Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and big-five personality (#64514)

First submission

Guidance from your Editor

Please submit by **3 Dec 2021** for the benefit of the authors (and your $200 publishing discount) .

Structure and Criteria
Please read the 'Structure and Criteria' page for general guidance.

Raw data check
Review the raw data.

Image check
Check that figures and images have not been inappropriately manipulated.

Privacy reminder: If uploading an annotated PDF, remove identifiable information to remain anonymous.

Files

Download and review all files from the materials page.

7 Figure file(s)
7 Table file(s)
1 Raw data file(s)
1 Other file(s)

Structure and Criteria

Structure your review

The review form is divided into 5 sections. Please consider these when composing your review:

1. **BASIC REPORTING**
2. **EXPERIMENTAL DESIGN**
3. **VALIDITY OF THE FINDINGS**
4. General comments
5. Confidential notes to the editor

You can also annotate this PDF and upload it as part of your review

When ready submit online.

Editorial Criteria

Use these criteria points to structure your review. The full detailed editorial criteria is on your guidance page.

BASIC REPORTING

- Clear, unambiguous, professional English language used throughout.
- Intro & background to show context. Literature well referenced & relevant.
- Structure conforms to PeerJ standards, discipline norm, or improved for clarity.
- Figures are relevant, high quality, well labelled & described.
- Raw data supplied (see PeerJ policy).

EXPERIMENTAL DESIGN

- Original primary research within Scope of the journal.
- Research question well defined, relevant & meaningful. It is stated how the research fills an identified knowledge gap.
- Rigorous investigation performed to a high technical & ethical standard.
- Methods described with sufficient detail & information to replicate.

VALIDITY OF THE FINDINGS

- Impact and novelty not assessed. *Meaningful* replication encouraged where rationale & benefit to literature is clearly stated.
- All underlying data have been provided; they are robust, statistically sound, & controlled.
- Conclusions are well stated, linked to original research question & limited to supporting results.

Standout reviewing tips

The best reviewers use these techniques

Tip	*Example*
Support criticisms with evidence from the text or from other sources	*Smith et al (J of Methodology, 2005, V3, pp 123) have shown that the analysis you use in Lines 241-250 is not the most appropriate for this situation. Please explain why you used this method.*
Give specific suggestions on how to improve the manuscript	*Your introduction needs more detail. I suggest that you improve the description at lines 57- 86 to provide more justification for your study (specifically, you should expand upon the knowledge gap being filled).*
Comment on language and grammar issues	*The English language should be improved to ensure that an international audience can clearly understand your text. Some examples where the language could be improved include lines 23, 77, 121, 128 – the current phrasing makes comprehension difficult. I suggest you have a colleague who is proficient in English and familiar with the subject matter review your manuscript, or contact a professional editing service.*
Organize by importance of the issues, and number your points	*1. Your most important issue* *2. The next most important item* *3. …* *4. The least important points*
Please provide constructive criticism, and avoid personal opinions	*I thank you for providing the raw data, however your supplemental files need more descriptive metadata identifiers to be useful to future readers. Although your results are compelling, the data analysis should be improved in the following ways: AA, BB, CC*
Comment on strengths (as well as weaknesses) of the manuscript	*I commend the authors for their extensive data set, compiled over many years of detailed fieldwork. In addition, the manuscript is clearly written in professional, unambiguous language. If there is a weakness, it is in the statistical analysis (as I have noted above) which should be improved upon before Acceptance.*

Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and big-five personality

Ahmad R Pratama [Corresp., 1], **Firman M Firmansyah** [2], **Fayruz Rahma** [1]

[1] Department of Informatics, Universitas Islam Indonesia, Sleman, Daerah Istimewa Yogyakarta, Indonesia

[2] Department of Technology and Society, Stony Brook University, Stony Brook, New York, United States

Corresponding Author: Ahmad R Pratama
Email address: ahmad.rafie@uii.ac.id

Single sign-on (SSO) enables users to authenticate across multiple related but independent systems using a single username and password. While the number of higher education institutions adopting SSO continues to grow, little is known about the academic community's security awareness regarding SSO. This paper aims to examine the security awareness of SSO across various demographic groups within a single higher education institution based on their age, gender, and academic roles. Additionally, we investigate some psychological factors (i.e., privacy concerns and personality traits) that may influence users' level of SSO security awareness. Using survey data collected from 283 participants (faculty, staff, and students) and analyzed using a hierarchical linear regression model, we discovered a generational gap, but no gender gap, in security awareness of SSO. Additionally, our findings confirm that students have a significantly lower level of security awareness than faculty and staff. Finally, we discovered that privacy concerns have no effect on SSO security awareness on their own. Rather, they interact with the user's personality traits, most notably agreeableness and conscientiousness. The findings of this study laid the groundwork for future research and interventions aimed at increasing cybersecurity awareness among users of various demographic groups as well as closing any existing gaps between them.

Security Awareness of Single Sign-On Account in the Academic Community: The Roles of Demographics, Privacy Concerns, and Big-Five Personality

Ahmad R. Pratama[1], Firman M. Firmansyah[2], Fayruz Rahma[1]

[1] Department of Informatics, Universitas Islam Indonesia, Sleman, DI Yogyakarta, Indonesia
[2] Department of Technology and Society, Stony Brook University, Stony Brook, NY, USA

Corresponding Author:
Ahmad R. Pratama[1]
Jl. Kaliurang Km 14,5, Sleman, DI Yogyakarta, 55584, Indonesia
Email address: ahmad.rafie@uii.ac.id

Abstract

Background. Single sign-on (SSO) enables users to authenticate across multiple related but independent systems using a single username and password. While the number of higher education institutions adopting SSO continues to grow, little is known about the academic community's security awareness regarding SSO. This paper aims to examine the security awareness of SSO across various demographic groups within a single higher education institution based on their age, gender, and academic roles. Additionally, we investigate some psychological factors (i.e., privacy concerns and personality traits) that may influence users' level of SSO security awareness.

Methods. Primary data collected through online survey from 283 participants (faculty, staff, and students) at one of the largest private universities in Indonesia, analyzed using hierarchical linear regression models.

Results. We discovered a generational gap, but no gender gap, in security awareness of SSO. Additionally, our findings confirm that students have a significantly lower level of security awareness than faculty and staff. Finally, we discovered that privacy concerns have no effect on SSO security awareness on their own. Rather, they interact with the user's personality traits, most notably agreeableness and conscientiousness. The findings of this study laid the groundwork for future research and interventions aimed at increasing cybersecurity awareness among users of various demographic groups as well as closing any existing gaps between them.

Introduction

Single sign-on (SSO) is a cybersecurity measure that enables the use of a single username and password to authenticate the same user across multiple related but independent network, computer, or information systems. SSO enables users to log in once and access multiple services without having to enter their authentication credentials multiple times. SSO can help end users increase their productivity, while also saving money for the institution that implements it (Chinitz, 2000). Due to early performance issues, it was not until the late 2000s that SSO adoption became more widespread in a wide variety of organizations and enterprises (Lane & Marie, 2010). Nonetheless, SSO adoption was not uniform across sectors and regions of the world. Even in the early 2010s, some people still refused to adopt SSO because they did not perceive an urgent need for it although that perception changed as SSO's design and implementation improved (Sun et al., 2011).

In the academic community, particularly higher education institutions, there are at least three distinct academic roles (i.e, students, faculty, and staff) involved in various types of information systems, such as learning management systems (LMS), academic information systems (AIS), management information systems (MIS), or payroll services. Historically, colleges and universities required users to have separate accounts for each system. This situation resulted in significant frustration for the users and increased support costs for the institution. Implementing SSO resolves that issue by allowing users to log in to all systems using the same username and password.

