Journal of the Brazilian Computer Society, 2026, 32:1, doi: 10.5753/jbcs.2026.5384

Cybersecurity knowledge and behaviors: An exploratory study in Brazil with data mainly from northeast and southeast

Marcelo Henrique Oliveira Henklain [**Federal University of Roraima** | ***marcelo.henklain@ufrr.br***]
Felipe Leite Lobo [**Federal University of Roraima** | ***felipe.lobo@ufrr.br***]
Eduardo Luzeiro Feitosa [**Federal University of Amazonas** | ***efeitosa@icomp.ufam.edu.br***]

Computer Science Department, Federal University of Roraima, Av. Cap. Ene Garcês, 2413 - Aeroporto, Boa Vista - RR, 69310-000, Brazil.

Received: 31 December 2024 • **Accepted:** 25 July 2025 • **Published:** 28 April 2026

Abstract Research about the importance of the human factor in cybersecurity is scarce. Aiming to contribute, we characterized cybersecurity knowledge and behaviors of internet users, assessing their relationship with the Big Five personality traits (openness, conscientiousness, extraversion, agreeableness, and neuroticism); 329 Brazilians, mostly from the North and the Southeast, participated. We observed higher scores in agreeableness and openness, and lower neuroticism. The knowledge level ranged from "moderate to good" and the frequency of cybersecurity behaviors was moderate. We found some weak evidence of an association between personality traits and cybersecurity knowledge and behavior. Future studies are needed to include a more diverse sample and improved instruments.

Keywords: Cybersecurity, Human factors, Personality

1 Introduction

Considering the human factor in cybersecurity is essential, as technology is designed by people and for people [Guilherme *et al*., 2021; Hoepers, 2024]. Understanding how individuals interact with security systems and policies — and why they behave in certain ways in specific situations — is key to addressing cybersecurity challenges [Parsons *et al*., 2017; Aljohani *et al*., 2020; Alanazi *et al*., 2022]. Such insights can inform the development of more resilient systems and more effective security policies [Hartwig and Reuter, 2021].

Historically, the cybersecurity literature has often portrayed users as the weakest link in security, primarily because they fail to behave as developers expect [Švábenský *et al*., 2020; Guilherme *et al*., 2021]. Data indicate that people typically do not follow best practices for password creation and usage [Aljohani *et al*., 2020], are prone to phishing attacks [Syafitri *et al*., 2022], and rarely understand how their online behavior can be monitored through techniques such as cookies and fingerprinting [Lin *et al*., 2023]. Therefore, it is essential to examine the human factor in cybersecurity to discover how systems and policies can better assist users in generating strong passwords, avoiding phishing attempts, and safeguarding their privacy [Ruoslahti *et al*., 2021].

Despite its urgency, few studies characterize or seek to understand human factors in cybersecurity [Rahman *et al*., 2021], particularly in Brazil [Soares *et al*., 2020]. Specifically, the literature on the relationship between personality and cybersecurity behaviors is scarce [Soares *et al*., 2020]. This gap persists despite its potential to customize educational interventions and campaigns on security best practices, identify personality profiles more likely to exhibit insecure behaviors and recommend protection strategies based on user personality [Kennison and Chan-Tin, 2020]. For this reason, our objective was to characterize cybersecurity knowledge and behaviors, evaluating their relationship with personality. To achieve this, we conducted an exploratory survey study with Brazilian participants aged 18 and older. Our study is innovative due to the preliminary development of instruments for cybersecurity research and the proposed analyses involving the Big Five-Factor Model of personality [Mansur-Alves and Saldanha-Silva, 2019].

This article is organized as follows: (1) the theoretical framework defines key concepts, including cybersecurity, the human factor, and the personality model adopted in this study; (2) the related work section highlights gaps in the existing literature that motivate our research; (3) the methods section describes the data collection procedure; and (4) the results and discussion present and interpret our findings. Finally, we finish with the conclusion.

2 Theoretical framework

Here, we define the concepts of cybersecurity, human factor, and personality. We also provide an overview of the Big Five Theory, which we adopt in this study.

2.1 Cybersecurity and the Human factor

Cybersecurity is a subfield of Computer Science and also an interdisciplinary endeavor, including law, psychology, ethics, and other fields, that comprises: "technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems" [Bishop *et al*., 2017, p. 5]. Ultimately, it seeks to safeguard the user of the computer or system [Rahman *et al*., 2021; da Silva, 2023].

Beyond technical solutions in computing, this area must consider how users interact with computers and the extent to

which they follow recommended practices to ensure proper functionality. It must, therefore, promote cybersecurity behavior, which involves avoiding or mitigating virtual threats [Alanazi *et al*., 2022]. In this context, knowledge about personality can be valuable.

2.2 Human personality

Psychology is a discipline that offers various approaches to studying personality. Personality can be broadly understood as a set of behaviors exhibited with a certain regularity that distinguish individuals from one another, and whose roots come from the interaction between nature and nurture‘ [Banaco *et al*., 2012]. The Big Five Theory (BFT) is a psychological approach to study personality supported by 30 years of empirical research [Mansur-Alves and Saldanha-Silva, 2019] and favorable evidence from studies conducted in over 50 countries [Schmitt *et al*., 2007]. For this reason, we adopted this theory as the framework to guide our study.

The BFT proposes that humans possess five basic personality traits rooted in the species' evolutionary history, which can be further detailed through facets (more specific characteristics). These traits encompass predispositions and sensitivities to stimuli (aspects of the environment that are somehow related to what an organism is doing) that may facilitate or hinder learning throughout life, thereby shaping personality.

