as self-efficacy and internet know-how.

Our scale is a lightweight tool for researchers and practitioners to (1) quantify and compare end users' attitudes toward using recommended security tools and practices, and (2) improve predictive modeling of who will adopt such behaviors. The field of usable security will benefit from this systematic method for assessing a user's awareness, motivation, and knowledge of expert-recommended tools and practices. We hope our work helps improve understanding of end-user compliance with security recommendations and the identification of users who are susceptible to attacks and open to changing their behaviors.

10. Acknowledgments

11. References

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (December 1999), 40–46. DOI:https://doi.org/10.1145/322796.322806

[2] Joyce Hoese Addae, Michael Brown, Xu Sun, Dave Towey, and Milena Radenkovic. 2017. Measuring attitude towards personal data for adaptive cybersecurity. *Inf. Comput. Secur.* 25, 5 (October 2017), 560–579. DOI:https://doi.org/10.1108/ICS-11-2016-0085

[3] Icek Ajzen. 1991. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* 50, 2 (December 1991), 179–211. DOI:https://doi.org/10.1016/0749-5978(91)90020-T

[4] Icek Ajzen. 2001. Nature and Operation of Attitudes. *Annu. Rev. Psychol.* 52, 1 (2001), 27–58. DOI:https://doi.org/10.1146/annurev.psych.52.1.27

[5} Icek Ajzen, 2006. Behavioral Interventions Based on the Theory of Planned Behavior.

[6] Icek Ajzen and Martin Fishbein. 2000. Attitudes and the Attitude-Behavior Relation: Reasoned and Automatic Processes. *Eur. Rev. Soc. Psychol.* 11, 1 (January 2000), 1–33. DOI:https://doi.org/10.1080/14792779943000116

[8] Icek Ajzen and Thomas J Madden. 1986. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *J. Exp. Soc. Psychol.* 22, 5 (September 1986), 453–474. DOI:https://doi.org/10.1016/0022-1031(86)90045-4

[9] Sebastian Bamberg. 2003. How does environmental concern influence specific environmentally related behaviors? A new answer to an old question. *J. Environ. Psychol.* 23, 1 (March 2003), 21–32. DOI:https://doi.org/10.1016/S0272-4944(02)00078-6

[11] Ann-Renee Blais and Elke Weber. 2006. *A Domain-Specific Risk-Taking (DOSPERT) Scale for Adult Populations*. Social Science Research Network, Rochester, NY. Retrieved November 14, 2017 from https://papers.ssrn.com/abstract=1301089

[12] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. 2011. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Secur. Priv.* 9, 2 (March 2011), 18–26. DOI:https://doi.org/10.1109/MSP.2010.198

[13] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the Internet. *J. Am. Soc. Inf. Sci. Technol.* 58, 2 (January 2007), 157–165. DOI:https://doi.org/10.1002/asi.20459

[14] John T. Cacioppo, Richard E. Petty, and Chuan Feng Kao. 1984. The Efficient Assessment of Need for Cognition. *J. Pers. Assess.* 48, 3 (June 1984), 306–307. DOI:https://doi.org/10.1207/s15327752jpa4803_13

[15] Robert B. Cialdini. 2001. *Influence: science and practice* (4th ed ed.). Allyn and Bacon, Boston, MA.

[16] Robert B. Cialdini and Noah J. Goldstein. 2004. Social Influence: Compliance and Conformity. *Annu. Rev. Psychol.* 55, 1 (January 2004), 591–621. DOI:https://doi.org/10.1146/annurev.psych.55.090902.142015

[17] Lorrie Faith Cranor. 2008. A Framework for Reasoning About the Human in the Loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security* (UPSEC'08), 1:1–1:15. Retrieved September 21, 2018 from http://dl.acm.org/citation.cfm?id=1387649.1387650

[18] Jonas Dalege, Denny Borsboom, Frenk van Harreveld, Helma van den Berg, Mark Conner, and Han L. J. van der Maas. 2016. Toward a formalized account of attitudes: The Causal Attitude Network (CAN) model. *Psychol. Rev.* 123, 1 (2016), 2–22. DOI:https://doi.org/10.1037/a0039802

[19] M. Dark and J. Mirkovic. 2015. Evaluation Theory and Practice Applied to Cybersecurity Education. *IEEE Secur. Priv.* 13, 2 (March 2015), 75–80. DOI:https://doi.org/10.1109/MSP.2015.27