However, along with the conveniences that SSO provides, there is an arguably greater risk associated with the fact that that same account now has access to everything the user has access to. If attackers gain access to an SSO account, they have the potential to cause additional damage, not just to the user whose SSO account was compromised, but also to other users and the institution itself. Even more so now that many universities have been forced to embrace fully online education in the aftermath of the COVID-19 pandemic, requiring everyone, including those with limited online experience, to quickly adapt to this digital transformation. As a result, safeguarding SSO accounts is becoming increasingly critical. ~~However, not all users may be initially aware of such issues.~~

While numerous studies have been conducted on security awareness, including in the academic community, little is known about the use of SSO in the academic community in general, and specifically about users' security awareness regarding their SSO accounts. This study aims to determine the level of security awareness among members of the academic community regarding SSO accounts. We are particularly interested in examining the psychological factors within individuals that can help predict their level of ~~security~~ awareness, specifically their privacy concerns and personalities, and determining whether there is any interaction between them. Additionally, we would like to determine whether the level of awareness varies by demographic characteristics (e.g., age, gender) and academic roles (i.e., student, faculty, and staff).

Demographics and Security Awareness

Among demographic variables, gender and age have been identified as significant factors that differentiate cyber security behaviors among users. For example, Anwar et al., (2017) discovered that female users are more likely than male users to have behaviors that increase the likelihood of becoming a victim of cybercrimes. For example, they tend to reuse the same passwords across multiple social media accounts, open email attachments from unknown people, and click peculiar short URLs posted on the Internet. Meanwhile, Grimes et al. (2010) discovered that older users are less familiar with cyber security measures (e.g., keeping their passwords private) and are less knowledgeable about cyber security risks (e.g., having difficulty in recognizing phishings, computer viruses, and spams). In another study, Pratama and Firmansyah (2021) revealed that females and older users were less likely to be aware of, let alone adopt, two-factor authentication (2FA), making them particularly vulnerable to cyber security threats. Taking these findings into account, we hypothesize that:

H1: Females are less aware of SSO security
H2: Older people are less aware of SSO security

It is worth highlighting that by no means do we assume that being female and older in and of itself then make people less aware of SSO security. Rather, in this study we examine whether such associations, which does not necessarily mean causation, as shown in the literature between the respected demographic variables and security awareness still exist and if they are also true in the case of SSO security. Such significant findings will expose demographic gaps needing to be addressed by future research, for instance, on why the gaps keep occurring and how to close them.

Academic Roles and Security Awareness

Most studies in cybersecurity awareness and behaviors in the academic community tend to focus on either students (Farooq et al., 2015; Ngoqo & Flowerday, 2015; Zwilling, 2020) or faculty/staff (Yerby & Floyd, 2018) only. In one study involving both academic roles, faculty/staff reported higher security behaviors than students (Gratian et al., 2018). Taking that into account and due to the nature of the role that faculty and staff usually have more systems and data to access within an academic institution, and thus more to lose than students should their SSO accounts be compromised, we hypothesize that:

H3: Students are less aware of SSO security than faculty and staff

SSO Familiarity and Security Awareness

SSO adoption in higher education is relatively new compared to the other domains, especially those engaged in industrial and commercial activities. In this particular institution where the study was conducted, SSO was not fully adopted until 2019, just a few months prior to the onset of COVID-19 pandemic. Taking that into account, we hypothesize that:

H4: Familiarity to SSO positively predicts SSO security awareness

Privacy Concerns and Security Awareness

Individual concerns over what, when, and how their private information is being shared to others when using information technology products and services have been widely discussed in the literature (Petronio & Child, 2020). For instance, multiple studies have revealed that the privacy paradox, discrepancy between stated privacy attitudes and actual privacy behaviors, in using the technologies does exist in various contexts and across cultures (Aleisa, 2020; Barth et al, 2019; Kokolakis, 2017). Some argue that this phenomenon can be explained by privacy calculus, which reflects the discrepancy between anticipated risks and expected benefits associated with letting go of some private information (e.g. Goad, 2021). Should the benefits be higher, users tend to compromise their privacy, and to hold it otherwise. These arguments suggest that privacy concerns lead to more cautious decisions in whether to use information technology related products or services. Bringing this finding to the current study's context, we predict that ~~privacy concerns are positively associated with SSO security awareness since users with higher privacy tend to be more cautious and sensitive with technology use.~~

H5: Privacy concerns positively predict SSO security awareness

Privacy Concerns and Security Awareness

SSO adoption in higher education is relatively new compared to the other domains, especially those engaged in industrial and commercial activities. In this particular institution where the study was conducted, SSO was not fully adopted until 2019, just a few months prior to the onset of COVID-19 pandemic. Taking that into account, we hypothesize that:

H4: Familiarity to SSO positively predicts SSO security awareness

Big-Five Personality and Security Awareness

Past psychological research has revealed the association between individual traits, which are parts of the Big-Five personality as shown in Table 1 (Gosling et al, 2003), and cyber security behavior. For instance, Russel et al. (2017) found negative correlations between emotional instability (neuroticism) and secure cyber behaviors (e.g., using protection software against malware and virus) and between conscientiousness and insecure cyber behaviors (e.g., using unsecured wireless networks). Whereas Shappie et al. (2020) revealed that in addition to conscientiousness, agreeableness and openness positively predict cybersecurity behaviors (e.g., keeping anti-virus software up to date). Meanwhile, Kennison and Chan-Tin (2020) reported rather different results: extraversion, agreeableness, and emotional stability -not openness nor conscientiousness- explain why some users are prone to commit risky cyber behaviors (e.g., not signing out of a shared computer, sharing password with someone else) while others are not. It appears that the relationships between Big-Five personality traits and cybersecurity awareness seem to vary across contexts and depend on the indicators measured in the study. However, in

terms of SSO security awareness, and also by taking into consideration the Indonesian context as a collectivist country, we argue that being extraverted and agreeable is associated with lower SSO security awareness. Users having these traits are more likely to share their passwords with someone else, either voluntarily out of trust or when asked by others they respect or fear due to social status. On the other hand, we argue that being conscientious, emotionally stable, and open is associated with higher SSO security awareness. Users having these traits are arguably more cautious in their decision making and thus will avoid risky behavior with their SSO accounts. Thus, our hypotheses are as follows:

H6: Extraversion negatively predicts SSO awareness
H7: Agreeableness negatively predicts SSO awareness
H8: Conscientiousness positively predicts SSO awareness
H9: Emotional stability positively predicts SSO awareness
H10: Openness positively predicts SSO awareness

Furthermore, since past studies reported significant correlations between agreeableness and privacy concerns (Korzaan & Boswell, 2008), and between conscientiousness and privacy concerns (Junglass et al., 2008), we thus expect the aforementioned variables will interact with each other in predicting SSO security awareness. As such, our two final hypotheses are as follows:

H11: Agreeableness interacts with privacy concerns in predicting SSO security awareness
H12: Conscientiousness interacts with privacy concerns in predicting SSO security awareness

Materials & Methods

Participants

After obtaining approval from the Directorate of Research and Community Services within the university (No: 01.A/DirDPPM/70/DPPM/I/2021), we sent out a link to an online survey through broadcast email and WhatsApp messages to the academic community at one of the largest private universities in Indonesia in May 2021. A total of 283 participants ranging from 17 to 59 years of age (M = 26.63, SD = 10.23) completed the survey after providing their consents. The questionnaire was delivered in Bahasa Indonesia (see Supplementary Materials). More information about the demographics of respondents is available in Table 2.

Measures

Apart from the three demographic variables (i.e., gender, age, and academic role), there are three independent variables (i.e., SSO familiarity, privacy concerns, and Big-Five personality) and one dependent variable (SSO account security awareness) in this study. Table 3 summarizes

some variables of interest along with their respective measurement items that we developed for this particular study.