The five traits are: (1) Neuroticism: the degree of emotional instability, susceptibility to aversive events, and the tendency to experience negative emotions such as anxiety, irritability, and emotional instability, especially in response to stress or failure; (2) Extraversion: the tendency to explore the environment, interact with others, and to be outgoing, energetic, and sociable, especially in group or team settings; (3) Agreeableness: the tendency to be cooperative, empathetic, considerate in social and team interactions, and the need of pursuing deep interpersonal relationships; (4) Conscientiousness: the tendency to be organized, responsible, and goal-oriented in pursuing tasks and meeting deadlines, i.e., behavioral control to accomplish tasks; and (5) Openness to New Experiences: the tendency to seek out novelty, embrace new ideas, and appreciate creative or unconventional solutions and innovation. According to the BFT, the interaction between "basic traits and learning" and "current bodily and environmental conditions" helps explain behaviors and, therefore, personality. Measuring these basic traits is useful for understanding the likelihood of certain behaviors.

Theoretically, we expect that more conscientious people and those who care more about following social rules (possibly those with higher agreeableness levels), will be more likely to engage in cybersecurity behaviors [McCormac *et al*., 2017]. However, for this to happen, individuals need to be aware of best cybersecurity practices. On the other hand, aspects of neuroticism can both help and hinder the display of safe behaviors. People who are concerned about the possibility of cyberattacks and confident that can act to prevent it, might adopt more precautionary measures [McCormac *et al*., 2017]. On the other hand, individuals with higher levels of hopelessness, which can also be associated with neuroticism, may believe that prevention efforts are futile because they will inevitably become victims of attacks [Kennison and Chan-Tin, 2020]. More extroverted people may be more inclined to expose themselves on the Internet, which can jeopardize their privacy [Kennison and Chan-Tin, 2020], and individuals who are open to new experiences may accept more risks than others who are more conservative [McCormac *et al*., 2017].

These examples illustrate the types of relationships we can investigate and help us consider potential interventions to mitigate the negative effects of a specific personality trait on the adoption of cybersecurity behaviors. For instance, if an extroverted person values broad social recognition, we might reward them publicly within an organization as someone who properly cares about security. This might have a reinforcing value for that person compared to someone more introverted. To measure these five personality traits, there are multiple instruments with evidence of favorable psychometric properties [Mansur-Alves and Saldanha-Silva, 2019]. Considering the variables of length and the existence of a cross-cultural adaptation available for Brazil, we will adopt the Big Five Personality Inventory, used by McCormac *et al*. [2017], and adapted to Brazilian culture by Andrade [2008].

3 Related work

In this section, we present studies that characterize or seek to understand cybersecurity knowledge and behaviors. These studies highlight gaps that justify the research problem we selected.

Cain *et al*. [2018] investigated the cybersecurity knowledge and behavior of 268 participants (92% from the U.S.). They observed that users update their antivirus software but do not perform regular scans. Most users share sensitive personal data on digital social networks and fail to check privacy settings. Older users are more cautious than younger ones, and men have more cybersecurity knowledge than women, although there is no gender difference in terms of secure behavior. The authors concluded that, typically, users do not adopt cybersecurity behaviors.

In one of the few Brazilian studies on this topic, Guilherme *et al*. [2021] assessed 207 internet users, typically young and without cybersecurity training, who spent more than 12 hours daily online. It was found that the Covid-19 pandemic increased internet usage, and more than 70% of users had downloaded suspicious programs, over 55% shared their phones or computers, more than 41% shared personal accounts, over 29% shared credit card information in messaging apps, more than 40% always used the same password, over 20% had clicked on links in suspicious emails, and more than 19% had accessed bank accounts over public Wi-Fi. These percentages raise concern and confirm previous findings in Brazil by Soares *et al*. [2020], that identified a paradox between users claims of how relevant privacy or security are and their actual behavior. However, data indicated that cybersecurity training helps promote secure behaviors.

The study by Kennison and Chan-Tin [2020] illustrates a line of research that seeks to explain cybersecurity behavior. They assessed whether personality, the tendency to engage in risky behaviors, sensation-seeking, and knowledge of passwords contribute to cybersecurity behaviors. A total of 292 participants, mostly young women from psychology and com-

munication courses, took part in the study. The following observations were made: (1) greater knowledge of passwords is associated with fewer insecure behaviors; (2) women, but not men, who seek sensations (e.g., appreciation for adventure and novelty) engage in more risky behaviors; (3) for women (but not for men), conscientiousness predicts risky behavior in an inversely proportional relationship; and (4) greater emotional instability predicts a higher degree of risky behavior. McCormac *et al*. [2017] also investigated individual differences, like personality, in information security awareness (ISA). They found that conscientiousness, agreeableness, emotional stability and risk-taking were important factors determining individuals' ISA.

Alanazi *et al*. [2022] assessed whether awareness of virtual threats, the intention to act securely, and perceived behavioral control promote cybersecurity behaviors. A total of 1,581 students from various programs participated, with over 98% being Saudi, aged between 18 and 30 years. It was observed that secure behavior is more closely related to knowing how to implement it than to understanding virtual threats. Therefore, practical training would be preferable to programs focused solely on conveying information. The study also found that social norms and awareness of risks increase the likelihood of adopting cybersecurity behaviors.

Finally, Rahman *et al*. [2021] investigated the scientific production in cybersecurity related to human factors, using data from events in this field. Between 2015 and 2020, 27 studies were identified, revealing three main research areas: user characteristics and behaviors, cybersecurity systems, and the measurement of system usability. Regarding users, most studies focused on computing students from the U.S. and Europe. Qualitative studies were the most prominent in terms of methodology. They also found that research on the development of tools for the cybersecurity field is scarce.