[20] Sauvik Das. 2017. Social Cybersecurity: Reshaping Security Through An Empirical Understanding of Human Social Behavior. *Dissertations* (May 2017). Retrieved from http://repository.cmu.edu/dissertations/982

[21] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The effect of social influence on security sensitivity. In *Proc. SOUPS*. Retrieved from https://pdfs.semanticscholar.org/cd64/4bceb458cfb63c16a86fdf0234c8cf54c004.pdf

[22] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2014. Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (CCS '14), 739–749. DOI:https://doi.org/10.1145/2660267.2660271

[23] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), 1416–1426. DOI:https://doi.org/10.1145/2675133.2675225

[24] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. *ACM CHI 2018 Conf. Hum. Factors Comput. Syst.* 1, 1 (2018), 2.

[25] Fred D. Davis. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Q.* 13, 3 (1989), 319–340. DOI:https://doi.org/10.2307/249008

[26] Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw. 1989. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Manag. Sci.* 35, 8 (August 1989), 982–1003. DOI:https://doi.org/10.1287/mnsc.35.8.982

[27] Carlo C. DiClemente, James O. Prochaska, and Michael Gibertini. 1985. Self-efficacy and the stages of self-change of smoking. *Cogn. Ther. Res.* 9, 2 (April 1985), 181–200. DOI:https://doi.org/10.1007/BF01204849

[28] Don A. Dillman, Jolene D. Smyth, and Leah Melani Christian. 2014. *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*. John Wiley & Sons.

[29] Paul Dourish, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Pers. Ubiquitous Comput.* 8, 6 (November 2004), 391–401. DOI:https://doi.org/10.1007/s00779-004-0308-5

[30] Alice H. Eagly and Shelly Chaiken. 1993. *The psychology of attitudes*. Harcourt Brace Jovanovich College Publishers, Orlando, FL, US.

[31] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '08), 1065–1074. DOI:https://doi.org/10.1145/1357054.1357219

[32] Serge Egelman, Marian Harbach, and Eyal Peer. 2016. Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), 5257–5261. DOI:https://doi.org/10.1145/2858036.2858265

[33] Serge Egelman and Eyal Peer. 2015. 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* (CHI '15), 2873–2882. DOI:https://doi.org/10.1145/2702123.2702249

[34] Serge Egelman and Eyal Peer. 2015. Predicting privacy and security attitudes. *ACM SIGCAS Comput. Soc.* 45, 1 (2015), 22–28.

[35] Serge Egelman and Eyal Peer. 2015. The Myth of the Average User: Improving Privacy and Security Systems through Individualization. In *Proceedings of the New Security Paradigms Workshop on ZZZ - NSPW '15*, 16–28. DOI:https://doi.org/10.1145/2841113.2841115

[36] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. 2015. A Study of Users' Experiences and Beliefs About Software Update Messages. *Comput Hum Behav* 51, PA (October 2015), 504–519. DOI:https://doi.org/10.1016/j.chb.2015.04.075

[37] Martin Fishbein and Icek Ajzen. 2010. *Predicting and changing behavior: The reasoned action approach*. Psychology Press, New York, NY, US.

[38] Gerry Fogarty, Patricia Cretchley, Chris Harman, Nerida Ellerton, and Nissam Konki. 2001. Validation of a questionnaire to measure mathematics confidence, computer confidence, and attitudes towards the use of technology for learning mathematics. *Math. Educ. Res. J.* 13, 2 (2001), 154–160.

[39] Floyd J. Fowler. 1995. *Improving Survey Questions: Design and Evaluation*. SAGE.

[40] McKenzie Funk. 2016. Opinion | Cambridge Analytica and the Secret Agenda of a Facebook Quiz. *The New York Times*. Retrieved March 19, 2018 from https://www.nytimes.com/2016/11/20/opinion/cambridge-analytica-facebook-quiz.html

[41] Shirley Gaw, Edward W Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail. (2006), 10.