SSO Familiarity. We developed three items to measure how well users are familiar with the SSO system in their university. The three items cover their overall knowledge of SSO along with its features and risk. We then aggregated the three items to calculate a composite score of SSO familiarity in the range of 0 to 100.

Privacy Concerns. We developed five items to measure user privacy concerns by adopting from the work of Buchanan et al. (2007). Specifically, we included only items related to user accounts. We also calculated a composite score of privacy concerns in the range of 0 to 100 by aggregating all five items.

SSO Account Security Awareness. To measure SSO Account Security Awareness in this study, we adopted the Human Aspects of the Information Security Questionnaire (HAIS-Q) (Parsons et al., 2017) in developing five items for each one of the Knowledge, Attitude, and Behavior dimension, yielding 15 measurement items in total. We then calculated a composite score of SSO account security awareness in the range of 0 to 100 by using the weighted average method (30% for Knowledge, 20% for Attitude, and 50% for Behavior) to be classified further into three categories, i.e., "Poor" (< 60), "Average" (60-79.99), and "Good" (≥ 80) as recommended by Kruger and Kearney (2006).

Data Analysis

We employed hierarchical linear regression in R 3.6.3 to analyze the data. As illustrated in Figure 1, we conducted three steps of regression analysis with some additional independent variables in each model. In the first regression, we included only SSO familiarity and privacy concerns in addition to the three demographic variables (i.e., gender, age, and academic role) as the predictors. Next, we introduced the Big-Five personality variables to the model in the second regression. Finally, we added the interaction terms between privacy concerns and two out of five Big-Five personality variables (i.e., agreeableness and conscientiousness) in the third regression. We ran several diagnostic tests to the regression model and identified two outliers and influential cases that we then omitted prior to repeating the hierarchical regression analysis. The R code and the dataset will be made available on our GitHub repository.

Results

The summary statistics are provided in Table 4 for the dependent variable and in Table 5 for the independent variables. As can be seen, the average SSO security awareness score for all participants in this study is 69.31 out of 100, which falls into the "Average" category according to the rubric by Kruger and Kearney (2006). When considering each individual measurement item, the mean for the majority of items ~~is indeed~~ between 60 and 79.99. Certain items relating to

password reuse (K1, A1), password length (K4, A4), and the use of incognito mode on a shared device (B5) are classified as "Poor", while others relating to account sharing (K2, A2, B2) and password complexity (K3) are classified as "Good". Applying the same categorization to SSO familiarity (i.e., 80.86 out of 100) and privacy concerns (i.e., 85.90 out of 100), however, means they both fall into the "Good" category.

The scatterplots in Figure 2 illustrate how SSO security scores vary by demographic variables. As can be seen, the SSO security awareness scores and age tend to form a negative linear relationship. This relationship is typically consistent across genders and academic roles. Additionally, the dumbbell plots in Figure 3 and Figure 4 indicate that SSO security awareness is relatively consistent across genders, but not across academic roles. Students consistently demonstrated significantly lower levels of knowledge, attitude, and behavior regarding SSO account security compared to faculty and staff. Apart from their score in attitude that is much lower and closer to student's score, staff scored fairly close to faculty in terms of knowledge and behavior, resulting in no significant differences in total score between the two.

Following that, Table 6 summarizes the results of the hierarchical regression analysis. As can be seen, all independent variables, with the exception of gender, were found to be statistically significant in the first regression and they remained significant in the second regression after the addition of Big-Five personality traits as independent variables in the model. While only one of the five personality traits was found to be statistically significant in the second regression, the addition of interaction terms with privacy concerns in the third regression altered this finding. As it turned out, statistical significance was found for all but one of the Big-Five personality traits (i.e., openness). With the addition of these interaction terms, another significant finding emerged: privacy concerns were no longer significant predictors of SSO security awareness on their own. Rather than that, they interact with agreeableness and conscientiousness, the final model's two strongest predictors. The interaction between privacy concerns and Big-Five personality traits in predicting SSO security awareness is depicted in Figure 3 for agreeableness and Figure 4 for conscientiousness.

Taking all of the preceding findings into account, Table 7 summarizes the results of hypothesis tests. ~~Meanwhile,~~ Figure 7 illustrates the final model based on those findings.

Discussion

Demographics and SSO Security Awareness

~~Our analysis~~ results ~~have~~ confirmed all demographic hypotheses except for gender. Even more so, the association between gender and SSO security awareness remains non-significant after putting psychological factors as well as their interaction terms with privacy concerns into the equation. These unexpected findings contradict past research reporting that female users tend to be less aware of cyber security measures (Anwar et al., 2017; Pratama & Firmansyah, 2021). Considering that this study takes place within a single higher education institution, it could be the case that both male and female users have already been exposed to similar levels of SSO usage within their institution. Ergo, such gender distinctions have no bearing on their security

awareness. The absence of statistically significant differences in SSO security awareness between males and females in this study is encouraging because it demonstrates that organizations can rely on both male and female users having the same level of SSO security awareness. It could also be attributed to the organization's success in educating users regardless of their gender.

On the other hand, past research indicating gender gap in cybersecurity awareness either took place in a workplace in which participants' chances to get exposed to such cyber measures might vary (Anwar et al., 2017) or their participants came from different places altogether (Pratama & Firmansyah, 2021). Those having IT related backgrounds and working directly with external clients might be more aware of cyber threats compared to those having no IT backgrounds and working with internal clients only. Considering that females are still underrepresented in IT related jobs (Richter, 2021), it could be the main reason why such a gender gap existed in past research. As such, we argue that any study revealing a gender disparity in cybersecurity awareness should delve deeper into the reason for it than simply gender.

Contrary to gender, the generational gap remains present in this study. While arguments from prior research that older people did not get the same chance as younger people did in terms of digital literacy exposure including cyber security measures (Grimes et al., 2010) may still hold water, this finding brings a more serious issue in this study's context. In Indonesia, which may also be true in many other countries, age arguably correlates with job seniority position. Putting this into the context of SSO, therefore, the older the users, the more systems and information are at risk should any cybersecurity incidents happen. Linking with our previous argument that users of the same educational setting should arguably receive similar exposure, it could be the case that such programs used by the IT department in introducing SSO technology and its security may not well address their older users yet. In other words, they seem to work effectively only for younger generations. The fact that SSO familiarity significantly predicts SSO awareness further supports our argument.

Our findings also highlight that~~,~~ students are indeed less aware of SSO security compared to staff and faculty, whereas no significant difference in SSO security awareness exists between staff and faculty. On one hand, it can be the case because they have less things to lose if such incidents happen. As Pratama and Firmansyah (2021) argue, how sensitive people are to cyber threats and how well they adhere to cyber security measures is directly proportional to the magnitude of their potential losses should such incidents occur. Students, arguably, have less to lose in regard to their SSO account. On the contrary, faculty and academic staff have a plethora of sensitive data at risk, ranging from financial and salary information to any other private or confidential data, both to them as users and to their institution. As such, it is unsurprising that faculty and staff are more cognizant of SSO account security than students are. On the other hand, the fact that students are significantly less aware of SSO account security also leads to another suspicious behavior. Some students might intentionally share their SSO accounts. While it is unethical to suspect all students, taking into consideration that academic cheating is perceived as collaboration, not competition, in such collectivistic cultures like in Indonesia (Jamaluddin et al.,

2020), the possibility that a few students intentionally misuse their SSO accounts for academic dishonesty cannot be ruled out.

