COMPUTERS & SECURITY 73 (2018) 345–358

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Correlating human traits and cyber security behavior intentions

Margaret Gratian [a], *Sruthi Bandi* [a], *Michel Cukier* [a], *Josiah Dykstra* [b,*], *Amy Ginther* [a]

[a] *The University of Maryland, College Park, MD, USA*
[b] *Laboratory for Telecommunication Sciences, College Park, MD, USA*

ARTICLE INFO

Article history:
Received 26 July 2017
Received in revised form 10 November 2017
Accepted 20 November 2017
Available online 29 November 2017

Keywords:
Human factors
Individual differences
Cyber security behaviors
Cyber security intentions
Surveys

ABSTRACT

In this paper, we correlate human characteristics with cyber security behavior intentions. While previous papers have identified correlations between certain human traits and specific cyber security behavior intentions, we present a comprehensive study that examines how risk-taking preferences, decision-making styles, demographics, and personality traits influence the security behavior intentions of device securement, password generation, proactive awareness, and updating. To validate and expand the work of Egelman and Peer, we conducted a survey of 369 students, faculty, and staff at a large public university and found that individual differences accounted for 5%–23% of the variance in cyber security behavior intentions. Characteristics such as financial risk-taking, rational decision-making, extraversion, and gender were found to be significant unique predictors of good security behaviors. Our study revealed both validations and contradictions of related work in addition to finding previously unreported correlations. We motivate the importance of studies such as ours by demonstrating how the influence of individual differences on security behavior intentions can be environment-specific. Thus, some security decisions should also depend on the environment.

Published by Elsevier Ltd.

1. Introduction

Humans are often identified as the weakest link in cyber security, since any technical security solution is still prone to failures caused by human error. As such, there is a considerable amount of research that seeks to better understand users and the factors that influence their security behaviors. Though several researchers have identified differences in human traits that correlate with poor security practices and increased susceptibility to becoming a victim of cyber crimes such as phishing or social engineering, work in this area is still limited (Egelman and Peer, 2015). Understanding how users' individual differences influence their cyber security behavior intentions is critical to helping researchers, security practitioners, and organizations identify users who are more susceptible to poor or potentially dangerous security practices. Such insights can help practitioners develop targeted educational efforts and focus on addressing the users in their community who pose the greatest challenge to overall cyber security.

In this paper, we present a study that correlates cyber security behavior intentions with four major categories of individual differences: demographic factors, personality traits, risk-taking preferences, and decision-making styles. We build

* *Corresponding author.*
E-mail addresses: mgratian@umd.edu (M. Gratian), sbandi@umd.edu (S. Bandi), mcukier@umd.edu (M. Cukier), jdykstra@ltsnet.net (J. Dykstra), aginther@umd.edu (A. Ginther)
https://doi.org/10.1016/j.cose.2017.11.015
0167-4048/Published by Elsevier Ltd.

upon the work of Egelman and Peer (2015) and Egelman et al. (2016), who were among the first to correlate the security behaviors of device securement, password generation, proactive awareness, and updating with individual differences related to risking-taking preferences and decision-making styles.

Through a survey of 369 students, faculty, and staff at a large public university, we make the following contributions:

- We validate the work of Egelman and Peer (2015) by applying their Security Behavior Intention Scale (SeBIS) and correlating risk-taking preferences and decision-making styles with cyber security behavior intentions
- We expand on the work of Egelman and Peer (2015) by correlating demographics and personality traits with cyber security behavior intentions. To the best of our knowledge, we are the first to present such a comprehensive evaluation of these human traits and cyber security behavior intentions
- We determine the individual differences that are significant unique predictors of security behaviors in a public university setting and motivate the need for additional work in this area by demonstrating that the influence of individual differences on security behaviors is environment-specific

The remainder of this paper is organized as follows. In Section 2, we provide an overview of the security behaviors and individual differences that are evaluated in this study and present our experiment hypotheses. In Section 3, we discuss the survey instrument and the data collection and analysis procedures. In Section 4, we present our correlation results. In Section 5, we provide a comparison of our results to previous research, practical implications of the results, and study limitations. And in Section 6, we state our conclusions.

2. Background and related work

2.1. Security behaviors

Egelman and Peer (2015) developed the SeBIS to measure user security behavior intentions. They began with a set of 30 potential end user behaviors derived from Internet service providers, the United States Computer Readiness and Security Team (US-CERT), industry consortia, and computer security expert feedback. Through a series of surveys on a representative sample of the United States population and extensive correlation analysis and reliability testing, the final scale resulted in a series of questions that measured four security behaviors: device securement, password generation, proactive awareness, and updating. These four behaviors were based on four distinct themes that emerged from items in the questionnaire that significantly predicted the variance in user responses.

In this study, we focus on the four major categories of user security behaviors suggested by Egelman and Peer: device securement, password generation, proactive awareness, and updating (Egelman and Peer, 2015). *Device Securement* refers to using PINs and passwords to lock devices, setting up automatic device or screen locking, and manually securing devices before leaving them unattended. *Password Generation* refers to choosing strong passwords and not reusing passwords between different accounts. *Proactive Awareness* refers to paying attention to contextual clues such as the URL bar or other browser indicators in websites or email messages, executing caution when submitting information to websites, and being proactive in reporting security incidents. Finally, *Updating* measures the extent to which users consistently apply security patches or otherwise keep their software up-to-date.

2.2. Individual differences

Individual differences can encompass a wide range of variables that vary between people (Egelman and Peer, 2015). We evaluate four major categories of individual differences: demographic factors, personality traits, risk-taking preferences, and decision-making styles. The following sections discuss these individual differences in more detail and justify their inclusion in this study. We also outline the experiment hypotheses.

2.2.1. Demographics

Demographics can encompass a number of characteristics in a human population. Because our study evaluates security behaviors in a university setting, we focus on the following demographic characteristics: age, gender, role at the university (student, faculty, or staff), major, citizenship, and employment length at the university. These represent standard university demographic characteristics that we hypothesized might correlate to security behavior. The subset of demographics is also informed by related work which examined the correlation between demographics and phishing susceptibility in university settings (Darkish et al., 2012; Mohebzada et al., 2012; Parrish et al., 2009; Sheng et al., 2010). Sheng et al. (2010) found women and people aged 18–25 to be more susceptible to phishing attacks than men and other age groups, respectively; Parrish et al. (2009) also found a correlation between people aged 18–25 and phishing attack susceptibility; and Darkish et al. (2012) found liberal arts students to be more susceptible to attacks than other majors. Mohebzada et al. (2012) however, suggested demographics were not conclusive in predicting attack susceptibility. There is also limited work examining how demographics influence other cyber security behaviors. Whitty et al. (2015) found that younger people were significantly more likely to engage in the poor security practice of password sharing.