Based on the studies reviewed, we observed that response biases are not always controlled, that instruments used to assess knowledge often require participants to self-assess without actually testing their knowledge through tasks with correct answers, and that Brazilians have been underrepresented in research. We also identified few studies evaluating the relationship between personality, knowledge, and behaviors related to cybersecurity. Therefore, the objective of this study was to characterize knowledge and cybersecurity behaviors, evaluating their relationship with personality. Our research questions regarding the sample of Brazilians investigated were: **PP01.** What are the personality characteristics of the sample? **PP02.** What are the characteristics of cybersecurity knowledge? **PP03.** What are the characteristics of cybersecurity behavior? **PP04.** To what extent do personality traits relate to knowledge and cybersecurity behaviors?

4 Methods

In this section we provide information about how our data was collected. We start characterizing the participants and move to a description of the instruments adopted. Finally, we explicit the procedure to collect data and analyze it.

4.1 Participants

A total of 333 individuals participated, but four were excluded due to attention problems and response bias. The demographic data of the remaining 329 participants, with an average age of 26.79 years (SD = 10.03), ranging from 18 to 66, are shown in Table 1. This sample is balanced in terms of gender masculine and feminine (but not considering non-binary and other genders), the identities of White and Brown, income ranging from "up to 2" to "more than 5 to 6 minimum wages", and degrees in Computing and Psychology. Most participants were aged 18 to 23 (55.32%), single (80.55%), childless (84.19%), with ongoing higher education (64.13%), residents of Roraima (54.41%), from the field of Informatics (25.87%, 64 men, 17 women, and 1 person as other), and has no disabilities (90.27%).

4.2 Instruments

The instruments applied in this study are described below. They can be accessed upon request to the first author.

Participant Characterization Questionnaire (QCP). It assessed: (1) age; (2) gender (masculine, feminine or other); (3) ethnic-racial identity; (4) presence of disability; (5) family income; (6) marital status; (7) existence of children or dependents; (8) education level; (9) technical education area for those who interrupted, are enrolled in, or completed it; (10) higher education course for those who interrupted, are studying, or have completed it; (11) state of residence, with an option to indicate if residing outside Brazil; (12) whether they have completed a cybersecurity course.

Big Five Personality Inventory (IGFP-5, adapted by Andrade, 2008). It consists of 32 items that assess the big five personality factors through self-report, with 9 items on Openness, 6 on Conscientiousness, 8 on Extraversion, 3 on Agreeableness, and 6 on Neuroticism. Responses are provided on a Likert scale of agreement, ranging from "1 = Strongly Disagree" to "5 = Strongly Agree". In psychometric studies, data were collected across Brazil, and the evidence was favorable. In this study, the Guttman Lambda (G6) was the following: Openness Subscale = 0.79; Conscientiousness Subscale = 0.75; Extraversion = 0.86; Agreeableness Subscale = 0.64; Neuroticism Subscale = 0.80. All the subscales indicated adequate reliability.

Marlowe-Crowne Social Desirability Scale – Shortened Version with 20 items (EDSMC20, adapted by Gouveia *et al.* [2009]. This scale measures a person's tendency to behave according to what they perceive as socially desirable. It is a self-report instrument, with responses given on a dichotomous scale of true or false. Our study demonstrated adequate psychometric evidence, with the Guttman Lambda (G6) of 0.69, indicating adequate reliability.

Cybersecurity Knowledge Inventory – Non-specialists Version (I2C). Developed for this study, it consists of 36 items, of which 14 were designed to assess knowledge about passwords, 12 about phishing, and 10 about privacy. This measure seeks to evaluate knowledge objectively, although the confidence in one's answers reflects the participant's perception of their knowledge. The I2C is answered on a four-level Likert scale: "1 = Totally sure the statement is false",

Variable	Frequency	%	Variable	Frequency	%
Gender			**Marital status**		
Masculine	163	49,54	Single	265	80,55
Feminine	161	48,94	Married	53	16,11
Other	5	1,52	Divorced	10	3,04
Age group (years)			Widowed	1	0,30
18 – 23	182	55,32	**Child**		
24 - 29	62	18,84	Yes	52	15,81
30 - 35	36	10,94	No	277	84,19
36 - 41	16	4,86	**Region of residence***		
42 - 47	15	4,56	North	189	57,45
48 - 53	6	1,82	Northeast	12	3,65
54 - 59	3	0,91	Central-West	6	1,82
60 - 65	8	2,43	Southeast	108	32,83
66 - 71	1	0,30	South	12	3,65
Ethno-racial identity			**State of residence**		
White	173	52,58	Roraima	179	54,41
Brown	123	37,39	Sao Paulo	103	31,31
Black	23	6,99	Others	47	14,29
Yellow	7	2,13	**Educational level**		
Indigenous	3	0,91	CHS e CTE	12	3,65
Household income (minimum wage)			IHE	4	1,22
≤ 02	56	17,02	OHE	211	64,13
> 02 a ≤ 03	50	15,20	CHE	39	11,85
> 03 a ≤ 05	70	21,28	IPS	2	0,61
> 05 a ≤ 06	45	13,68	OPS	13	3,95
> 06 a ≤ 08	24	7,29	CPS	48	14,59
> 08 a ≤ 10	29	8,81	**Undergrad major (*n* = 317)**		
> 10 a ≤ 15	30	9,12	Computer Science	66	20,82
> 15 a ≤ 20	14	4,26	Psychology	59	18,61
> 20 a ≤ 30	6	1,82	Medicine	32	10,10
> 30	5	1,52	Others	160	50,47
Deficiency			**Higher Educational Area (*n* = 317)**		
Yes	32	9,73	Informatics	82	25,87
No	297	90,27	Others	235	74,13

Note. CHS: Completed High School; CTE: Completed Technical Education; IHE: Interrupted Higher Education; OHE: Ongoing Higher Education; CHE: Completed Higher Education; IPS: Interrupted Postgraduate Studies; OPS: Ongoing Postgraduate Studies; CPS: Completed Postgraduate Studies; * = 2 Brazilian participants (0,61%) living abroad.