Privacy Concerns, Big-Five Personality, and SSO Security Awareness

As expected, privacy concerns are positively associated with SSO security awareness, at least in the first two regressions. Holding all other variables constant, the more concerned users are about their privacy, the more aware they are of SSO security. Interestingly, when we factor in their interaction with the Big-Five personality constructs, this association becomes irrelevant. In other words, the extent to which privacy concerns may affect users' SSO security awareness is determined by their personality traits. Users with a high degree of agreeableness (i.e., warm, not critical) are generally less aware of SSO security, but this would change if they also had increased privacy concerns. On the contrary, users who are naturally conscientious (i.e., organized, cautious) tend to have a high level of security awareness regarding their SSO accounts regardless of their privacy concerns, even if the latter can help those with a low degree of conscientiousness improve their security awareness. In this regard, regardless of their level of privacy concerns, it is the users' personality that naturally compels them to be more circumspect and critical, thereby increasing their awareness of the risks associated with their SSO accounts. In contrast to the two aforementioned traits, extraversion and emotional stability account for SSO security awareness in ways that go beyond privacy concerns. In this regard, the more extraverted users are, the less aware they are of SSO security. By contrast, users who are emotionally stable are more likely to be aware of SSO security. Interestingly, even after controlling for demographic and privacy concerns variables, only the openness trait has no significant association with SSO security awareness. Our attempt to determine whether there are any interactions between these three characteristics and privacy concerns, which revealed none, confirms that these findings are robust.

These findings altogether suggest the needs of a tailored approach should interventions be designed to increase users' SSO security awareness. For example, intervention emphasizing privacy risk may work best for users with a high degree of agreeableness but is less efficient for users with high degree of conscientiousness. While for users with a high degree of emotional stability, it may be better to teach them about SSO security measures. A particular attention should be paid to users with extraverted traits. Some conventional interventions may not work as effectively as it is for other personality traits. Perhaps, such further behavioral interventions may be needed. We suggest future research to explore this area more to shed light on different types of education and interventions that can work better for different types of personality traits.

Conclusions

Our study discovered unique relationships between SSO security awareness, demographic characteristics, privacy concerns, and personality traits. The degree to which users are aware of SSO security varies according to their demographic characteristics and is determined by their personality traits, some of which (i.e., agreeableness and conscientiousness) interact with their

level of privacy concerns. The absence of gender disparities in SSO security awareness in this study suggests that the gap can be closed under the right circumstances, including but not limited to education and policy. It also suggests that closing generational gaps may be a greater challenge than closing gender gaps in cybersecurity awareness.
Additionally, this study lays the groundwork for future research and interventions aimed at increasing user awareness of SSO security and closing any existing gaps between different demographic groups of users, particularly in higher education settings. With the growing adoption of SSO by colleges and universities worldwide, addressing this issue of SSO security awareness is becoming increasingly important. Finally, we propose researchers to conduct similar studies in other parts of the world to account for cultural differences that may affect cybersecurity awareness, particularly regarding SSO security.

Acknowledgements

-

References

Akhtar, H. (2018). Translation and validation of the Ten-Item Personality Inventory (TIPI) into Bahasa Indonesia. International Journal of Research Studies in Psychology, 7, 59-69. DOI: 10.5861/ijrsp.2018.3009

Aleisa, N., Renaud, K., & Bongiovanni, I. (2020). The privacy paradox applies to IoT devices too: A Saudi Arabian study. *Computers & Security*, *96*, 101897. https://doi.org/10.1016/j.cose.2020.101897

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics*, *41*, 55-69. https://doi.org/10.1016/j.tele.2019.03.003

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. Journal of the American society for information science and technology, 58(2), 157-165.

Chinitz, J. (2000). Single sign-on: Is it really possible? *Information Systems Security, 9*(3), 1–14. https://doi.org/10.1201/1086/43310.9.3.20000708/31359.5

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information security awareness in educational institution: An analysis of students' individual factors. In 2015 IEEE Trustcom/BigDataSE/ISPA (Vol. 1, pp. 352-359). IEEE.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology, 36*(3), 173-192. https://doi.org/10.1080/03601270903183065

Goad, D., Collins, A. T., & Gal, U. (2021). Privacy and the Internet of Things− An experiment in discrete choice. *Information & Management*, *58*(2), 103292. https://doi.org/10.1016/j.im.2020.103292

Gosling, S. D., Rentfrow, P. J., & Swann, W. B., Jr. (2003). A very brief measure of the Big Five personality domains. *Journal of Research in Personality, 37*, 504-528. https://doi.org/10.1016/S0092-6566(03)00046-1

Kennison, S. M., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Frontiers in Psychology*, *11*, 2020. https://doi.org/10.3389/fpsyg.2020.546546

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, *48*(4), 15-24.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Jamaluddin, S. F., Adi, S. P., & Lufityanto, G. (2020). Social influences on cheating in collectivistic culture: Collaboration but not competition. *Group Dynamics: Theory, Research, and Practice*. https://doi.org/10.1037/gdn0000122

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387-402. https://doi.org/10.1057/ejis.2008.29

Lane, M., & Marie, M. (2010). The adoption of single sign-on and multifactor authentication in organisations-A critical evaluation using TOE framework. *Information in Motion, 7*, 161.

Ngoqo, B., & Flowerday, S. V. (2015). Exploring the relationship between student mobile information security awareness and behavioural intent. *Information & Computer Security, 23*(4), 406-420. https://doi.org/10.1108/ICS-10-2014-0072

Parsons, K., Calic, D., Pattinson, M., Butavičius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security, 66*, 40-51.

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology*, *31*, 76-82. https://doi.org/10.1016/j.copsyc.2019.08.009

Pratama, A. R., & Firmansyah, F. M. (2021). Until you have something to lose! Loss aversion and two-factor authentication adoption. *Applied Computing and Informatics, early cite*. https://doi.org/10.1108/ACI-12-2020-0156

Richter, F. (2021, July 1). *Women's Representation in Big Tech*. Statista Infographics. https://www.statista.com/chart/4467/female-employees-at-tech-companies/

Russell, J. D., Weems, C. F., Ahmed, I., & Richard III, G. G. (2017). Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. *Journal of Cyber Security Technology*, *1*(3-4), 163-174. https://doi.org/10.1080/23742917.2017.1345271

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 475-480. https://doi.org/10.1037/ppm0000247

Sun, S. T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2011). What makes users refuse web single sign-on? An empirical investigation of OpenID. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (pp. 1-20).

Yerby, J., & Floyd, K. (2018). Faculty and staff information security awareness and behaviors. *Journal of The Colloquium for Information Systems Security Education, 6*(1), 23-23.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 1-16. https://doi.org/10.1080/08874417.2020.1712269

Table 1(on next page)

Big-Five Personality and some trait examples

Table 1 Big-Five Personality ~~and some trait examples~~

Personality	Traits
Extraversion	Enthusiastic, not reserved, extraverted, not quiet
Agreeableness	Not critical, sympathetic, warm, not quarrelsome
Conscientiousness	Organized, careful, dependable, self-disciplined
Emotional stability	Not anxious, not easily upset, calm, emotionally stable
Openness	Creative, not conventional, open to new experience, complex

Table 2(on next page)

Demographic information of all participants (N=283)

Table 2. Demographic information of all participants (N=283)

Variable	Frequency	Percentage
Gender		
- Male	148	52%
- Female	135	48%
Age		
- ≤ 19 years old	72	25%
- 20-29 years old	132	47%
- 30-39 years old	38	13%
- 40-49 years old	31	11%
- ≥ 50 years old	10	4%
Academic Role		
- Student	197	70%
- Faculty member	34	12%
- Staff	52	18%

Table 3(on next page)