Therefore, we test the following hypothesis:

H1. *Users' demographic factors will significantly correlate with their security behavior intentions of device securement, password generation, proactive awareness, and updating.*

2.2.2. Personality traits behaviors

There are five major categories of personality traits in the widely accepted "Big Five" model: agreeableness, conscientiousness, neuroticism, openness, and extraversion (John and Srivastava, 1995). Agreeableness measures cooperative traits; conscientiousness measures dependable and organized traits; neuroticism, also sometimes categorized as emotional stability, measures insecure and nervous traits; openness measures

intellectual and imaginative traits; finally, extraversion measures energetic and outgoing traits (John and Srivastava, 1995). While personality is widely studied in psychology literature, few studies examine the relationship between personality traits and security behaviors. Personality traits have largely been studied in the context of phishing susceptibility. Halevi et al. (2013) found a correlation between females with high neuroticism and phishing susceptibility and a correlation between openness and weak privacy settings. Pattinson et al. (2012) found high openness and extraversion to be related to decreased phishing susceptibility. High extraversion has also been correlated with reduced perception of security risk when online shopping (Riquelme and Roman, 2014).

Therefore, we test the following hypothesis:

H2. *Users' personality traits of agreeableness, conscientiousness, neuroticism, openness, and extraversion will significantly correlate with their security behavior intentions of device securement, password generation, proactive awareness, and updating.*

2.2.3. *Risk-taking preferences*

Risk-taking is a measure of risk attitude and shapes decision-making, which is examined in the literature in relation to several forms of risky behavior (Arnett, 1996). There are five dimensions of risk-taking preferences that are studied in relation to security behaviors: ethical (RTE), financial (RTF), health/safety (RTH), recreational (RTR), and social (RTS) risk-taking. Egelman and Peer (2015) found that risk-taking was a significant predictor of security behaviors, demonstrating that willingness to take health/safety risks was inversely correlated with proactive awareness and updating behaviors. Sheng et al. (2010) found that risk-averse users were less likely to fall for phishing, again demonstrating that risk-taking preferences can influence security behaviors.

Therefore, we test the following hypothesis:

H3. *Users' willingness to take risks will significantly correlate with their security behavior intentions of device securement, password generation, proactive awareness, and updating.*

2.2.4. *Decision-making styles*

Decision-making style is the response pattern exhibited by an individual in a decision-making situation (Thunholm, 2004). Decision-making styles are generally categorized into five broad categories: rational (DMR), avoidant (DMA), dependent (DMD), intuitive (DMI), and spontaneous (DMD) decision-making. Rational refers to using logic when making decisions; avoidant refers to delaying decision-making; dependent refers to relying on others for decision-making help; intuitive refers to decision-making based on instincts; lastly, spontaneous refers to quick decision-making (Scott and Bruce, 1995). Egelman and Peer found both dependent decision-making and impulsive decision-making to be inversely correlated with good security behaviors (Egelman and Peer, 2015). Multiple studies have also evaluated the connection between decision-making style and phishing susceptibility (Leach, 2003; Ng and Xu, 2009). Jeske et al. (2016) examined how impulsive decision-making influenced mobile security practices.

Therefore, we test the following hypothesis:

H4. *Users' decision-making styles will significantly correlate with their security behavior intentions of device securement, password generation, proactive awareness, and updating.*

3. Methodology

3.1. *Research approach*

The goal of this study was to determine the individual differences that are predictive of good security behaviors. Thus, we tested four predictor variables representing the four major categories of individual differences: demographic factors, personality traits, risk-taking preferences, and decision-making styles. The research outcome variables represent the four major categories of security behaviors: device securement, password generation, proactive awareness, and updating.

3.2. *Survey instrument*

We developed a web-based survey[1] on Qualtrics, a popular online survey platform. The survey asked users to self-report on personality traits, decision-making styles, and risk-taking preferences.

To measure personality traits, we used the International Personality Item Pool (IPIP) scale to measure agreeableness, conscientiousness, neuroticism, openness, and extraversion (Goldberg et al., 2006). We used a 50-item questionnaire from this pool using 5-point Likert ratings ranging from "Very Inaccurate" to "Very Accurate."

To measure risk-taking preferences, we used the Domain-Specific Risk-Taking (DOSPERT) inventory (Appelt et al., 2011) to measure ethical, financial, health/safety, recreational, and social risk-taking. The DOSPERT scale is a 30-item assessment with 5 subscales using a 7-point Likert scale ranging from "Very Unlikely" to "Very Likely."

To measure decision-making styles, we used the General Decision-Making Style (GDMS) questionnaire (Scott and Bruce, 1995) to measure rational, intuitive, dependent, avoidant, and spontaneous decision-making styles. GDMS is widely used to assess how individuals approach decision-making situations and contains a 25-item scale with 5 subscales using 5-point Likert ratings ranging from "Strongly Disagree" to "Strongly Agree."

Finally, we used the Security Behavior Intentions Scale (SeBIS) to measure user security behavior intentions (Egelman and Peer, 2015). The security behavior intentions measured by this scale are used as a proxy to evaluate actual user security behaviors. This decision is validated by Egelman et al. (2016), in which they correlated the SeBIS with the security behaviors of device securement, password generation, proactive awareness, and updating. SeBIS is a 16-item scale with four subscales using 5-point Likert ratings ranging from "Never" to "Always."

Institutional Review Board (IRB) approvals were received for the developed survey instrument and the study procedures.

[1] The full survey instrument can be found in the Appendix.

3.3. Data collection and recruitment

Egelman and Peer (2015) used the SeBIS, DOSPERT, and the GDMS scales to correlate user security behavior intentions with risk-taking preferences and decision-making styles. They recruited 500 participants through Amazon Mechanical Turk and considered their sample representative of the US population: 52.8% were male, 37.8% held bachelor's degrees, 14% completed some graduate school, ages ranged between 19 and 71, and median household income was between $35,000 and $50,000 (Egelman and Peer, 2015).

In this study, we chose to focus on higher education and recruited participants from a large, public university. We did this for several reasons. First, recruiting from a different population allowed us to evaluate the ecological validity of the correlations observed in Egelman and Peer (2015). Second, this enabled us to expand the individual differences that we tested for correlations with security behavior intentions; for example, we were able to test for the impact of major and citizenship on good security behavior intentions. Lastly, universities have been the victims of several high profile phishing attacks, so this study is also motivated by a need to better understand users in a university population in order to improve overall university security.

Email invitations to participate were sent to a representative sample of students, faculty, and staff at a large public university. We were approved by the university to sample 10% of the total population, so 1000 staff/faculty and 3000 undergraduate/graduate students received invitations. Upon clicking the survey link in the email invitation, participants were presented with a consent form and details of the study before receiving the questionnaire. Questions were not mandatory and participants could skip any questions they did not wish to answer. Survey completion time ranged from 12 to 20 minutes. Upon survey completion, participants were entered into a drawing for 50 $10 Amazon gift cards.

The survey was active for a three-week period and two intermediate email reminders were sent during this time frame. We received a total of 385 complete responses and 150 partial responses. The complete responses were cleaned for inconsistencies and missing values and the partial responses were discarded from the analysis. This resulted in 369 usable responses.