[42] Samuel D Gosling, Peter J Rentfrow, and William B Swann. 2003. A very brief measure of the Big-Five personality domains. *J. Res. Personal.* 37, 6 (December 2003), 504–528. DOI:https://doi.org/10.1016/S0092-6566(03)00046-1

[43] Heesup Han and Hae Jin Yoon. 2015. Hotel customers' environmentally responsible behavioral intention: Impact of key constructs on decision in green consumerism. *Int. J. Hosp. Manag.* 45, (February 2015), 22–33. DOI:https://doi.org/10.1016/j.ijhm.2014.11.004

[44] Eszter Hargittai. 2005. Survey Measures of Web-Oriented Digital Literacy. *Soc. Sci. Comput. Rev.* 23, 3 (August 2005), 371–379. DOI:https://doi.org/10.1177/0894439305275911

[45] Cormac Herley. 2009. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop* (NSPW '09), 133–144. DOI:https://doi.org/10.1145/1719030.1719050

[46] Timothy R. Hinkin, J. Bruce Tracey, and Cathy A. Enz. 1997. Scale Construction: Developing Reliable and Valid Measurement Instruments. *J. Hosp. Tour. Res.* 21, 1 (February 1997), 100–120. DOI:https://doi.org/10.1177/109634809702100108

[47] Daire Hooper, Joseph Coughlan, and Michael Mullen. Structural Equation Modelling: Guidelines for Determining Model Fit. 11.

[38] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My data just goes everywhere:" User mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*, 39–52.

[49] Stephen J. Kraus. 1995. Attitudes and the Prediction of Behavior: A Meta-Analysis of the Empirical Literature. *Pers. Soc. Psychol. Bull.* 21, 1 (January 1995), 58–75. DOI:https://doi.org/10.1177/0146167295211007

[50] Mary Madden and Lee Rainie. 2015. Americans' Attitudes About Privacy, Security and Surveillance | Pew Research Center. Retrieved February 28, 2019 from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

[51] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Inf. Syst. Res. Linthicum* 15, 4 (December 2004), 336–355.

[52] Philip Menard, Gregory J. Bott, and Robert E. Crossler. 2017. User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *J. Manag. Inf. Syst.* 34, 4 (October 2017), 1203–1230. DOI:https://doi.org/10.1080/07421222.2017.1394083

[53] Richard G. Netemeyer. 2003. *Scaling procedures : issues and applications*. Sage Publications,.

[54] Kenneth Olmstead and Aaron Smith. 2017. Americans and Cybersecurity. *Pew Research Center: Internet, Science & Tech*. Retrieved November 6, 2017 from http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

[55] Will Oremus. 2016. "Is This Something That's Going to Haunt Me the Rest of My Life?" *Slate*. Retrieved September 17, 2018 from http://www.slate.com/articles/technology/future_tense/2016/12/an_interview_with_charles_delavan_the_it_guy_whose_typo_led_to_the_podesta.html

[56] Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies.

Comput. Secur. 66, (May 2017), 40–51. DOI:https://doi.org/10.1016/j.cose.2017.01.004

[57] Sandy Kristin Piderit. 2000. Rethinking Resistance and Recognizing Ambivalence: A Multidimensional View of Attitudes Toward an Organizational Change. *Acad. Manage. Rev.* 25, 4 (October 2000), 783–794. DOI:https://doi.org/10.5465/amr.2000.3707722

[58] J. O. Prochaska and W. F. Velicer. 1997. The transtheoretical model of health behavior change. *Am. J. Health Promot. AJHP* 12, 1 (October 1997), 38–48.

[59] Elissa M. Redmiles, John P. Dickerson, Krishna P. Gummadi, and Michelle L. Mazurek. 2018. Equitable Security: Optimizing Distribution of Nudges and Resources. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (CCS '18), 2270–2272. DOI:https://doi.org/10.1145/3243734.3278507

[60] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (CCS '16), 666–677. DOI:https://doi.org/10.1145/2976749.2978307

[61] Everett M. Rogers. 2010. *Diffusion of Innovations, 4th Edition*. Simon and Schuster.