Table 1. Sociodemographic characterization of the sample (n = 329).

"2 = Partially sure the statement is false", "3 = Partially sure the statement is true", and "4 = Totally sure the statement is true". In scoring, levels 1 and 2 are coded as "false" and levels 3 and 4 as "true". The count of responses 1 and 4 is used as a measure of the security level.

The instrument was designed so that half of the items have the correct answer as true, and the other half is false. This rule applies to each of its three dimensions (passwords, phishing, and privacy). The G6 was 0.72, which is acceptable. Before the I2C, we included three open-ended items to assess to what extent participants create strong passwords, thinking of protecting a social network, an email account, and a bank account. This instrument does not yet have studies evaluating its psychometric properties.

Self-Assessment Scale on Cybersecurity Behaviors (EACC). Developed for this research, with 13 items, including 3 on passwords (2 positive items indicating secure behaviors, and 1 negative item indicating insecure behavior), 2 on phishing (1 positive and 1 negative), 5 on privacy (3 positive and 2 negative), and 3 on malware (1 positive and 2 negative). This instrument is answered using a four-level Likert scale: "1 = Never" to "4 = Always". The G6 was 0.66, which is acceptable. In association with this instrument, but without contributing to its score, we asked whether the participant knew what the following terms are and whether they use software to block them: (1) fingerprinting and whether they use software to block it; (2) cookies and whether they use software to block them; (3) malware and whether they use antivirus software; (4) privacy protection software; (5) phishing and whether they use software for protection against this type of attack. This instrument does not yet have studies evaluating its psychometric properties.

4.3 Data Collection and Analysis Procedure

This research was approved by the Ethics Committee. In the Google Forms we created, participants were required to express their agreement with the Informed Consent Term before beginning their participation. The participants then

completed the instruments in the following order: QCP, IGFP-5, I2C, EACC, and EDSMC20. The link to the form was shared for two and a half months on the Internet and sent to contacts of the authors of this study.

We included five items throughout the form to examine whether participants were responding attentively, requiring a specific response option selection. Any error would result in the exclusion of the participant. We also checked if the same answers were provided for all items of the IGFP-5, the EDSMC20, the I2C, and the EACC. If this occurred, it would also lead to exclusion. Furthermore, we examined whether the participant provided an impossible or inconsistent response with the study's participation requirements. Upon reviewing the data, we found that one participant provided the same answers for all 20 items of the EDSMC and another one for all the IGFP-5 items, both showing extreme responding. We also found one participant that made an attention mistake, and another that reported being 11 years old. As a result, their data were excluded.

We calculated descriptive statistics for personality characterization, knowledge, knowledge security, and cybersecurity behaviors. We conducted parametric inferential statistical analyses, including t-tests and ANOVA (α = 5%), as the variables we examined typically tended towards normality when their Q-Q plots and values of skewness and kurtosis (between -1 and 1) were analyzed. Although the Shapiro-Wilk tests we ran showed the opposite, when we conducted all tests with non-parametric statistics, our results did not change. We also verified that, typically, the groups we compared showed equal variances.

For the purposes of statistical analysis, we classified four of the five "Other" responses as female and one as male, considering the names provided by our participants. We chose this approach because performing a statistical analysis (for instance, inferential analysis) with a group of only five participants would be inappropriate, especially given the need to compare it with the much larger male and female groups. Our hypothesis was that the names likely indicate the gender assigned to these participants in their civil records, which was the only reasonable criterion we identified to enable the analysis of these data, since our evaluation was that we should take into account these participants' responses.

Nonetheless, we acknowledge that our approach may not accurately reflect the self-identified gender of these participants, which constitutes a limitation of our study. As a result, our findings cannot be generalized to non-binary individuals or those who identify with other genders, and interpretations should take this limitation into careful consideration. Importantly, our analytical decision was made with the intention of including the experiences of these participants. By analyzing their responses, we aimed to ensure that their perspectives were represented in the study since our initial intention was to gather a bigger sample of other genders to analyze them. Unfortunately, this was not possible.

We encourage future research to expand participation of individuals who identify with diverse genders, thereby generating knowledge that can inform cybersecurity interventions and policies that truly address the needs and realities of this population. In this sense, it is important that future research includes other types of gender in the response options, moving forward from the approach of including only the option "others".

5 Results and Discussion

In this section we exhibit our findings and discuss it to explicit the answers to the research questions.

5.1 PP01 – What are the personality traits of the sample?

Figure 1 exhibits our findings about personality traits (Figure 1A) and the data concerning social desirability (Figure 1B). The asterisks represent the average.