We obtained demographic factors of age, gender, role at the university, major, citizenship, and employment length with the university from the human resources and registrar offices on campus. A protocol for de-identifying the data was approved through the university's IRB Human Subjects Approval process. Requests were submitted to University Human Resources (UHR) and Office of the Registrar via the offices' respective procedures; each request was granted. The offices' data use policies for the protection of university data were consistent with the IRB-approved protocol. Table 1 summarizes the demographics of the sample, the respondents, and the non-respondents.

3.4. Data analysis

Correlation analysis, factor analysis and reliability testing, multiple regression analysis, and ANOVA with post-hoc analysis were performed on the 369 survey responses. The following sections discuss the data analysis in more detail.

3.4.1. Correlation analysis

Pearson correlation analysis was performed on all the predictor variables in the model to evaluate the data for multicollinearity issues. For variables that appeared similar, weaker variables were dropped from the analysis. For example, the variable recreational risk-taking preference was highly correlated with decision-making avoidance style. Due to high collinearity ($r = -0.769$, $p < 0.01$), recreational risk-taking preference was dropped from the analysis.

3.4.2. Factor analysis and reliability testing

Since SeBIS is a relatively new scale, principal component analysis with varimax rotation was performed to verify the factor loadings onto the four SeBIS subscales of device securement, password generation, proactive awareness, and updating. The loadings closely resembled those reported by Egelman and Peer (2015). The four security behaviors accounted for 52.9% of the overall variance, with device securement accounting for 11.07%, password generation accounting for 13.09%, proactive awareness accounting for 13.8%, and updating accounting for 14.97%. As with prior results (Egelman and Peer, 2015), the four components accounted for 55.6% of the overall variance, with device securement accounting for 26.7%, password generation

Table 1 – Sample, respondent, and non-respondent demographic summary.

Demographic Factors	Groups	Full Sample Percentages	Respondent Percentages	Non-Respondent Percentages
Age	18–25	67.5%	57.7%	68.3%
	26–35	12%	11%	12.1%
	36–45	6.9%	9.3%	6.7%
	46–55	6%	9.3%	5.7%
	56–65	5.1%	8.7%	4.7%
	66 +	2.5%	4.1%	2.5%
Gender	Female	44.7%	59.4%	43.3%
	Male	55.3%	40.5%	56.7%
Role	Student	75.8%	65.8%	76.8%
	Faculty/Staff	24.2%	34.2%	23.2%
Citizenship	U.S. Citizen	87.2%	90.1%	87%
	Non U.S. Citizen	12.8%	9.9%	13%

Table 2 – Factor loadings for 16 items of the SeBIS. Factor loadings <0.3 have been suppressed.

	Device Securement	Password Generation	Proactive Awareness	Updating
When I'm prompted for a software update, I install it right away.				0.78
I try to make sure the programs I use are up to date.				0.826
I manually lock my computer screen when I step away from it.	0.375	0.333		0.39
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	0.725			
I use a PIN or passcode to unlock my mobile phone.	0.682			
I use a password/passcode to unlock my laptop or tablet.	0.748			
If I discover a security problem, I continue what I was doing because I assume someone else will fix it.			0.686	
When someone sends me a link, I open it without first verifying where it goes.			0.793	
I verify that my antivirus software has been regularly updating itself.				0.731
When browsing websites, I mouse over links to see where they go, before clicking them.			–0.368	0.439
I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.			0.701	
I do not change my passwords, unless I have to.		–0.606		
I use different passwords for different accounts that I have.		0.587		
I do not include special characters in my password if it's not required.		–0.694		
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.		0.722		
I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).		–0.357	0.562	
Eigenvalues	1.156	1.556	1.972	3.785
Percentage of variance	11.07%	13.09%	13.8%	14.97%
Total variance		52.93%		

accounting for 11.6%, proactive awareness accounting for 9.0%, and updating accounting for 8.3%.

Factor analysis was not performed for the other scales (IPIP, DOSPERT, and GDMS) since these are well-established scales in the literature. See Table 2 for a summary of our SeBIS factor loadings.

Reliability testing was then performed on all the predictor and outcome variable scales. Regarding IPIP, moderate to excellent internal consistency was observed with the following Cronbach's alphas: $\alpha = 0.804$ for agreeableness, $\alpha = 0.857$ for conscientiousness, $\alpha = 0.873$ for neuroticism, $\alpha = 0.803$ for openness, and $\alpha = 0.868$ for extraversion. Regarding DOSPERT, moderate to excellent internal consistency was also observed with the following Cronbach's alphas: $\alpha = 0.802$ for ethical; $\alpha = 0.767$ for financial; $\alpha = 0.748$ for health/safety; $\alpha = 0.624$ for social. Regarding GDMS, moderate to excellent internal consistency was also observed with the following Cronbach's alphas: $\alpha = 0.767$ for rational; $\alpha = 0.78$ for intuitive; $\alpha = 0.759$ for dependent; $\alpha = 0.91$ for avoidant; and $\alpha = 0.859$ for spontaneous. Finally, regarding SeBIS, moderate internal consistency was found with the following Cronbach's alphas: $\alpha = 0.604$ for device securement; $\alpha = 0.646$ for password generation; $\alpha = 0.675$ for proactive awareness; and $\alpha = 0.749$ for updating.

3.4.3. *Multiple regression analysis*

Multiple regression analysis was conducted with the predictor variables of demographic factors, personality traits, risk-taking preferences, and decision-making styles on the four outcome variables of security behaviors, device securement, password generation, proactive awareness, and updating. Only demographic factors of age, gender, role, and citizenship were included in the regression model, as major and employment length did not apply to the entire sample. Table 3 contains a summary of the regression analysis coefficients regarding the

Table 3 – Summary of regression analysis coefficients regarding demographic factors and personality traits.

	Securement	Passwords	Awareness	Updating
Age				
Gender		0.157**	0.135*	0.135*
Role				
Citizenship				
Extraversion	0.142*			
Agreeable				
Conscientiousness		0.166*		0.181*
Neuroticism				
Openness				

*$p < 0.005$.
**$p < 0.01$.

Table 4 – Summary of regression analysis coefficients in our study (first value) and Egelman and Peer (2015) (second value).

	Securement	Passwords	Awareness	Updating
RTE		–	–0.152*	–
		–0.201**	–0.226**	–0.201**
RTF		0.141*		
		–		
RTH		–0.21**	–	–0.172*
		–	–0.204**	–0.164**
RTS		–		
		0.141**		
DMR	0.164**	–	0.135*	0.153**
	–	0.145**	0.224**	0.229**
DMI				
DMD			–0.108*	
			–0.157**	
DMA	–	–0.149*	–0.157*	–
	–0.133*	–0.220**	–0.230**	–0.247**
DMS				0.243***
				–0.129*

*$p < 0.005$.
**$p < 0.01$.
***$p < 0.001$.

demographic factors (age, gender, role, and citizenship) and personality traits (extraversion, agreeableness, conscientiousness, neuroticism, and openness). Table 4 contains a summary of the regression analysis coefficients and a comparison with the risk-taking preferences and decision-making styles results of Egelman and Peer (2015). RTE, RTF, RTH, and RTS refer respectively to Risk-Taking Ethical, Financial, Health/Safety, and Social; DMR, DMI, DMD, DMA, and DMS refer respectively to Decision-Making Rational, Intuitive, Dependent, Avoidant, and Spontaneous.