Variables of interest and measurement items

reverse items (*) were inverted prior to calculation

1 Table 3. Variables of interest and measurement items

Variable	Code
Familiarity with SSO	**F**
1. I know what the university's SSO account is.	F1
2. I know what systems and data are accessible with my university's SSO account.	F2
3. I am aware of the risk of negative impacts if my university's SSO account is used by other people.	F3
Privacy concerns	**Pr**
1. In general, how concerned are you about your privacy while you are using the internet?	Pr1
2. Are you concerned about online organizations not being who they claim they are?	Pr2
3. Are you concerned about online identity theft?	Pr3
4. Are you concerned about people online not being who they say they are?	Pr4
5. Are you concerned that an email you send may be read by someone else besides the person you sent it to?	Pr5
Knowledge	**K**
1. Using the same password for the university's SSO account and other personal accounts like social media is not prohibited.	K1r*
2. Sharing my password for the university's SSO account to other people, including friends or colleagues, is not prohibited.	K2r*
3. A combination of uppercase, lowercase, numbers, and special characters is a must when choosing password, including for the university's SSO account.	K3
4. Using a password that is 8 characters long or shorter is not prohibited.	K4r*
5. When signing-in to the university account through the SSO system on a device that is not my own, using the incognito or private mode in the web browser is necessary.	K5
Attitude	**A**
1. It is safe enough to use the same password for the university's SSO account and other personal accounts like social media.	A1r*
2. Sharing my password for the university's SSO account to other people, including friends or colleagues, is a bad idea.	A2
3. It is safe enough to use a password that consists of a combination of only alphabets, including for the university's SSO account.	A3r*
4. It is safe enough to use a password that is 8 characters long or shorter, including for the university's SSO account.	A4r*
5. Signing into the university's SSO account on a device that is not my own without using the incognito or private mode in the web browser is risky.	A5

Behavior	**B**
1. I use a different password for the university's SSO account than my other personal accounts like social media.	B1
2. I share my password for the university's SSO account with friends or colleagues at the university.	B2r*
3. I use a combination of uppercase, lowercase, numbers, and special characters for all my passwords, including the university's SSO account.	B3
4. I always use passwords that are more than 8 characters long, including for the university's SSO account.	B4
5. I hardly ever use incognito or private mode in the web browser when signing into the university's SSO account on a device that is not my own.	B5r*
Security Awareness Score	**Score**

Note: reverse items (*) were inverted prior to calculation

2

Table 4(on next page)

Summary statistics of the dependent variable

1 Table 4. Summary statistics of the dependent variable

Variable	Mean	SD
Knowledge (0-100)	**66.91**	**16.26**
K1: password reuse	47.00	34.59
K2: sharing SSO account	82.86	26.00
K3: password complexity	84.28	25.18
K4: password length	46.38	33.32
K5: incognito mode	74.03	26.07
Attitude (0-100)	**62.69**	**18.90**
A1: password reuse	51.50	33.32
A2: sharing SSO account	80.83	28.97
A3: password complexity	60.51	30.11
A4: password length	42.84	31.29
A5: incognito mode	77.74	24.35
Behavior (0-100)	**73.41**	**14.96**
B1: password reuse	77.56	27.37
B2: sharing SSO account	86.31	23.45
B3: password complexity	78.45	24.72
B4: password length	75.00	26.46
B5: incognito mode	49.73	31.54
Composite Score (0-100)	**69.31**	**13.62**

Note: reverse items (*) were inverted prior to calculation

2

Table 5(on next page)

Summary statistics of the independent variables

Table 5. Summary statistics of the independent variables

Variable	Mean	SD
Familiarity with SSO (0-100)	**80.86**	**18.56**
F1: know what SSO is	82.60	20.19
F2: know what systems and data are accessible with SSO	77.12	23.06
F3: aware of the risk of SSO account being used by others	82.86	23.40
Privacy Concerns (0-100)	**85.90**	**14.54**
P1: general privacy concerns on the Internet	79.95	20.46
P2: false identity of organizations online	84.72	20.59
P3: online identity theft	84.28	20.20
P4: false identity of other individuals online	93.11	14.78
P5: confidentiality of messages	87.46	19.57
Big-Five Personality (1-7)		
Extraversion	4.14	1.18
Agreeableness	5.30	1.03
Conscientiousness	5.14	1.05
Emotional Stability	4.71	1.20
Openness	5.33	1.07

Table 6(on next page)

Estimates from hierarchical regression analysis

* Faculty member is used as the reference category;

numbers in blue indicate $p < .05$

Table 6. Hierarchical regression analysis

Predictor Variables	Regression 1				Regression 2				Regression 3			
	B	**SE B**	**β**	***p***	**B**	**SE B**	**β**	***p***	**B**	**SE B**	**β**	***p***
Constant	63.37	8.68	-	<.001	67.83	9.49	-	<.001	71.46	25.67	-	.006
Gender (Male)	-0.14	1.55	-0.01	.931	-0.77	1.57	-0.03	.625	-0.82	1.54	-0.03	.592
Age	**-0.36**	**0.14**	**-0.28**	**.010**	**-0.34**	**0.14**	**-0.26**	**.013**	**-0.35**	**0.14**	**-0.27**	**.011**
Academic Role *												
- Staff	-2.40	2.80	-0.07	.391	-2.77	2.77	-0.08	.317	-2.87	2.73	-0.08	.294
- Student	**-13.79**	**3.50**	**-0.48**	**<.001**	**-12.88**	**3.46**	**-0.45**	**<.001**	**-13.25**	**3.42**	**-0.46**	**<.001**
Familiarity with SSO Account	**0.11**	**0.04**	**0.16**	**.007**	**0.10**	**0.04**	**0.14**	**.023**	**0.10**	**0.04**	**0.14**	**.024**
Privacy concerns	**0.15**	**0.06**	**0.17**	**.007**	**0.15**	**0.06**	**0.16**	**.010**	0.11	0.29	-0.12	.692
Big-Five Personality												
- Extraversion					**-1.47**	**0.66**	**-0.13**	**.027**	**-1.31**	**0.65**	**-0.12**	**.046**
- Agreeableness					-0.93	0.86	-0.07	.282	**-16.11**	**5.04**	**-1.22**	**.002**
- Conscientiousness					1.57	0.87	0.12	.074	**15.43**	**5.41**	**1.21**	**.005**
- Emotional Stability					1.37	0.79	0.12	.085	**1.63**	**0.79**	**0.15**	**.038**
- Openness					-0.73	0.83	-0.06	.385	-0.73	0.82	-0.06	.378
Interaction Terms												
- Privacy concerns x Agreeableness									**0.17**	**0.06**	**1.56**	**.003**
- Privacy concerns x Conscientiousness									**-0.16**	**0.06**	**-1.42**	**.011**
Observations	280				280				280			
df	273				268				266			
p	<.001				<.001				<.001			
R^2	0.125				0.170				0.201			

Adjusted R^2	0.106	0.136	0.162
ΔR^2	-	0.045	0.031
ΔAdjusted R^2	-	0.030	0.026

Note: * Faculty member is used as the reference category; numbers in blue indicate $p < .05$

Table 7 (on next page)

Summary of hypothesis tests results

Table 7. Summary of hypothesis tests results

Hypothesis	Relationship	Result
H1	Females are less aware of SSO security	Not supported
H2	Older people are less aware of SSO security	Supported
H3	Students are less aware of SSO security than faculty and staff	Supported
H4	Familiarity to SSO positively predicts SSO security awareness	Supported
H5	Privacy concerns positively predict SSO security awareness	Not supported
H6	Extraversion negatively predicts SSO awareness	Supported
H7	Agreeableness negatively predicts SSO awareness	Supported
H8	Conscientiousness positively predicts SSO awareness	Supported
H9	Emotional stability positively predicts SSO awareness	Supported
H10	Openness positively predicts SSO awareness	Not supported
H11	Agreeableness interacts with privacy concerns in predicting SSO security awareness	Supported
H12	Conscientiousness interacts with privacy concerns in predicting SSO security awareness	Supported