[62] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change1. *J. Psychol.* 91, 1 (September 1975), 93–114. DOI:https://doi.org/10.1080/00223980.1975.9915803

[63] Richard M. Ryan and Edward L. Deci. 2000. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *Am. Psychol.* 55, 1 (2000), 68–78. DOI:https://doi.org/10.1037//0003-066X.55.1.68

[64] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17), 2202–2214. DOI:https://doi.org/10.1145/3025453.3025926

[65] Susanne G. Scott and Reginald A. Bruce. 1995. Decision-Making Style: The Development and Assessment of a New Measure. *Educ. Psychol. Meas.* 55, 5 (October 1995), 818–831. DOI:https://doi.org/10.1177/0013164495055005017

[66] Mark Sherer, James E. Maddux, Blaise Mercandante, Steven Prentice-Dunn, Beth Jacobs, and Ronald W. Rogers. 1982. The Self-Efficacy Scale: Construction and Validation. *Psychol. Rep.* 51, 2 (October 1982), 663–671. DOI:https://doi.org/10.2466/pr0.1982.51.2.663

[67] Matthew S. Stanford, Charles W. Mathias, Donald M. Dougherty, Sarah L. Lake, Nathaniel E. Anderson, and Jim H. Patton. 2009. Fifty years of the Barratt Impulsiveness Scale: An update and review. *Personal. Individ. Differ.* 47, 5 (October 2009), 385–395. DOI:https://doi.org/10.1016/j.paid.2009.04.008

[68] Alan Strathman, Faith Gleicher, David S. Boninger, and Scott Edwards. 1994. *The Consideration of Future Consequences: Weighing Immediate and Distant Outcomes of Behavior*. DOI:https://doi.org/10.1037/0022-3514.66.4.742

[69] Stephen Sutton. 1998. Predicting and Explaining Intentions and Behavior: How Well Are We Doing? *J. Appl. Soc. Psychol.* 28, 15 (August 1998), 1317–1338. DOI:https://doi.org/10.1111/j.1559-1816.1998.tb01679.x

[70] M. Tischer, Z. Durumeric, S. Foster, S. Duan, A. Mori, E. Bursztein, and M. Bailey. 2016. Users Really Do Plug in USB Drives They Find. In *2016 IEEE Symposium on Security and Privacy (SP)*, 306–319. DOI:https://doi.org/10.1109/SP.2016.26

[71] Viswanath Venkatesh and Fred D. Davis. 2000. A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Manag. Sci.* 46, 2 (2000), 186–204.

[72] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. User Acceptance of Information Technology: Toward a Unified View. *Manag. Inf. Syst. Q.* 27, 3 (2003), 5.

[73] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10), 11:1–11:16. DOI:https://doi.org/10.1145/1837110.1837125

[74] Rick Wash, Emilee Rader, and Ruthie Berman. 2016. Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. *USENIX Symp. Usable Priv. Secur.* (2016), 15.

[75] Thomas Llewelyn Webb, Paschal Sheeran, Thomas L. Webb, and Paschal Sheeran. 2006. Does changing behavioral intentions engender behavioral change? A meta-analysis of the experimental evidence. In *at PENNSYLVANIA STATE UNIV on September 19, 2016adh.sagepub.comDownloaded from Zigarmi and Nimon 15*, 249–268.

[76] G. L. Zimmerman, C. G. Olsen, and M. F. Bosworth. 2000. A "stages of change" approach to helping patients change behavior. *Am. Fam. Physician* 61, 5 (March 2000), 1409–1416.

[77] 2018. It's Time to Do Something: Mitigating the Negative Impacts of Computing Through a Change to the Peer Review Process. *ACM FCA*. Retrieved September 17, 2018 from https://acm-fca.org/2018/03/29/negativeimpacts/

[78] 2018 Data Breach Investigations Report. *Verizon Enterprise Solutions*. Retrieved April 13, 2018 from http://www.verizonenterprise.com/verizon-insights-lab/dbir/

[79] The Perfect Weapon: How Russian Cyberpower Invaded the U.S. - The New York Times. Retrieved September 17, 2018 from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

[80] 2018 Federal Poverty Level Guidelines (FPL): 2018 LIS Qualifications and Benefits. Retrieved February 22, 2019 from https://q1medicare.com/q1group/MedicareAdvantagePartD/Blog.php?blog=2018-Federal-Poverty-Level-Guidelines--FPL---2018-2019-LIS-Qualifications-and-Benefits&blog_id=674&category_id=8