3.4.4. *ANOVA analysis*

ANOVA's along with post-hoc tests of Tukey HSD and Games-Howell were conducted to test the mean differences of cyber security behaviors across the demographics of age, gender, role, major, citizenship, and employment length.

4. Results

This section presents the analysis results for each cyber security behavior intention subscale.

4.1. *Device securement*

There was no significant unique effect of any demographic factor on users' security behavior intention of device securement. In personality traits, extraversion ($\beta = 0.142$, $p < 0.05$) was found to be a significant unique predictor. There was no significant unique effect of any risk-taking preference on users' security behavior intention of device securement. In decision-making styles, rational decision-making style ($\beta = 0.164$, $p < 0.01$) was a significant unique predictor. Overall, the predictors in the regression model account for 5.2% of the variance in users' security behavior intention of device securement.

4.2. *Password generation*

In demographic factors, gender ($\beta = 0.157$, $p < 0.01$) had a unique significant effect on users' security behavior intention of password generation. In personality traits, conscientiousness ($\beta = 0.166$, $p < 0.05$) was found to be a significant unique predictor. In risk-taking preferences, financial risk-taking ($\beta = 0.141$, $p < 0.01$) and health/safety risk-taking ($\beta = -0.211$, $p < 0.05$) were found to be significant unique predictors of strong password generation. In decision-making styles, avoidant decision-making style ($\beta = -0.149$, $p < 0.05$) was a significant unique predictor. Overall, the predictors in the regression model account for 16.8% of the variance in users' security behavior intention of password generation.

4.3. *Proactive awareness*

In demographic factors, gender ($\beta = 0.135$, $p < 0.01$) had a unique significant effect on users' security behavior intention of proactive awareness. There was no significant unique effect of any personality traits on users' security behavior of proactive awareness. In risk-taking preferences, ethical risk-taking preference ($\beta = -0.152$, $p < 0.05$) was found to be a unique significant predictor. In decision-making styles, rational decision-making style ($\beta = -0.135$, $p < 0.05$), dependent decision-making style ($\beta = -0.108$, $p < 0.05$), and avoidant decision-making style ($\beta = -0.157$, $p < 0.05$) had significant unique effects on proactive awareness. Overall, the predictors in the regression model account for 22.8% of the variance in users' security behavior intention of proactive awareness.

4.4. *Updating*

In demographic factors, gender ($\beta = 0.135$, $p < 0.05$) had a significant unique effect on users' security behavior intention of updating. In personality traits, conscientiousness ($\beta = 0.181$, $p < 0.05$) was found to be a significant unique predictor. In risk-taking preferences, health/safety risk-taking ($\beta = -0.172$, $p < 0.05$) was found to be a unique significant predictor of updating behavior. In decision-making styles, rational decision-making style ($\beta = 0.153$, $p < 0.01$) and spontaneous decision-making style ($\beta = 0.243$, $p < 0.001$) had significant unique effects. Overall, the predictors in the regression model account for 12.6% of the variance in users' security behavior intention of updating.

Table 5 summarizes our hypotheses and results.

5. Discussion

This section presents a deeper interpretation of the results by providing implications for theory and for practice. We also include a discussion of the study limitations.

5.1. *Implications for theory*

5.1.1. *Device securement*

Although demographic factors did not have a significant unique effect on the regression model, the ANOVA testing found that engineering majors reported a higher security behavior intention

Table 5 – Summary of results for each hypothesis in the four categories of user security behavior.

	Device Securement	Password Generation	Proactive Awareness	Updating
H1: Users' demographic factors will significantly correlate with their security behavior intentions.	Not supported	Supported for gender	Supported for gender	Supported for gender
H2: User personality traits of agreeableness, conscientiousness, neuroticism, openness, extraversion, and risk avoidance will significantly correlate with their security behavior intentions.	Supported for extraversion	Supported for conscientiousness	Supported for conscientiousness	Supported for conscientiousness
H3: Users' willingness to take risks will significantly correlate with their security behavior intentions.	Not supported	Supported for health/safety risk-taking and supported in the reverse direction for financial risk-taking	Supported for ethical risk-taking	Supported for health/safety risk-taking
H4: Users' decision-making styles will significantly correlate with their security behavior intentions.	Supported for rational decision-making	Supported for avoidant decision-making	Supported for rational decision-making and supported in the reverse direction for spontaneous decision-making	Supported for rational decision-making and supported in the reverse direction for spontaneous decision-making

of device securement in comparison to humanity majors. This result was not significant so further evaluation of demographics is necessary.

We found extraversion to be a significant unique predictor of good device securement behavior intention. This suggests that among our population, those with outgoing personalities are more likely to be careful about locking their devices than those with introverted personalities.

In line with previous literature, risk-taking preferences did not correlate with the security behavior intention of device securement. This confirms the findings of Egelman and Peer (2015) and reinforces the understanding that risk-taking is not an important influence on this security behavior intention.

While our results supported Egelman and Peer (2015) for risk-taking preferences, we determined a previously unreported correlation between decision-making styles and device securement. We found rational decision-making to be a significant unique predictor of good device securement intentions. This suggests that among our population, people who exhibit strong device securement practices may do so because they have rationally evaluated the benefits of securing their device and determined it to be a logical choice. Additionally, in our university setting, there was no observed relationship between the avoidant decision-making style and device securement in the regression model, contradicting the correlation found in Egelman and Peer (2015).

Since only 5% of the variance in the outcome variable was explained by the predictor variables, there are other factors that should be evaluated to identify the individual differences that influence good device securement behavior intentions.

5.1.2. *Password generation*

In terms of demographic factors, gender was a significant unique predictor of password generation behavior intentions. Specifically, females reported weaker password generation behaviors than males. Previous research suggests that women are more susceptible to phishing attacks than men; our results reveal another area where there is a significant correlation between gender and a security behavior (Sheng et al., 2010).

Although the age demographic did not have a significant unique effect on the regression model, ANOVA testing revealed that respondents aged 18–25 and humanities majors reported weaker password generation behavior intentions than other demographics. Previous literature has reported increased phishing susceptibility in these two demographic groups (Sheng et al., 2010); our results reveal that password generation is another area where these two groups may have poorer security practices in comparison to other demographic groups.

Similarly, while the demographic of major did not have a significant unique effect on the regression model, engineering major individuals tended to report better password generation intentions compared to humanities majors. Again, since these results were not significant, further analysis could be done to understand password generation behaviors in these groups.