Figure 1

Conceptual model of SSO account security awareness in this study

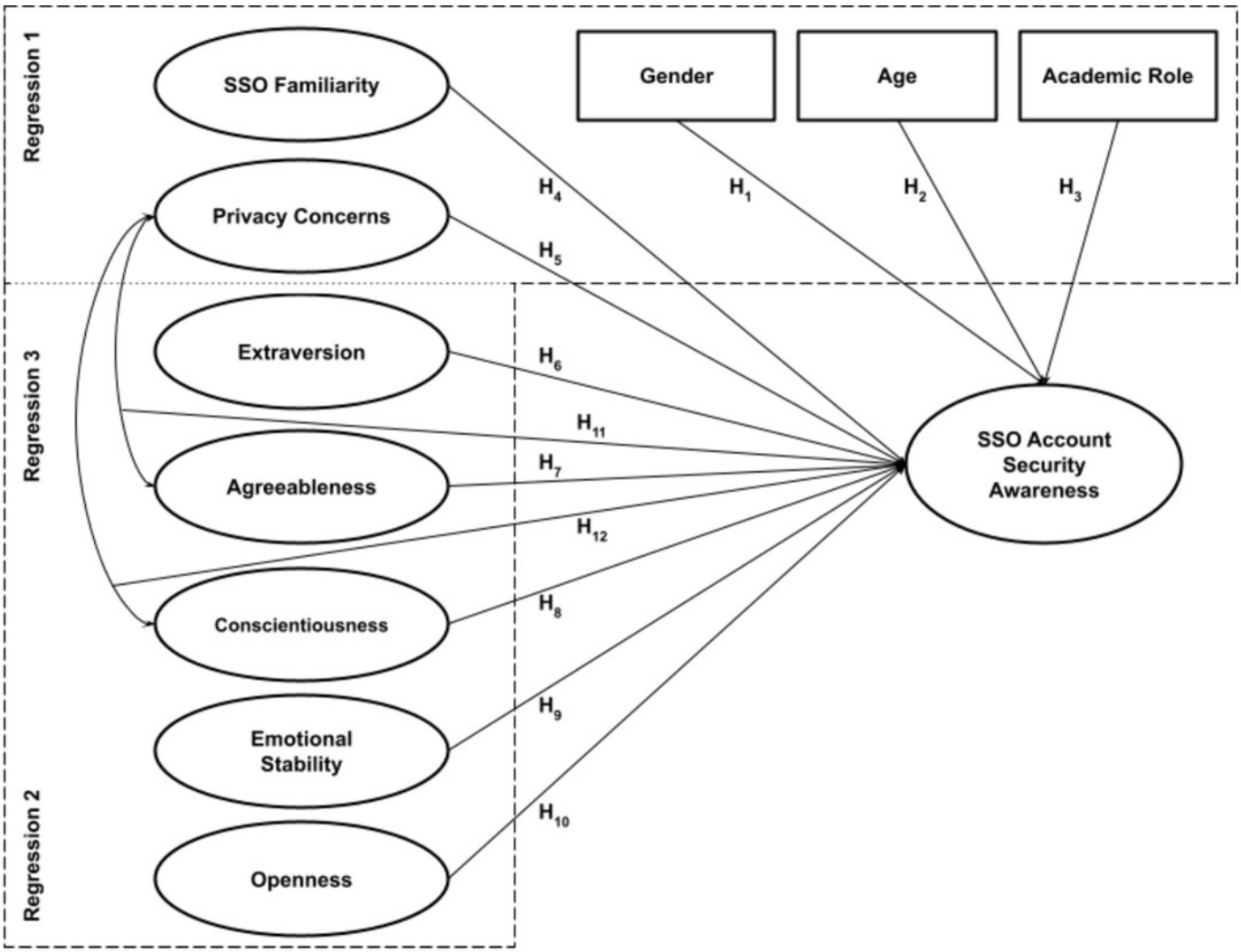

Figure 2

Scatterplots of SSO security awareness score by age, gender, and academic roles

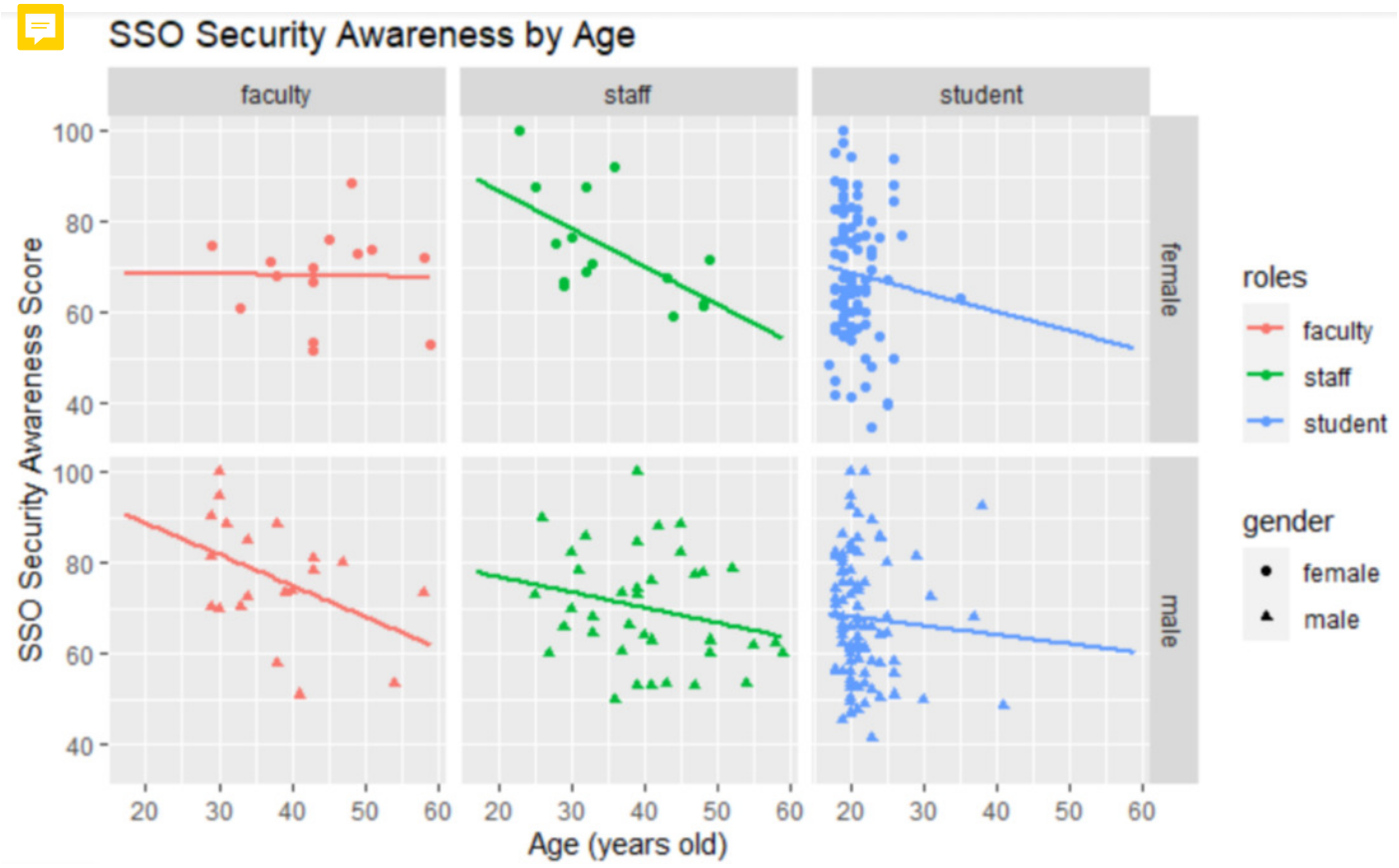

Figure 3