According to Figure 1A, the traits of agreeableness (*Mean* = 4.34; *SD* = 0.61) and openness (*Mean* = 3.76, *SD* = 0.64) stood out showing higher scores, while neuroticism (*Mean* = 2.82, *SD* = 0.88) showed more scores at the lowest levels of the scale. These data suggest that, for our participants, deep relationships (agreeableness) and engagement with new experiences (openness) are important, and they manage negative life events in a balanced manner (low neuroticism). Except for openness and extraversion, we found statistically significant differences in scores between men and women, with women consistently showing higher means in conscientiousness ($t_{(327)}$ = -2.311, p = 0.021, d = -0.255), agreeableness ($t_{(327)}$ = -3.681, $p < 0.001$, d = -0.406), and neuroticism ($t_{(327)}$ = -3.548, $p < 0.001$, d = -0.391). This difference aligns with findings by Kennison and Chan-Tin [2020]. We will consider this result in our analysis of the relationship between ICGFP-5, I2C, and EACC.

In Figure 1B, we observed that 50% of the data fell between scores of 7.5 and 13, suggesting that the present sample exhibited a moderate level of social desirability, with a mean score of 10.61 and a median of 10.00. While we found a difference between men (*Mean* = 10.88, *SD* = 3.23) and women (*Mean* = 10.34, *SD* = 3.41), it was not statistically significant ($t_{(327)}$ = 1.472, p = 0.142). Later, we will assess the correlation degree between social desirability scores and other measures in this study to examine whether any findings fail to represent the participants' true opinions.

Regarding personality, no statistically significant association was found between the EDSMC20 score and openness (r = -0.063, p = 0.257) or extraversion (r = -0.043, p = 0.440). However, we identified associations with agreeableness (r = 0.176, $p < 0.001$), conscientiousness (r = 0.281, $p < 0.001$), and neuroticism (r = -0.465, $p < 0.001$). The positive associations were weak but suggest that individuals with higher agreeableness and conscientiousness also tend to act more in alignment with social desirability. The strongest correlation indicated that the more emotionally unstable behaviors a person exhibits, the less they realize that they act according to social desirability. This finding is consistent with expectations, as people with higher neuroticism generally perceive themselves as less socially desirable. Collectively, these results suggest that the responses to the IGFP-5 were consistent with participants' genuine self-perceptions.

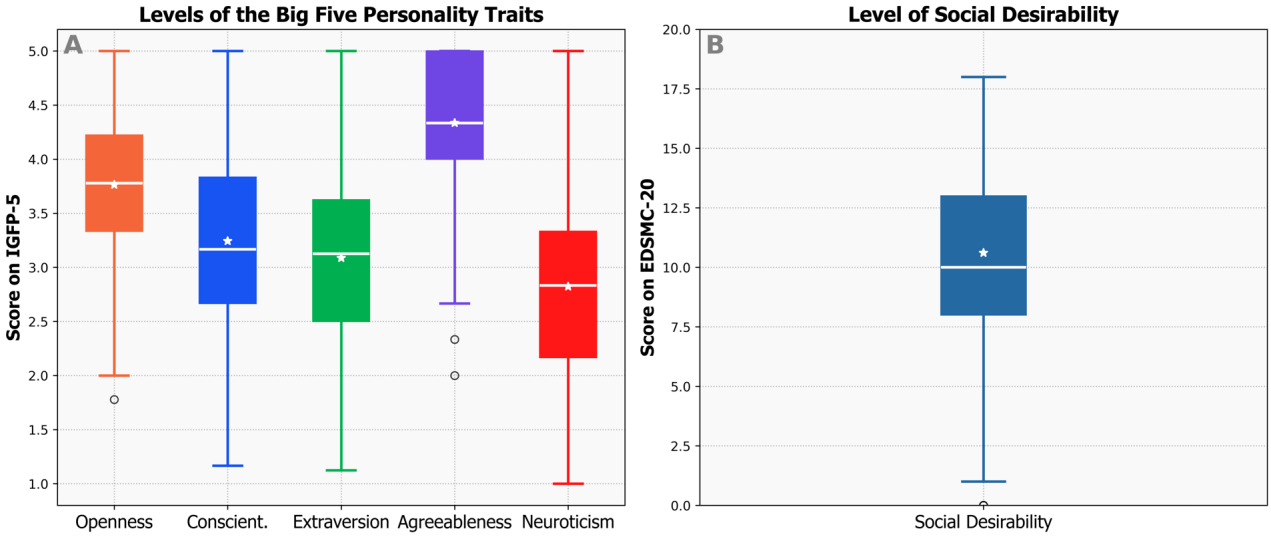

Figure 1. Results on IGFP-5 (Figure 1A) and on EDSMC-20 (Figure 1B).

5.2 PP02 – What are the characteristics of cybersecurity knowledge?

Figure 2 exhibits findings concerning what our participants know about cybersecurity. In Figure 2A we see that this sample showed a general knowledge ranging from "moderate to good" since the hit average was 65.93% (*SD* = 9.43). The 82 participants from informatics showed a hit average of 69.82% (*SD* = 8.93), while the other 235 participants achieved 64.60% (*SD* = 9.29). This difference was statistically significant, with a moderate effect size ($t_{(315)}$ = -4.425, $p < 0.001$, d = -0.568).

The fact that the d was not higher suggests that the items of I2C could be correctly answered by anyone, not just those in the field of informatics. This is positive, as we aimed to characterize the behavior of users in general. We also found a statistically significant difference, this time with a small effect size ($t_{(327)}$ = -2.920, p = 0.004, d = -0.398), between the knowledge of those who reported taking a cybersecurity course (n = 68, *Mean* = 68.87, *SD* = 9.63) and those who had not taken any (n = 261, *Mean* = 65.17, *SD* = 9.24). Our data suggest that investment in training on general IT and, specifically, cybersecurity, enhances cybersecurity knowledge, although it remains uncertain whether this translates into everyday practices [Kennison and Chan-Tin, 2020; Rahman *et al.*, 2021].