Egelman and Peer's work suggested that ethical and social risk-taking are significant predictors of security behavior intentions (Egelman and Peer, 2015). Our study did not find significant correlations between these two risk-taking preferences and password generation intentions.

In this study, only the avoidant decision-making style was found to be a significant predictor for strong password generation. Though Egelman and Peer found correlations between password generation and both rational and avoidant decision-making styles (Egelman and Peer, 2015), our results suggest that it is not safe to assume that rational decision-makers will necessarily practice better password generation behaviors.

The predictors in the regression model explained nearly 17% of the variance in the outcome variable. This suggests that individual differences influence password generation intentions.

5.1.3. *Proactive awareness*

In terms of demographic factors, gender was again a significant unique predictor of proactive awareness. Specifically, females reported weaker proactive awareness intentions than males.

In ANOVA testing for differences by demographic factors, women and respondents aged 18–25 reported weak proactive awareness behavior intentions. Again, these two groups were more likely to have poorer security practices than other demographic groups in our study. When tested for role at the university, the faculty/staff reported higher security behaviors of proactive awareness, even when controlling for age. With educational background, earlier research found that business, education and liberal arts students were more vulnerable to spear phishing attacks than technology and science students (Darkish et al., 2012). Our study did not find any significant differences to support that there are poor security behaviors-specific to the business, education, and liberal arts student group.

Like Egelman and Peer, we also found that ethical risk-taking had a significant effect on proactive awareness. However, we did not identify health/safety risk-taking preferences as significant unique predictors like they did.

Our findings also support Egelman and Peer's correlations between proactive awareness and rational, avoidant, and dependent decision-making styles (Egelman and Peer, 2015).

The predictors in the regression model explained 23% of the variance in proactive awareness. This suggests that individual differences influence proactive awareness intentions.

5.1.4. *Updating*

Gender was a significant unique predictor of updating behavior intentions. Specifically, females reported weaker updating behaviors than males. Again, our results demonstrate that women tend to report poorer security behavior intentions than males. These results further demonstrate that women might be a population more susceptible to weak security practices in comparison to other demographic groups.

When tested for the effect of demographics, age did not have a unique effect in the regression model, but the ANOVA findings suggested that respondents aged 18–25 had weaker updating behavior intentions.

Egelman and Peer correlated individuals willing to take ethical and health/safety risks with poor security behavior intentions (Egelman and Peer, 2015). Our results contradict this finding. While health/safety risk-taking preference still remained a significant predictor of updating security behavior intentions, there was no relationship between ethical risk-taking preferences and updating intentions. Since the earlier study only explored correlations and did not also test for unique influence of the factors on updating, it can be inferred that ethical risk-taking does not predict a user's security updating behavior intention.

Egelman and Peer found positive correlations between updating behavior intention and rational, avoidant, and spontaneous decision-making styles (Egelman and Peer, 2015). In our study, the same three factors correlated significantly before the addition of personality traits. By adding personality traits, conscientiousness suppressed the effect of the avoidant decision-making style. Risk aversion was also found to be a significant predictor of strong updating behaviors.

The predictors in the regression model explained 12.6% of the variance in updating. Thus, there are other factors that could be evaluated to identify the individual differences that influence good updating behavior intentions.

5.2. *Implications for practice*

These results have immediate and practical implications. Security training and education is expensive to implement. According to a 2016 SANS Institute IT Security Spending Report, large organizations spend nearly 35% of their annual security budget on end user training and awareness (Filkins and Hardy, 2016). Our results can help security practitioners prioritize their training efforts on end users who exhibit individual differences that are significant predictors of poor security behavior intentions. In this section, we discuss how individual differences in gender, age, decision-making styles, and risk-taking preferences can be taken into consideration when developing tailored training campaigns.

For example, in this study, women were found to exhibit significantly weaker security behavior intentions for password generation, updating, and proactive awareness than males. Therefore, women may be a demographic group in need of additional cyber security training and guidance. In the university setting, the security office might be motivated to develop targeted educational campaigns for women to encourage better security behaviors. Similarly, ANOVA testing revealed 18–25 year olds and humanities majors reported poorer security behavior intentions than older respondents and engineering majors, respectively. Thus, the 18–25 age group and humanities majors might be other groups in need of additional security training and guidance. At the university examined in this study, the security office, with a team of undergraduates in a cyber security program, has been developing an online game to teach good cyber security practices with the intention of making this a mandatory training for undergraduate students, similar to the alcohol safety training that incoming freshman must complete.

Security messaging, educational campaigns, and training might also be more effective if they appeal to individual differences in users. Several studies have found that understandings of individual differences can also be successfully leveraged to craft more impactful security messaging and training. For example, Kajzer et al. (2014) found that users with higher agreeableness were more receptive to security campaigns that emphasized morals, regret, and deterrence and that older users were more receptive to security awareness messages in general. Similarly, Shropshire et al. (2006) found conscientiousness to be correlated with higher security compliance. Insights from these studies can potentially be coupled with our findings to develop even stronger and more effective security messaging.

For the security behavior intention of device securement, since rational decision-making was found to be a significant unique predictor of good device securement behavior intention, security messaging to such users can primarily appeal to logic. Similarly, since extraversion was also a significant unique predictor, messaging to these users can emphasize how others

in their social group are benefiting from good device securement practices.

For the security behavior intention of password generation, users exhibiting high financial risk-taking might be receptive to security training and messaging that demonstrates the benefits of strong passwords on keeping investment accounts safe, while users scoring low on health/safety risk-taking may be receptive to an emphasis on the threats to health and safety if weak passwords are used. The avoidant decision-making style was also a significant predictor, so messaging to these users could emphasize how procrastinating or delaying good password practices could allow consequences to escalate and worsen over time.

For the security behavior intention of updating, since individual differences such as conscientiousness and risk-averse preferences were significant predictors, security training and messaging could be tailored to appeal to these types of users. Messaging to conscientious users can focus on how updating is the right thing to do because it reduces the impact and scope of vulnerabilities. Messaging to risk-averse users can focus on the severity and likelihood of the consequences of failing to update.

Finally, for the security behavior intention of proactive awareness, messaging can potentially be more effective for rational decision-makers if it logically explains how various actions and failures to be proactive can lead to different consequences.

There is of course added cost associated with developing customized training, so additional research and pilot studies would need to be performed to identify if this up-front investment is more cost-effective and yields better results than generic training does in the long term.

5.3. *Limitations*

There are several limitations to our study. First, we would have preferred a higher survey response rate than 9%. Second, a significant non-response bias was found for the demographic factors of age, gender, role at the university, and citizenship. Respondents were older than non-respondents, more likely to be female, more likely to be faculty or staff, and more likely to be US citizens. This poses a threat to the external validity, since the respondents may differ from the total university population. Third, while SeBIS factor analysis and reliability testing showed excellent internal consistency for the predictor variables, it showed only moderate internal consistency for the outcome variables, suggesting that findings are in need of further evaluation. Fourth, the SeBIS only measures self-reported behavior intentions. While Egelman et al. (2016) correlated the SeBIS with security behaviors, this correlation has not been widely validated and thus our study cannot claim to provide insights into actual user behaviors. Finally, because our results were determined through a survey, it is possible that random clicking, fatigue, or failures to carefully read questions affected the accuracy of the responses.