Dumbbell plots of SSO security awareness by gender

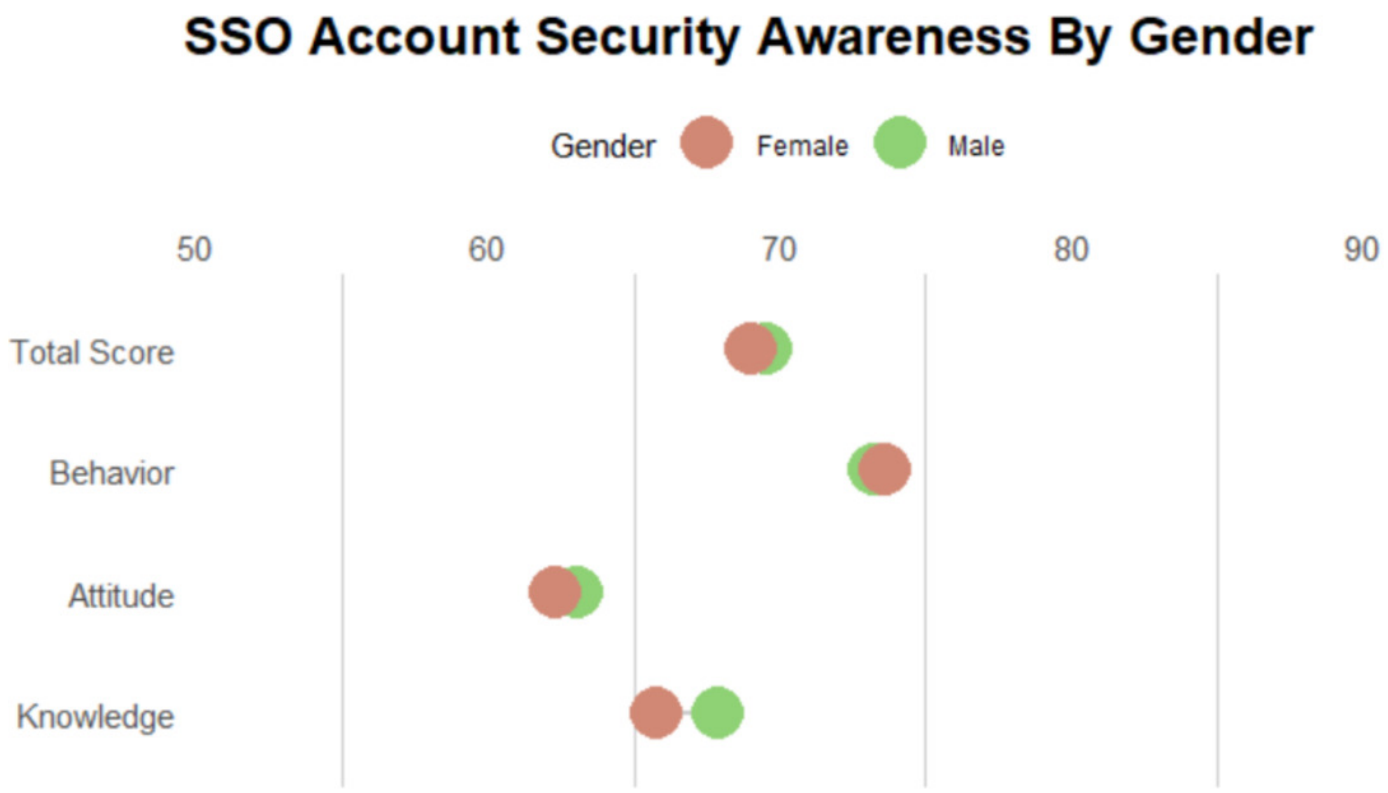

Figure 4

Dumbbell plots of SSO security awareness by academic roles

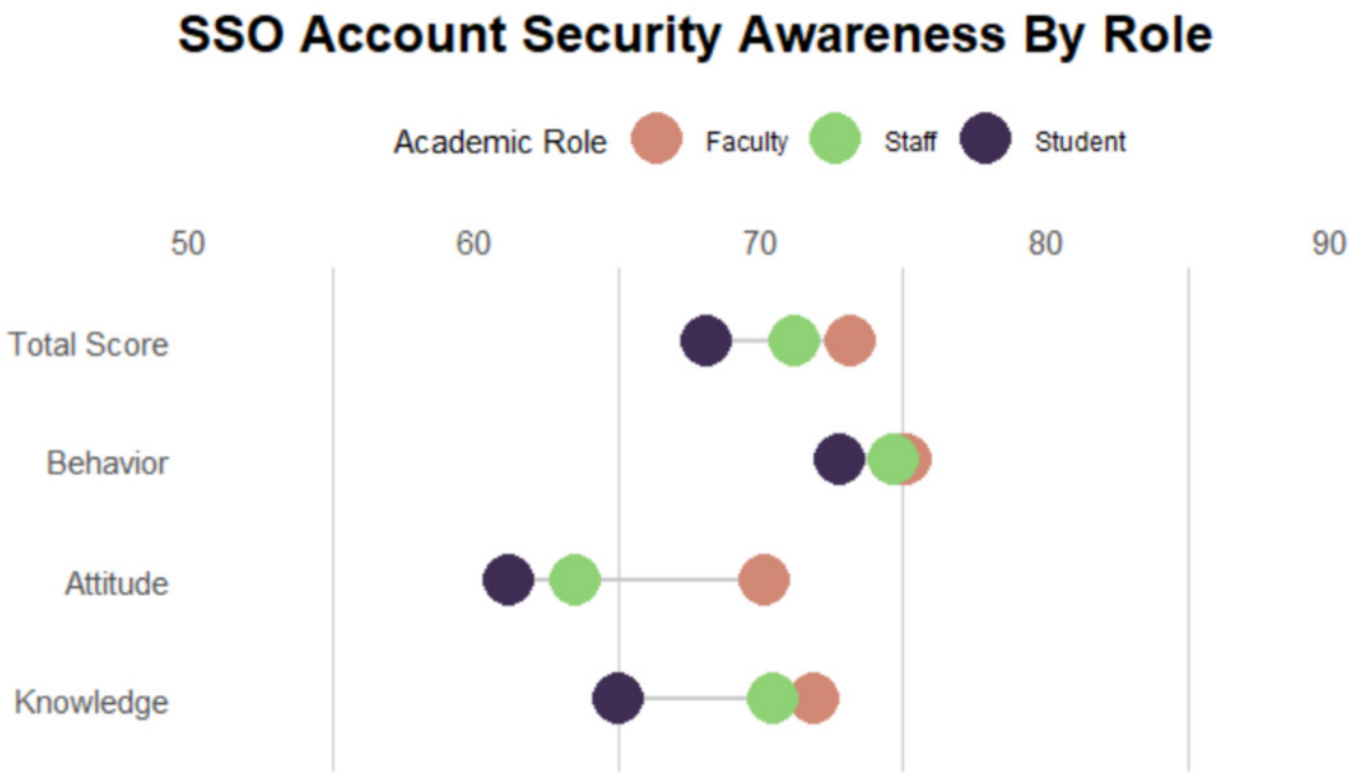

Figure 5

Marginal effects of the interaction terms between privacy concerns and agreeableness