12. Appendices

12.1. Table of Measures Used in this Report

Measures used in this report	Rationale for including
SeBIS scale, 16 items [33]	Test correlation with SA-6
Recalled Security Actions, 10 items	Test variances with SA-6
Internet Know-How, 9 items [48]	Test correlation with SA-6
Technical Know-How, 9 items [48]	Test correlation with SA-6
IUIPC scale, 10 items [51]	Test correlation with SA-6
Frequency of falling victim to a security breach, 2 items *	Test variances with SA-6
Amount heard or seen about security breaches, 1 item *	Test variances with SA-6
Whether respondent's security behavior is influenced by other factors or strategies, 1 item	Doubles as attention check; participants directed to leave an answer or type in "None."
Barratt Impulsiveness Scale, 30 items [67]	Test correlation with SA-6
Privacy Concern Scale, 16 items [13]	Test correlation with SA-6
Ten-Item Personality Inventory, 10 items [42]	Test correlation with SA-6
General Self-Efficacy scale, 11 items [76]	Test correlation with SA-6
Social Self-Efficacy scale, 5 items [76]	Test correlation with SA-6
Confidence in Using Computers, 12 items [38]**	Test correlation with SA-6
Web-Oriented Digital Literacy, 25 items [44]***	Test correlation with SA-6
Need for Cognition scale, 18 items [14]	Test correlation with SA-6
GDMS Avoidance and Dependence subscales, 10 items [65]	Test correlation with SA-6
DoSpeRT Health/Safety subscales, 12 items [11]	Test correlation with SA-6
Consideration of Future Consequences scale, 12 items [68]	Test correlation with SA-6
Age range, 1 item ****	Test variances in SA-6
Gender, 1 item ****	Test variances in SA-6
Level of formal education, 1 item ****	Test variances in SA-6
Household income level, 1 item ****	Test variances in SA-6
Employment status, 1 item	Test variances in SA-6

*reworded from IUIPC survey **reworded item 12 from original scale ***cut down from 43 items in original scale ****worded to be comparable with Pew surveys

12.2. List of Candidate Items for Scale Finalizing

The following is the selected list of n=48 candidate items for SA-6 (chosen items are shaded), along with the sources of the items. These were deployed in questionnaires on Amazon Mechanical Turk, the university-run study pool and to the Qualtrics U.S. Census-tailored panel.

Candidate items (n=48) analyzed for scale	Source
A security breach, if one occurs, is not likely to cause significant harm to my online identity or accounts.	[1,20,21,23]
Generally, I am aware of existing security threats.	[20–23]
Generally, I am willing to spend money to use security measures that counteract the threats that are relevant to me.	[21,45]
Generally, I care about security and privacy threats.	[20–23]
Generally, I diligently follow a routine about security practices.	[author generated]
Generally, I know how to figure out if an email was sent by a scam artist.	[20]
Generally, I know how to use security measures to counteract the threats that are relevant to me.	[20–23]
Generally, I know which security threats are relevant to me.	[20–23]
Generally, I want to use measures that can counteract security and privacy threats.	[20–23]
I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.	[15,21]
I always trust experts' recommendations about security measures (such as using unique passwords or a password manager, installing recommended software updates, etc.).	[15,21]
I am confident that I am taking the necessary steps to keep my online data and accounts safe.	[20–23]
I am confident that I can change my security behaviors, if needed, to protect myself against threats (such as phishing, computer viruses, identity theft, password hacking) that are a danger to my online data and accounts.	[76]
I am confident that I could change my security behaviors if I decided to.	[76]
I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.	[20–23]
I am extremely knowledgeable about how to take the necessary steps to keep my online data and accounts safe.	[20–23]
I am extremely knowledgeable about which security threats (such as phishing, computer viruses, malware, password hacking) are a danger to my online data and accounts.	[20–23]
I am extremely motivated to take all the steps needed to keep my online data and accounts safe.	[20–23]
I am extremely well aware of existing security threats (such as phishing, computer viruses, identity theft, password hacking).	[20–23]
I am extremely well aware of the necessary steps that I can take to counteract security threats (such as phishing, computer viruses, identity theft, password hacking).	[20–23]
I am too busy to put in the effort needed to change my security behaviors.	[21,29]