6. Conclusion

Universities have been the victims of high profile cyber attacks. Studying the security behaviors of users in a university environment is a logical first step toward understanding how to improve security and make universities more resilient to cyber attacks. Through a survey of 369 students, faculty, and staff at a large public university, we correlated individual differences in demographic factors, personality traits, risk-taking preferences, and decision-making styles with the cyber security behavior intentions of device securement, password generation, proactive awareness, and updating. These individual differences accounted for 5%–23% of the variance in reported cyber security behavior intentions.

Our work is important for several reasons. First, by applying the SeBIS to correlate risk-taking preferences and decision-making styles with cyber security intentions, we contribute to enhancing the science of security by validating the work of Egelman and Peer. The SeBIS is a relatively new scale and has yet to be extensively used. Our work verifies the factor loadings of the four SeBIS subscales and presents a comparison of our regression analysis coefficients to those presented in Egelman and Peer (2015).

Second, our work deepens understandings of the influence of individual differences on cyber security behavior intentions by including demographic factors and personality traits in our survey, thereby expanding on the work of Egelman and Peer. These results are practical for informing the design and deployment of more effective cyber security, including technological protections and user education.

Finally, our work motivates the importance of environment-specific studies to understand users. Our study focused on evaluating users in a university environment. This revealed both confirmations and contradictions of previous work: rational decision-making and gender were significant predictors of good security behavior intentions, while ethical risk-taking was often not a significant predictor. Additionally, our study also revealed previously unreported findings; for example, financial risk-taking was found to be a significant predictor of good password generation behavior.

The differences between our findings and previous work demonstrate that the influence of individual differences on security behavior intentions can vary between environments. Insights into user behavior intentions may not generalize across all settings and user populations. This is analogous to the field of criminology, where studies are often repeated in different cities to identify variance. By making our methodology and study instruments available, researchers can replicate this study with other populations.

From a practical perspective, the results of this study are useful at the university level because they give our security practitioners and decision-makers insights into which populations have weak security behaviors and therefore may benefit from extra attention. These results will be used at the university to develop customized security solutions and training, with the goal of encouraging better security behaviors and compliance with security policy.

Because our study was tailored to a university population, our security practitioners have population-specific insights to work with. If this study is replicated for practical use in other environments, there may be different individual traits and security behaviors that are of interest. For example, university demographics such as major or role may not have any relevance in a corporate environment. Similarly, the security

behavior of updating may not be of importance in an environment where regular updating and patching are enforced by an IT department. Thus, researchers and security practitioners wishing to better understand their user populations can apply our methodology but also tailor their selection of traits and behaviors to their environment.

From a broader perspective, we hope that researchers and security practitioners at other institutions will use this study as motivation to evaluate their populations for correlations between individual differences and security behaviors in order to continue developing the security community's understanding of users.

Acknowledgment

The authors acknowledge the support of the U.S. Department of Defense. The views and conclusions expressed in this paper are those of the authors, and do not necessarily represent those of the Department of Defense or U.S. Federal Government.

Appendix

A. *Survey instrument*

Section 1: Personality traits (IPIP)

Please indicate to what extent each of the following statements applies to you.

(1) Very Inaccurate, (2) Moderately Inaccurate, (3) Neither Inaccurate nor Accurate, (4) Moderately Accurate, (5) Very Accurate.

Extraversion

1. I feel comfortable around people.
2. I make friends easily.
3. I am skilled in handling social situations.
4. I am the life of the party.
5. I know how to captivate people.
6. I have little to say.
7. I keep in the background.
8. I would describe my experiences as somewhat dull.
9. I don't like to draw attention to myself.
10. I don't talk a lot.

Agreeableness

11. I have a good word for everyone.
12. I believe that others have good intentions.
13. I respect others.
14. I accept people as they are.
15. I make people feel at ease.
16. I have a sharp tongue.
17. I cut others to pieces.
18. I suspect hidden motives in others.
19. I get back at others.
20. I insult people.

Conscientiousness

21. I am always prepared.
22. I pay attention to details.
23. I get chores done right away.
24. I carry out my plans.
25. I make plans and stick to them.
26. I waste my time.
27. I find it difficult to get down to work.
28. I do just enough work to get by.
29. I don't see things through.
30. I shirk my duties.

Neuroticism

31. I often feel blue.
32. I dislike myself.
33. I am often down in the dumps.
34. I have frequent mood swings.
35. I panic easily.
36. I rarely get irritated.
37. I seldom feel blue.
38. I feel comfortable with myself.
39. I am not easily bothered by things.
40. I am very pleased with myself.

Openness to experience

41. I believe in the importance of art.
42. I have a vivid imagination.
43. I tend to vote for liberal political candidates.
44. I carry the conversation to a higher level.
45. I enjoy hearing new ideas.
46. I am not interested in abstract ideas.
47. I do not like art.
48. I avoid philosophical discussions.
49. I do not enjoy going to art museums.
50. I tend to vote for conservative political candidates.

Risk-Avoidance

51. I would never go hang-gliding or bungee jumping.
52. I would never make a high-risk investment.
53. I avoid dangerous situations.
54. I seek danger.
55. I am willing to try anything once.
56. I do dangerous things.
57. I enjoy being reckless.
58. I seek adventure.
59. I take risks.
60. I do crazy things.

Section 2: Decision-making style (GDMS)

Please indicate to what extent you agree or disagree with each of the following statements, according to the five-point scale below ranging from Strongly Disagree to Strongly Agree.

(1) Strongly Disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly Agree.

1. When I make decisions, I tend to rely on my intuition. *(Intuitive)*
2. I rarely make important decisions without consulting other people. *(Dependent)*
3. When I make a decision, it is more important for me to feel the decision is right than to have a rational reason for it. *(Intuitive)*
4. I double check my information sources to be sure I have the right facts before making decisions. *(Rational)*
5. I use the advice of other people in making my important decisions. *(Dependent)*
6. I put off making decisions because thinking about them makes me uneasy. *(Avoidant)*
7. I make decisions in a logical and systematic way. *(Rational)*
8. When making decisions I do what feels natural at the moment. *(Spontaneous)*
9. I generally make snap decisions. *(Spontaneous)*
10. I like to have someone steer me in the right direction when I am faced with important decisions. *(Dependent)*
11. My decision-making requires careful thought. *(Rational)*
12. When making a decision, I trust my inner feelings and reactions. *(Intuitive)*
13. When making a decision, I consider various options in terms of a specified goal. *(Rational)*
14. I avoid making important decisions until the pressure is on. *(Avoidant)*
15. I often make impulsive decisions. *(Spontaneous)*
16. When making decisions, I rely upon my instincts. *(Intuitive)*
17. I generally make decisions that feel right to me. *(Intuitive)*
18. I often need the assistance of other people when making important decisions. *(Dependent)*
19. I postpone decision-making whenever possible. *(Avoidant)*
20. I often make decisions on the spur of the moment. *(Spontaneous)*
21. I often put off making important decisions. *(Avoidant)*
22. If I have the support of others, it is easier for me to make important decisions. *(Dependent)*
23. I generally make important decisions at the last minute. *(Avoidant)*
24. I make quick decisions. *(Spontaneous)*
25. I explore all of my options before making a decision. *(Rational)*

Section 3: *Online security behaviors (SeBIS)*

Please indicate your response to the following questions based on how they apply to you.