Regarding security in their own responses, as shown in Figure 2B, the data variability was higher. The range of responses was 97.22 compared to 61.11 in the knowledge data. This result suggests that many participants felt insecure about their responses on the I2C. The average security score was 50.67% (*SD* = 20.79). Participants from the IT field (n = 82, *Mean* = 57.18, *SD* = 19.49) or those who took cybersecurity courses (n = 68, *Mean* = 61.64, *SD* = 18.76) reported higher security than those from other fields (n = 235, *Mean* = 48.06, *SD* = 21.01) or those who had not taken any cybersecurity course (n = 261, *Mean* = 47.81, *SD* = 20.37). These differences were statistically significant, with a small to moderate effect size (IT participants versus others: $t_{(315)}$ = -3.447, $p < 0.001$, d = 0.442; with versus without cybersecurity course: $t_{(327)}$ = -5.069, $p < 0.001$, d = 0.690).

This advantage for those from the IT field or who had taken cybersecurity courses, in terms of correct answers and security, suggests that the instrument accurately reflected the expected difference between groups. Finally, there was no statistically significant difference in knowledge based on gender ($t_{(327)}$ = -0.215, p = 0.830), although we observed a slightly higher score among women (n = 165, *Mean* = 66.04, *SD* = 9.38) compared to men (n = 164, *Mean* = 65.82, *SD* = 9.51). Despite this, women felt less secure (n = 165, *Mean* = 47.00, *SD* = 20.51) than men (n = 164, *Mean* = 54.35, *SD* = 20.47, $t_{(327)}$ = 3.253, p = 0.001, d = 0.359), corroborating findings about the challenges women face in entering the computing field [Teles *et al.*, 2023].

In Figure 2C, we show our participants knowledge claims about online common threats to security or privacy. We observed that most of them claimed to know what cookies (80.85%) and malware (70.82%) are. On the other hand, few people, despite it being a common attack, know what phishing is (56.03%). Even fewer are familiar with fingerprinting (26.44%).

In Figure 2D, when we calculate the average scores on the I2C for those who answered "yes" and "no" to each of these four concepts and subtracted one average from the other, we found that participants who are familiar with these concepts score higher on the I2C. When we perform this procedure, calculating the averages only for the I2C items related to 'passwords', 'phishing', 'privacy', 'cookies', and 'fingerprinting', the pattern remains consistent. Even when we calculate t-tests comparing the means of the 'yes' and 'no' groups, the results were mostly statistically significant, with moderate effect sizes (e.g., know what phishing is: $t_{(327)}$ = -5.684, $p < 0.001$, d = -0.629). This data suggests that a participant's self-reported knowledge of concepts seems to be informative of their actual knowledge, with special value placed on the information regarding the knowledge of the concept of 'phishing'.

In the context of cybersecurity knowledge, we assessed the extent to which participants created strong passwords to protect social media, email, and bank accounts. Table 2 presents the overall entropy results of the passwords created, as well