I care very much about the issue of security threats (such as phishing, computer viruses, identity theft, password hacking).	[20–23]
I dread that using recommended security measures will backfire on me (such as forgetting a needed password, updated software becoming unusable, etc.).	[21,45]
I feel guilty when I do not use recommended security measures (such as by reusing passwords, putting off software updates, etc.).	[21]
I generally am aware of existing security measures that I can use to counteract security threats.	[20–23]
I generally am aware of methods to send email or text messages that can't be spied on.	[20–23]
I have much bigger problems than my risk of a security breach.	[21,29]
I need to change my security behaviors to improve my protection against security threats (such as phishing, computer viruses, identity theft, password hacking).	[20,76]
I often am interested in articles about security threats.	[24]
I seek out opportunities to learn about security measures that are relevant to me.	[21]
I usually will not use security measures if they are inconvenient.	[20–23]
I usually will not use security measures unless I am forced to.	[20–23]
I want to change my security behaviors in order to keep my online data and accounts safe.	[20,76]
I want to change my security behaviors to improve my protection against threats (such as phishing, computer viruses, identity theft, password hacking) that are a danger to my online data and accounts.	[20,76]
I worry that I'm not doing enough to protect myself against threats (such as phishing, computer viruses, identity theft, password hacking) that are a danger to my online data and accounts.	[20,62]
It is a lost cause to take all the steps needed to keep my online data and accounts safe.	[author generated]
It is important for me to change my security behaviors to improve my protection against security threats (such as phishing, computer viruses, identity theft, password hacking).	[20,76]
It is not possible for me to do more than I already am to counteract security threats (such as phishing, computer viruses, identity theft, password hacking) that are a danger to my online data and accounts.	[author generated]
It's a sign of paranoia to use numerous security measures to protect against threats.	[21,41]
It's a sign of paranoia to use recommended security measures (such as using unique passwords or a password manager, installing recommended software updates, etc.).	[21,41]
My current lapses in using security measures are harmless.	[1,21]
My own actions can make a significant difference in keeping my online data and accounts safe.	[10]
Oftentimes, as soon as I discover a security problem, I report it to someone who can fix it.	[33]
Oftentimes, I am running on "automatic pilot" when I sift through my email and text messages.	[author generated]

Oftentimes, I will check that my anti-virus software has been regularly updating itself.	[33]
The exposure of my online data and accounts in a security incident, if one occurs, would be a significant problem for me.	[author generated]
The theft of my online data or accounts in a security breach, if one occurs, would be a significant problem for me.	[author generated]
There are good reasons why I do not take the necessary steps to keep my online data and accounts safe.	[21]

12.3. Pairwise Comparisons for MTurk and University Samples

The following table contains the chi-square statistics for all of the age-level pairwise comparisons (*1=18-29, 2=30-39, 3=40-49, 4=50-59, 5=60 or older; adj. p <.005*). No pairwise comparisons were statistically significant.

Pair	N	df	X^2	p
1 vs. 2	377	1	2.88	(n.s.)
1 vs. 3	271	1	2.39	(n.s.)
1 vs. 4	257	1	6.44	(n.s.)
1 vs. 5	242	1	1.26	(n.s.)
2 vs. 3	202	1	0.18	(n.s.)
2 vs. 4	188	1	2.48	(n.s.)
2 vs. 5	173	1	3.41	(n.s.)
3 vs. 4	82	1	1.10	(n.s.)
3 vs. 5	67	1	3.62	(n.s.)
4 vs. 5	53	1	6.86	(n.s.)

The following table contains the chi-square statistics for all of the education-level pairwise comparisons (*1=Some high school, 2=High school degree or equivalent, 3=Some college, technical degree or associate's degree, 4=Bachelor's degree, 5=Graduate or professional degree; adj. p <.005*). Some pairwise comparisons were statistically significant, with the sample from the university-run study pool skewing toward higher levels of educational attainment.

Pair	N	df	X^2	p
1 vs. 2	38	1	8.16	**0.004**
1 vs. 3	140	1	0.86	(n.s.)
1 vs. 4	212	1	0.64	(n.s.)
1 vs. 5	242	1	1.26	(n.s.)
2 vs. 3	172	1	12.44	**0.001**
2 vs. 4	144	1	15.48	**0.001**
2 vs. 5	129	1	33.6	**0.001**
3 vs. 4	346	1	0.39	(n.s.)
3 vs. 5	231	1	14.86	**0.001**
4 vs. 5	303	1	13.03	**0.001**

The following table contains the chi-square statistics for all of the income-level pairwise comparisons (*1=Under $25,000, 2=$25K to $49,999, 3=$50K to $74,999, 4=$75K to $99,999, 5=$100K or higher; adj. p <.005*). Some pairwise comparisons were statistically significant, with the sample from the university-run study pool skewing toward higher levels of yearly household income.