(1) Never, (2) Rarely, (3) Sometimes, (4) Often, (5) Always.

1. When I'm prompted about a software update, I install it right away. *(Updating)*
2. I try to make sure that the programs I use are up-to-date. *(Updating)*
3. I manually lock my computer screen when I step away from it. *(Device Securement)*
4. I set my computer screen to automatically lock if I don't use it for a prolonged period of time. *(Device Securement)*
5. I use a PIN or passcode to unlock my mobile phone. *(Device Securement)*
6. I use a password/passcode to unlock my laptop or tablet. *(Device Securement)*
7. If I discover a security problem, I continue what I was doing because I assume someone else will fix it. *(Proactive Awareness)*
8. When someone sends me a link, I open it without first verifying where it goes. *(Proactive Awareness)*
9. I verify that my anti-virus software has been regularly updating itself. *(Updating)*
10. When browsing websites, I mouse over links to see where they go, before clicking them. *(Proactive Awareness)*
11. I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar. *(Proactive Awareness)*
12. I do not change my passwords, unless I have to. *(Password Generation)*
13. I use different passwords for different accounts that I have. *(Password Generation)*
14. I do not include special characters in my password if it's not required. *(Password Generation)*
15. When I create a new online account, I try to use a password that goes beyond the site's minimum requirements. *(Password Generation)*
16. I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon). *(Proactive Awareness)*

Section 4: *Risk-taking preferences (DOSPERT)*

For each of the following statements, please indicate the likelihood that you would engage in the described activity or behavior if you were to find yourself in that situation.

(1) Extremely Unlikely, (2) Moderately Unlikely, (3) Somewhat Unlikely, (4) Not Sure, (5) Somewhat Likely, (6) Moderately Likely, (7) Extremely Likely.

1. Admitting that your tastes are different from those of a friend. *(Social)*
2. Going camping in the wilderness. *(Recreational)*
3. Betting a day's income at the horse races. *(Financial)*
4. Investing 10% of your annual income in a moderate growth mutual fund. *(Financial)*
5. Drinking heavily at a social function. *(Health/Safety)*
6. Taking some questionable deductions on your income tax return. *(Ethical)*
7. Disagreeing with an authority figure on a major issue. *(Social)*
8. Betting a day's income at a high-stake poker game.
9. Having an affair with a married person. *(Ethical)*
10. Passing off somebody else's work as your own. *(Ethical)*
11. Going down a ski run that is beyond your ability. *(Recreational)*
12. Investing 5% of your annual income in a very speculative stock. *(Financial)*
13. Going whitewater rafting at high water in the spring. *(Recreational)*
14. Betting a day's income on the outcome of a sporting event. *(Financial)*
15. Engaging in unprotected sex. *(Health/Safety)*
16. Revealing a friend's secret to someone else. *(Ethical)*
17. Driving a car without wearing a seat belt. *(Health/Safety)*

18. Investing 10% of your annual income in a new business venture. *(Financial)*
19. Taking a skydiving class. *(Recreational)*
20. Riding a motorcycle without a helmet. *(Health/Safety)*
21. Choosing a career that you truly enjoy over a more prestigious one. *(Social)*
22. Speaking your mind about an unpopular issue in a meeting at work. *(Social)*
23. Sunbathing without sunscreen. *(Health/Safety)*
24. Bungee jumping off a tall bridge. *(Recreational)*
25. Piloting a small plane. *(Recreational)*
26. Walking home alone at night in an unsafe area of town. *(Health/Safety)*
27. Moving to a city far away from your extended family. *(Social)*
28. Starting a new career in your mid-thirties. *(Social)*
29. Leaving your young children alone at home while running an errand. *(Ethical)*
30. Not returning a wallet you found that contains $200. *(Ethical)*

Section 5: Demographic questions

We would like you to tell us about your background so that we can review our practices and develop new strategies to improve online security for all our community members.

1. What is your gender?
   - ( ) Male
   - ( ) Female
   - ( ) Trans male/trans man
   - ( ) Trans female/trans woman
   - ( ) Gender queer/gender non-conforming
   - ( ) Different identity
   - ( ) Decline to respond
2. What is your age? (respondents should be 18 or over) (pick one)
   - ( ) 18–24
   - ( ) 25–34
   - ( ) 35–44
   - ( ) 45–54
   - ( ) 55–64
   - ( ) 65+
3. What is your ethnicity? (check all that apply)

Are you of Hispanic, Latino, or Spanish origin?
   - ( ) No, not of Hispanic, Latino, or Spanish origin
   - ( ) Yes, Mexican, Mexican American, Chicano
   - ( ) Yes, Puerto Rican
   - ( ) Yes, Cuban
   - ( ) Yes, another Hispanic, Latino, or Spanish origin
   - ( ) Unavailable/Unknown
   - ( ) Decline to respond
4. What is your race? (check all that apply)
   - ( ) American Indian/Alaska Native
   - ( ) Asian
   - ( ) Black or African American
   - ( ) Native Hawaiian/Other Pacific Islander
   - ( ) White
   - ( ) Some other race
   - ( ) Decline to respond
   - ( ) Unavailable/Unknown
5. What is your highest level of education? (pick one)
   - ( ) Some high school
   - ( ) High school graduate
   - ( ) Some college/Currently in college (undergraduate)
   - ( ) College graduate
   - ( ) Some graduate/Currently in graduate or professional program
   - ( ) Graduate degree or professional program completed
   - ( ) Other _____
6. Are you: (pick one)
   - ( ) Not currently a student (skip 6a)
   - ( ) A student in an undergraduate program
   - ( ) A student in a graduate program
   - ( ) A student in some other type of program? Specify: _____

6.a. What is your undergraduate major or name of your graduate program? _____

7. Employment status: are you currently (check all that apply)
   - ( ) Employed for wages
   - ( ) Self-employed
   - ( ) Out of work and looking for work
   - ( ) Out of work but not currently looking for work
   - ( ) A homemaker
   - ( ) A student
   - ( ) Military
   - ( ) Retired
   - ( ) Unable to work
8. What is your marital status? (pick one)
   - ( ) Single, never married
   - ( ) Married or domestic partnership
   - ( ) Widowed
   - ( ) Divorced
   - ( ) Separated
9. Are you a citizen of the United States? (pick one)
   - ( ) Yes, born in the United States (skip 9a)
   - ( ) Yes, born in Puerto Rico, Guam, the U.S. Virgin Islands, or Northern Marianas.
   - ( ) Yes, born abroad of US citizen parent or parents
   - ( ) Yes, US citizen by naturalization. Print year of naturalization: _____
   - ( ) No