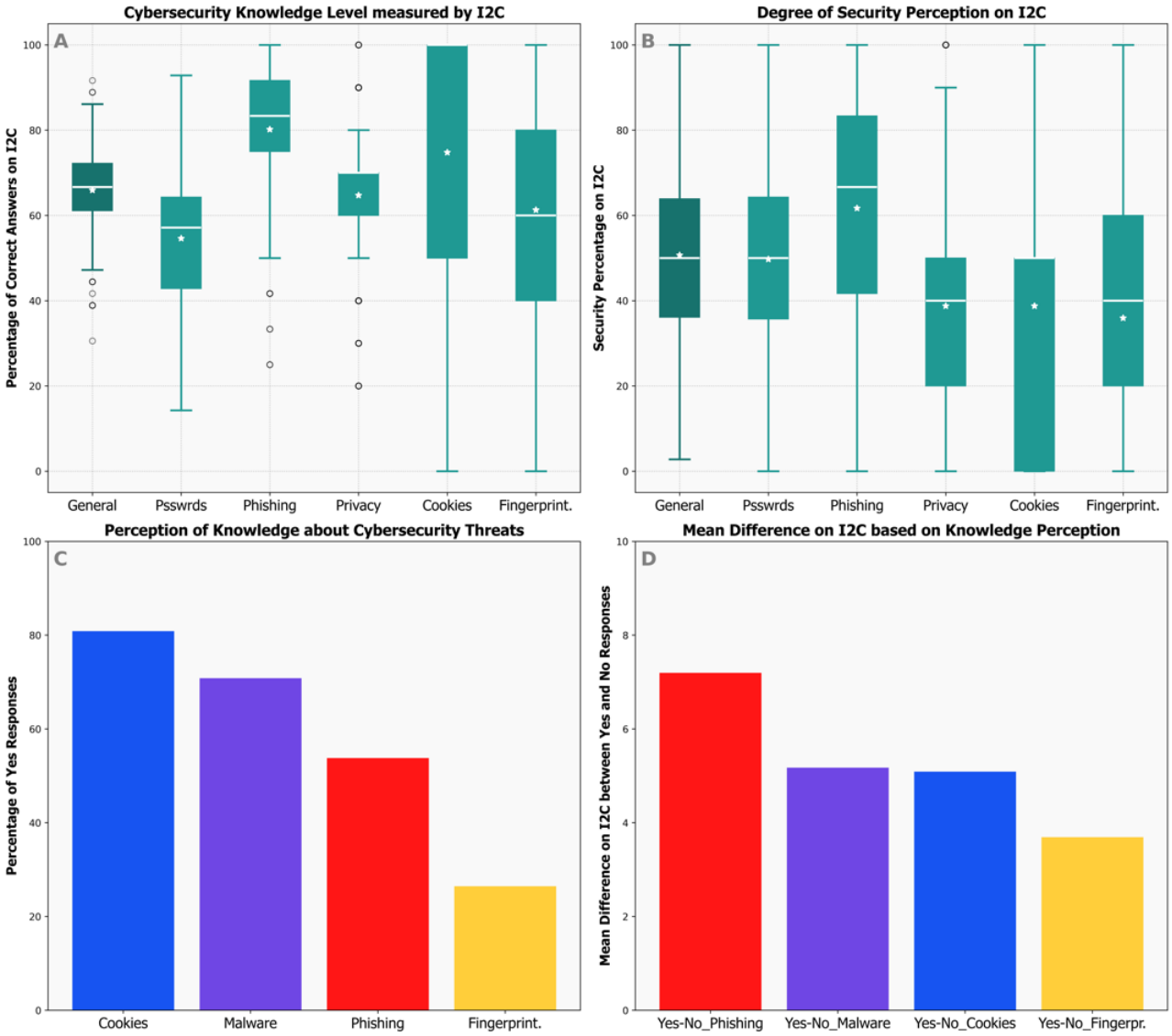

Figure 2. Results of correct answers on I2C (Figure 2A), Results of security about answers on I2C (Figure 2B), Responses 'yes' to questions concerning knowledge about threats to cybersecurity (Figure 2C) and Mean differences on I2C based on knowledge about threats to cybersecurity (Figure 2D).

as a description of the types of characters used. We observed that entropy was similar for social media and email passwords and, surprisingly, lower for bank passwords. Our hypothesis for this finding is that, despite the instruction that there were no restrictions on length or character types, participants assumed that bank passwords could only consist of numbers as is typical in real life Brazilian bank accounts. The absence of character data supports this idea, as bank passwords showed a higher absence of uppercase letters, lowercase letters, and special characters.

In terms of entropy, a password is considered strong if it has at least 60 bits [Glory *et al*., 2019]. On average, the passwords created met this requirement. However, we identified passwords with very low entropy, like 13.29, as well as an average entropy for bank passwords below 60 bits. Up to the first quartile, none of the passwords met the 60-bit criterion, with entropy values ranging from 19.93 (bank) to 58.99 (social media).

Notably, even in a research setting where participants were asked to create only three passwords, 6.38% of them reused the same password for social media, email, and bank accounts. The repetition rates for 'social media and bank,' 'email and bank,' and 'social media and email' were 6.69%, 8.21%, and 16.72%, respectively. These findings confirm the historical tendency found in scientific literature that users tend to create weak passwords and reuse them across multiple accounts [Ji *et al*., 2017; Bošnjak *et al*., 2018].

Regarding password characteristics, we observed moderate length, with an average exceeding 10 characters, but limited use of uppercase letters and special characters. Including these elements would make passwords significantly stronger without requiring substantial additional effort. This is an example of the valuable insights studies like this can provide, which support the development of effective training programs, and cybersecurity policies.

Finally, we observed that the I2C scores (r = -0.022, p = 0.692), level of confidence (r = 0.066, p = 0.236), and self-reported knowledge of cookies (r = 0.033, p = 0.548), malware (r = 0.045, p = 0.416), phishing (r = 0.100, p = 0.070), and fingerprinting (r = 0.071, p = 0.200), as well as the entropy of the passwords created by participants (Password 1: r = -0.068, p = 0.218; Password 2: r = 0.025, p = 0.651; Password 3: r = -0.036, p = 0.518), showed no relevant association with the EDSMC20. This provides evidence that such data are not associated with social desirability bias. Except for confidence levels and self-reported knowledge, this outcome was expected, as the other variables mentioned do not involve participants' opinions or self-reports.

5.3 PP03 – What are the characteristics of cybersecurity behavior?

Figure 3 presents the findings on cybersecurity behaviors reported by users based on their self-perception (Figure 3A), covering (1) password creation and usage, (2) handling phishing and malware attacks, and (3) privacy protection, which includes defenses against tracking techniques (cookies, supercookies, and fingerprinting), basic knowledge of the Brazilian LGPD (General Data Protection Law), and safe Internet practices. Figure 3B displays the "yes" and "no" responses regarding the use of software for digital protection.

As shown in Figure 3A, more than 50% of participants scored above 2 on the EACC. For the overall score and phishing-related items, more than 50% scored above 2.5. However, the mean and median scores were generally equal to or less than 3, suggesting that cybersecurity behaviors occur infrequently. Regarding password use and phishing protection, the median score was 3, with over 25% of participants scoring between 3 and 3.5. This indicates that these behaviors are frequent but have not yet reached the standard of always occurring. Furthermore, Figure 3B reveals that antivirus software is the most used, but even in this case, only 56.23% of participants reported adopting it. These findings replicate those reported by Cain *et al*. [2018] and Guilherme *et al*. [2021].

To delve deeper in this data, we need to relate it to what we saw previously, in Figure 2C. Although, the majority of our sample claimed to know what cookies are, when questioned if they use software to block it, only 9.12% did. The three most cited softwares were AdBlock, Brave (the browser), and Kaspersky. In a more balanced relationship between knowledge and precautions, we identified that 70.82% know what malwares are, and more than 50% reported using software to avoid malware infection. The three most cited softwares were Kaspersky, Microsoft Defender, and Avast. On the other hand, few people, despite it being a common attack, know what phishing is (56.03%), and reported using any software to protect them against it (3.95%).