Pair	N	df	X^2	p
1 vs. 2	256	1	2.79	(n.s.)
1 vs. 3	207	1	5.35	(n.s.)
1 vs. 4	180	1	0.02	(n.s.)
1 vs. 5	186	1	11.44	**0.001**
2 vs. 3	229	1	0.75	(n.s.)
2 vs. 4	202	1	1.58	(n.s.)
2 vs. 5	208	1	23.62	**0.001**
3 vs. 4	153	1	3.53	(n.s.)
3 vs. 5	159	1	26.73	**0.001**
4 vs. 5	132	1	9.58	**0.002**

The following table contains the chi-square statistics for all of the frequency-level pairwise comparisons for a close tie's experiences of a security breach (*1=Very infrequently, 2=Infrequently, 3=Neither infrequently nor frequently, 4=Frequently, 5=Very frequently; adj. p <.005*). No pairwise comparisons were statistically significant.

Pair	N	df	X^2	p
1 vs. 2	329	1	1.14	(n.s.)
1 vs. 3	223	1	3.05	(n.s.)
1 vs. 4	191	1	1.45	(n.s.)
1 vs. 5	140	1	3.46	(n.s.)
2 vs. 3	282	1	0.87	(n.s.)
2 vs. 4	250	1	4.12	(n.s.)
2 vs. 5	199	1	4.41	(n.s.)
3 vs. 4	144	1	6.25	(n.s.)
3 vs. 5	93	1	5.40	(n.s.)
4 vs. 5	61	1	2.28	(n.s.)

The following table contains the chi-square statistics for all of the frequency-level pairwise comparisons for personal experiences of a security breach (*1=Very infrequently, 2=Infrequently, 3=Neither infrequently nor frequently, 4=Frequently, 5=Very frequently; adj. p <.005*). No pairwise comparisons were statistically significant.

Pair	N	df	X^2	p
1 vs. 2	374	1	0.04	(n.s.)
1 vs. 3	301	1	2.16	(n.s.)
1 vs. 4	284	1	1.01	(n.s.)
1 vs. 5	254	1	0.44	(n.s.)
2 vs. 3	185	1	2.24	(n.s.)
2 vs. 4	168	1	0.70	(n.s.)
2 vs. 5	138	1	0.35	(n.s.)
3 vs. 4	95	1	3.49	(n.s.)
3 vs. 5	65	1	1.51	(n.s.)
4 vs. 5	48	1	0.02	(n.s.)

The following table contains the chi-square statistics for all of the amount-level pairwise comparisons for what participants have heard or seen about online security breaches (*1=None at all, 2=A little, 3=A moderate amount, 4=A lot, 5=A great deal; adj. p <.005*). No pairwise comparisons were statistically significant.

Pair	N	df	X^2	p
1 vs. 2	179	1	1.45	(n.s.)
1 vs. 3	193	1	1.95	(n.s.)
1 vs. 4	115	1	1.34	(n.s.)
1 vs. 5	63	1	2.36	(n.s.)
2 vs. 3	324	1	0.13	(n.s.)
2 vs. 4	246	1	0.00	(n.s.)
2 vs. 5	194	1	0.57	(n.s.)
3 vs. 4	260	1	0.08	(n.s.)
3 vs. 5	208	1	0.29	(n.s.)
4 vs. 5	130	1	0.48	(n.s.)

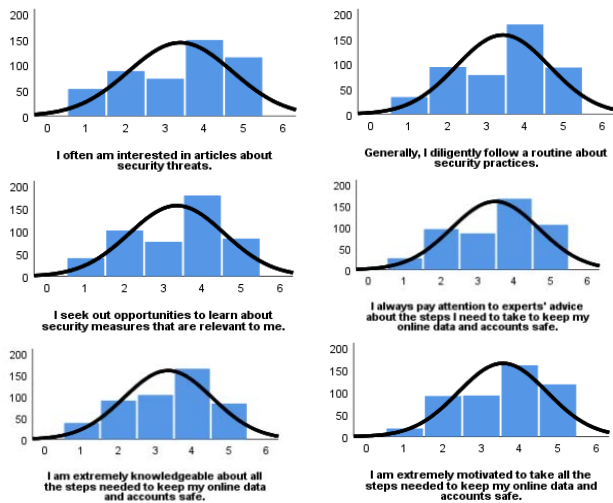## 12.4. Factor Loadings, Alpha if Item Deleted and Item Histograms for SA-6 Scale Finalization (n=478)