9.a. When did you come to live in the United States? (If you came to live in the US more than once, print latest year) _____

10. Do you speak a language other than English at home?
    - ( ) Yes (please answer 10a and 10b)
    - ( ) No (skip 10a and 10b)

10.a. What language(s) do you speak at home? _____

10.b. How well do you understand/read written English? (pick one)
   - ( ) Beginner
   - ( ) Intermediate
   - ( ) Advanced
   - ( ) Native proficiency

11. Rate your level of experience with computers/Internet: (pick one)
   - ( ) None
   - ( ) Beginner

- ( ) Intermediate
- ( ) Advanced
- ( ) Expert

12. Do you use any of the following types of computers? (check all that apply)
    - Desktop
      ____ yes ____ no
    - Laptop
      ____ yes ____ no
    - Tablet or other portable wireless computer
      ____ yes ____ no
    - Some other type of computer
      ____ yes ____ no
13. How many hours do you average online per day? (pick one)
    - ( ) 0–2
    - ( ) 3–4
    - ( ) 5–6
    - ( ) 7–8
    - ( ) 9 or more

REFERENCES

Appelt KC, Milch KF, Handgraaf MJJ, Weber EU. The decision making individual differences inventory and guidelines for the study of individual differences in judgment and decision-making research. Judgm Decis Mak 2011;6:252–62.

Arnett JJ. Sensation seeking, aggressiveness, and adolescent reckless behavior. Pers Individ Dif 1996;20:693–702.

Darkish A, El Zarka A, Aloul F. Towards understanding phishing victims' profile. Computer Systems and Industrial Informatics; 2012, pp. 1–5.

Egelman S, Peer E. Scaling the security wall: developing a security behavior intentions scale (SeBIS). Proceedings of the ACM Conference on Human Factors in Computing Systems, Seoul; 2015, pp. 2873–82.

Egelman S, Harbach M, Peer E. Behavior ever follows intention?: a validation of the security behavior intentions scale (SeBIS), Proceedings of the ACM Conference on Human Factors in Computing System, San Jose, CA; 2016, pp. 5257–61.

Filkins B, Hardy GM. IT Security Spending Trends. SANS Institute; 2016.

Goldberg LR, Johnson JA, Eber HW, Hogan R, Ashton MC, Cloninger CR, et al. The international personality item pool and the future of public-domain personality measures. J Res Pers 2006;40:84–96.

Halevi T, Lewis J, Memon N. A pilot study of cyber security and privacy related behavior and personality traits. Proceedings of the 22nd International Conference on World Wide Web, Rio de Janeiro; 2013, pp. 737–44.

Jeske D, Briggs P, Coventry L. Exploring the relationship between impulsivity and decision-making on mobile devices. Personal and Ubiquitous Computing; 2016, pp. 545–55.

John OP, Srivastava S. The big five trait taxonomy: history, measurement and theoretical perspectives. In: Handbook of personality, theory and research. New York/London: The Guildford Press; 1995. p. 102–38.

Kajzer M, D'Arcy J, Crowell CR, Striegel A, Van Bruggen D. An exploratory investigation of message-person congruence in information security awareness campaigns. Computers and Security, 2014, pp. 64–76.

Leach J. Improving user security behavior. Comput Secur 2003;22:685–92.

Mohebzada JG, El Zarka A, Bhojani AH, Darkish A. Phishing in a university community: two large scale phishing experiments. International Conference on Innovations in Information Technology, Abu Dhabi; 2012, pp. 249–54.

Ng B, Xu Y. Studying users' computer security behavior: a health belief perspective. Decis Support Syst 2009;46:815–25.

Parrish JL Jr, Bailey JL, Courtney JF. A personality based model for determining susceptibility to phishing attacks. Decision Sciences Institute; 2009, pp. 285–96.

Pattinson M, Jerram C, Parsons K, Mccormac A, Butavicius M. Why do some people manage phishing e-mails better than others? Information Management & Computer Security; 2012, pp. 18–28.

Riquelme I, Roman S. Is the influence of privacy and security on online trust the same for all type of consumers? Electronic Markets; 2014, pp. 135–49.

Scott SG, Bruce RA. Decision-making style: the development and assessment of a new measure. Educ Psychol Meas 1995;55:818–31.

Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the ACM Conference on Human Factors in Computing Systems, Atlanta, GA; 2010, pp. 373–82.

Shropshire J, Warkentin M, Johnston A, Schmidt M. Personality and IT security: an application of the five-factor model. Proceedings of the Twelfth Americas Conference on Information Systems, Acapulco, Mexico; 2006, pp. 3443 – 9.

Thunholm P. Decision-making style: habit, style or both? Pers Individ Dif 2004;36:931–44.

Whitty M, Doodson J, Creese S, Hodges D. Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychology, Behavior and Social Networking; 2015, pp. 3–7.

Margaret Gratian is a researcher at the Department of Defense and a PhD student in Reliability Engineering at the University of Maryland, College Park. She has a BS degree in Mathematics and Computer Science from the University of Maryland. Her research interests include evaluating and quantifying user cyber security behaviors and user susceptibility to cyber crime.

Sruthi Bandi is a quantitative data analyst who uses business analytics to influence IT investment decision-making. She holds a master's degree in Information Management and a bachelor's degree in Computer Science. She has conducted research on human behavior and information systems in the domains of health care and cyber security at the University of Maryland, College Park. She is a former software engineer and has experience developing simulators and optimization systems for thermal power plants.

Michel Cukier is an associate professor of reliability engineering with a joint appointment in the Department of Mechanical Engineering at the University of Maryland, College Park. He is also the director for the Advanced Cybersecurity Experience for Students (ACES). His research covers dependability and security issues. His latest research focuses on the empirical quantification of cyber security. Dr. Cukier has published more than 70 papers in journals and refereed conference proceedings in those areas.

Josiah Dykstra holds the PhD degree in Computer Science from the University of Maryland, Baltimore County. Dr. Dykstra is a Senior Researcher at the Laboratory for Telecommunication Sciences in College Park, Maryland. His research interests include network security, digital forensics, cloud computing, and human resilience in cyber security including augmented reality. He is a Fellow of the American Academy of Forensic Sciences and member of ACM.

Amy Ginther is an IT Specialist at the University of Maryland where she directs Project NEThics, a Division of Information Technology, Security Office group charged with promoting acceptable use of information technology and addressing misuse incidents. She supports student researchers in puzzling out ethical practice issues and administrative challenges. Usable security is a primary research interest area, including improving organizational practice through data driven decision-making. Ms. Ginther holds an MEd from the University of Vermont and worked in residential life and student conduct/academic integrity roles before moving into IT.