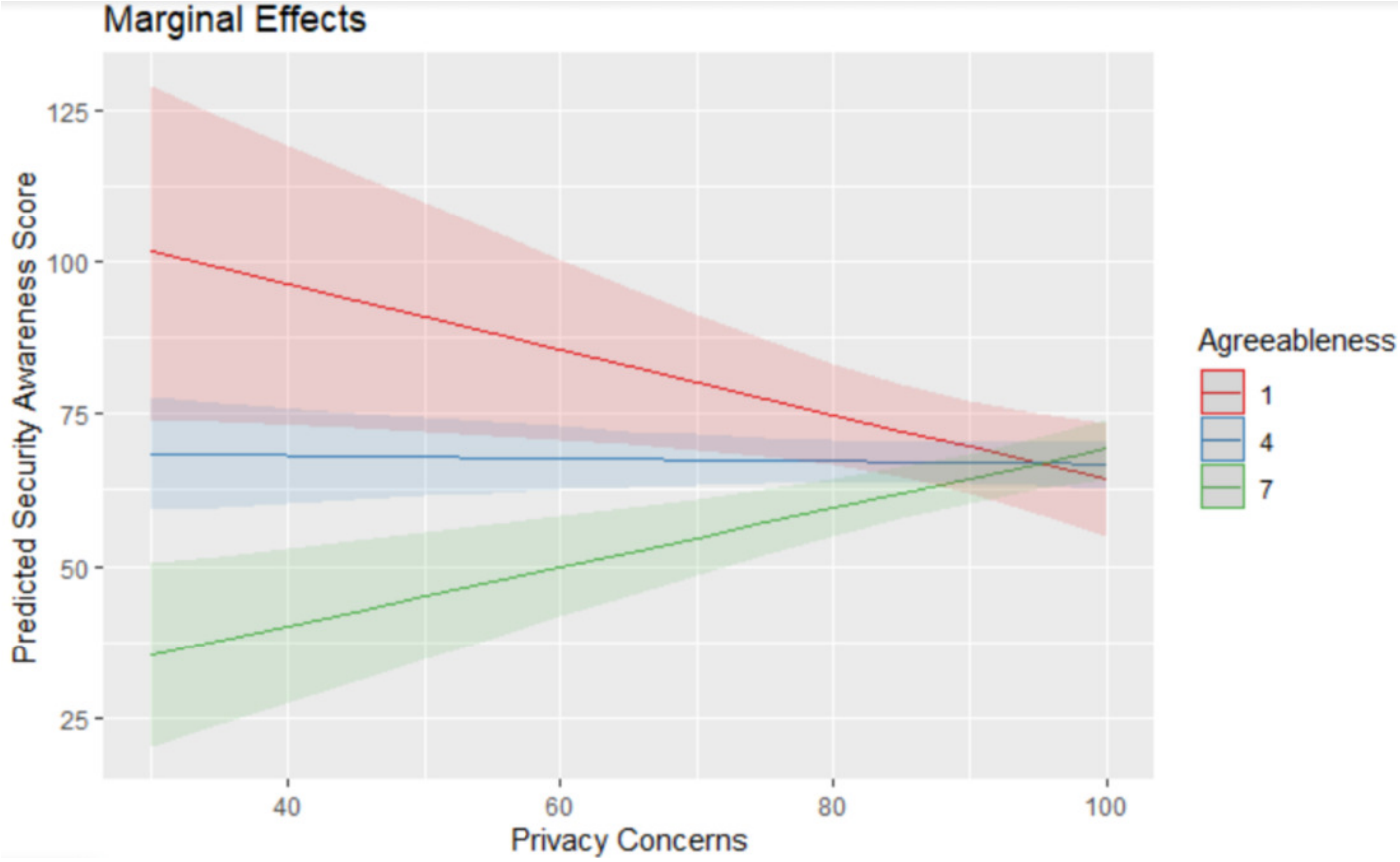

Figure 6

Marginal effects of the interaction terms between privacy concerns and conscientiousness

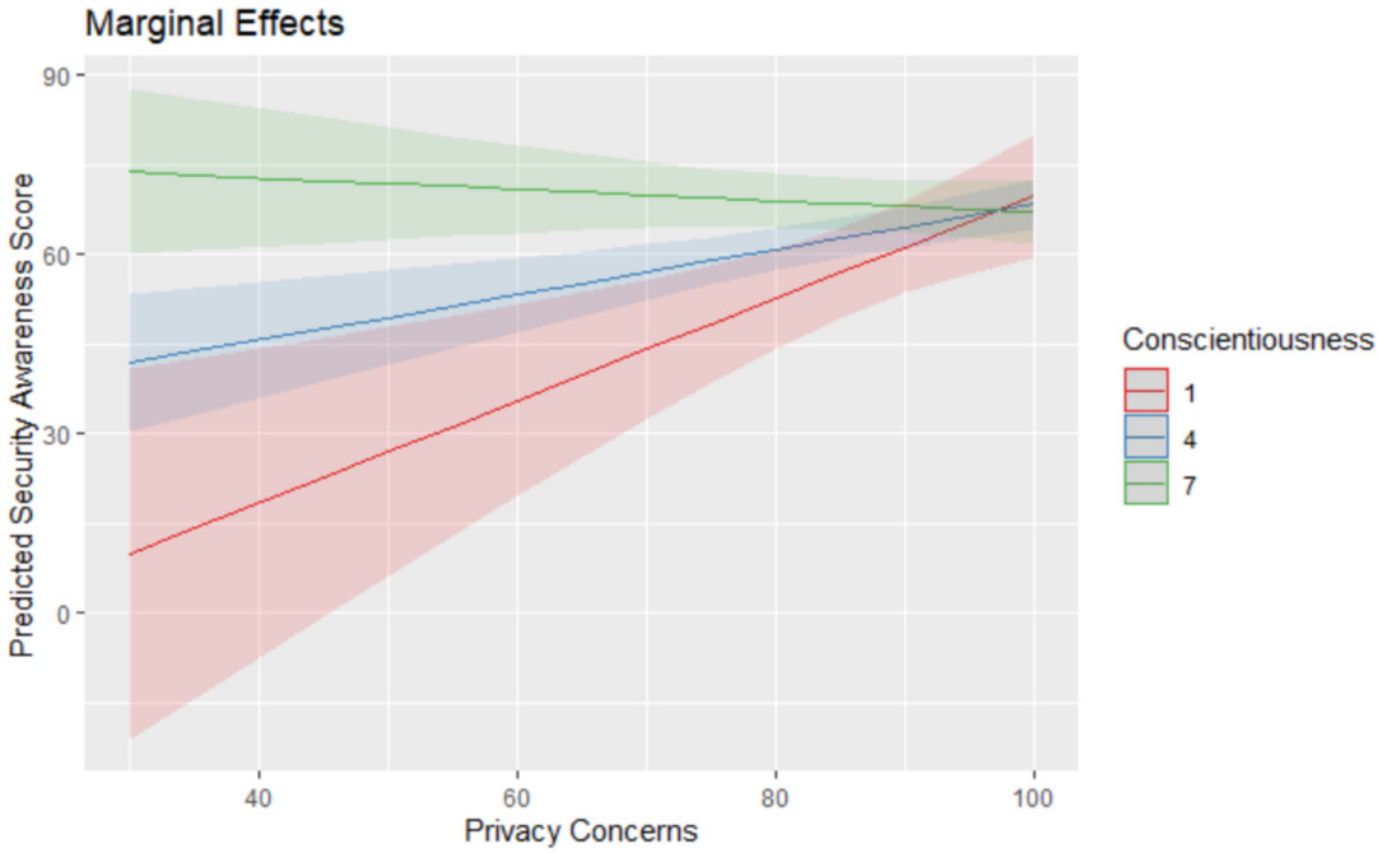

Figure 7

The final model of SSO account security awareness in this study