Principal Component Analysis - Factor Loading

I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.	0.84
Generally, I diligently follow a routine about security practices.	0.82
I seek out opportunities to learn about security measures that are relevant to me.	0.81
I am extremely motivated to take all the steps needed to keep my online data and accounts safe.	0.80
I often am interested in articles about security threats.	0.79
I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.	0.74

Cronbach's Alpha if Item Deleted (overall = .89)

I often am interested in articles about security threats.	0.87
Generally, I diligently follow a routine about security practices.	0.86
I seek out opportunities to learn about security measures that are relevant to me.	0.86
I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.	0.86
I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.	0.88
I am extremely motivated to take all the steps needed to keep my online data and accounts safe.	0.87

Histograms (1=Strongly disagree, 5=Strongly agree)

12.5. Cronbach's alpha for composite measures incl. for convergent and discriminant validity (threshold = .70)

Measure	Alpha
Barratt Impulsivity Scale	**0.86**
Big5-Agreeableness	0.40
Big5-Conscientiousness	0.53
Big5-Emotional Stability	0.60
Big5-Extraversion	**0.70**
Big5-Openness to Experiences	0.37
Confidence in Using Computers	**0.89**
Consideration of Future Consequences	**0.77**
DoSpERT - Risk-perception subscale	**0.89**
DoSpERT - Risk-taking subscale	**0.84**
GDMS – Avoidance subscale	**0.91**
GDMS – Dependence subscale	**0.81**
Kang Internet Know-How scale	**0.91**
Kang Technical Know-How scale	0.63
Need for Cognition scale	**0.88**
Privacy – Internet Users' Infor. Privacy Concerns	**0.88**
Privacy – Privacy Concerns Scale	**0.96**
SeBIS – Security Behavior Intentions Scale	**0.70**
Self-Efficacy - General	**0.90**
Self-Efficacy - Social	**0.75**
Web-oriented Digital Literacy	**0.94**

12.6. Classification Tables for Selected Logistic Regressions

Q24_4b "*In the past week, I have downloaded and installed at least one available update for my computer's operating system within 24 hours of receiving a notification that it was available*":

Predicted – Constant only

Observed		Q24_4b 1.00	Q24_4b 2.00	Percentage Correct
Q24_4b	1.00	0	79	.0
	2.00	0	112	100.0
Overall Percentage				58.6

Predicted – SeBIS only

Observed		Q24_4b 1.00	Q24_4b 2.00	Percentage Correct
Q24_4b	1.00	41	38	51.9
	2.00	24	88	78.6
Overall Percentage				67.5

Predicted – SeBIS with SA-6

Observed		Q24_4b 1.00	Q24_4b 2.00	Percentage Correct
Q24_4b	1.00	45	34	57.0
	2.00	27	85	75.9
Overall Percentage				68.1

Q24_7b "*In the past week, I have verified at least once that I am running antivirus software that is fully updated*":

Predicted – Constant only

Observed		Q24_7b 1.00	Q24_7b 2.00	Percentage Correct
Q24_7b	1.00	108	0	100.0
	2.00	97	0	.0
Overall Percentage				52.7

Predicted – SeBIS only

Observed		Q24_7b 1.00	Q24_7b 2.00	Percentage Correct
Q24_7b	1.00	74	34	68.5
	2.00	38	59	60.8
Overall Percentage				64.9

Predicted – SeBIS with SA-6

Observed		Q24_7b 1.00	Q24_7b 2.00	Percentage Correct
Q24_7b	1.00	72	36	66.7
	2.00	34	63	64.9
Overall Percentage				65.9

Q24_10b "*In the past week, I have used a password/passcode at least once to unlock my tablet*":

Predicted – Constant only

Observed		Q24_10b 1.00	Q24_10b 2.00	Percentage Correct
Q24_10b	1.00	136	0	100.0
	2.00	57	0	.0
Overall Percentage				70.5

Predicted – SeBIS only

Observed		Q24_10b 1.00	Q24_10b 2.00	Percentage Correct
Q24_10b	1.00	125	11	91.9
	2.00	34	23	40.4
Overall Percentage				76.7

Predicted – SeBIS with SA-6

Observed		Q24_10b 1.00	Q24_10b 2.00	Percentage Correct
Q24_10b	1.00	125	11	91.9
	2.00	33	24	42.1
Overall Percentage				77.2