For instance, as we can see, most of our participants did not realize that antivirus and spam filters that they already use could be cited as software that helps protecting them against phishing. This data suggests that at least to our participants, it's really not clear what phishing is. Even fewer are familiar with fingerprinting (26.44%), and adopt any software to protect them (3.34%). Participants are more familiar with antivirus software, but as our data showed they seem not to fully understand its function. A small portion is familiar with and uses ad blockers or specific browsers, such as Brave, which aim to protect privacy. In future studies, it may be interesting to assess knowledge about specific software for security and privacy protection.

As with the examination of knowledge, we conducted t-tests to compare groups. The differences in mean scores for the adoption of cybersecurity behaviors were statistically significant ($t_{(315)}$ = -3.351, p < 0.001, d = -0.430) for participants in the field of computer science (*Mean* = 2.95, *SD* = 0.36) compared to those from other fields (*Mean* = 2.78, *SD* = 0.41). It is worth noting that, although the average score of participants in the computer science field was higher than that of others and close to 3 – a score indicative of frequent behavior – the mean score was not as high as expected for specialists in the field. This finding aligns with Cain *et al*. [2018], who also observed modest differences between experts and non-experts.

When we grouped only the items assessing specific behaviors, such as secure password practices, phishing protection, privacy protection, and malware protection, and calculated their score (as shown in Figure 3A), we found that participants in the computer science field outperformed those from

Password	Entropy				
	Mean	**SD**	**Median**	**Minimum**	**Maximum**
Social media	78.50	39.24	72.10	19.93	471.93
Email	76.67	36.77	72.10	19.93	471.93
Bank	57.13	43.98	52.44	13.29	471.93
Password	**Average character occurrence**				
	Capital	**Lowercase**	**Number**	**Special**	**Length**
Social media	1.48	5.50	4.12	1.51	12.62
Email	1.48	5.54	3.91	1.44	12.37
Banco	1.07	3.03	5.13	1.12	10.35
Password	**Count of missing characters in relation to the 329 participants**				
	Capital	**Lowercase**	**Number**	**Special**	**Total**
Social media	72	27	17	0	116
Email	72	27	20	91	210
Bank	172	155	15	165	507

Table 2. Entropy and characterization passwords created by participants (n = 329).

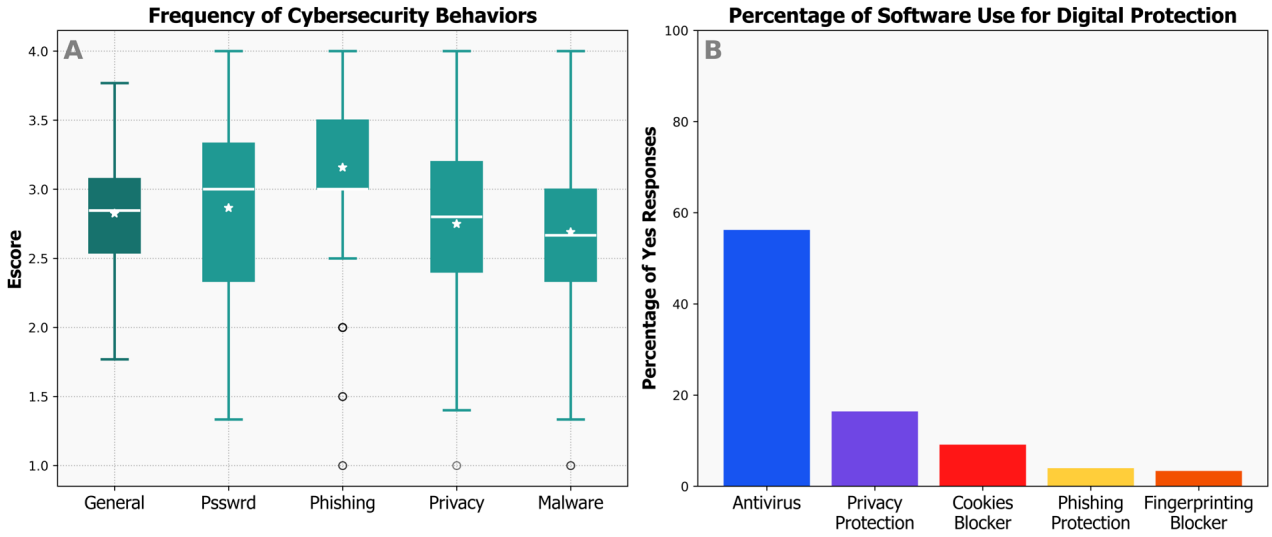

Figure 3. Results on EACC (Figure 3A) and 'Yes' responses about software use (Figure 3B).

other fields in all cases except phishing-related practices. For the other areas, excluding phishing, the t-tests were significant. A similar pattern emerged when comparing scores based on whether participants had completed a cybersecurity course. The key difference was that individuals who had taken a course in cybersecurity also outperformed others in phishing-related practices.

Regarding gender, we observed a small but statistically significant difference ($t_{(327)} = 5.444$, $p < 0.001$, $d = 0.600$) between men (*Mean* = 2.94, *SD* = 0.37) and women (*Mean* = 2.71, *SD* = 0.40). These differences were also evident when we analyzed specific practices related to passwords, phishing, privacy, and malware. Notably, for the last two (privacy and malware), the effect size of the gender difference was larger. Our hypothesis for these observed gender differences is that cultural conditions distancing women from technology [Teles *et al*., 2023; Lopes *et al*., 2023] likely reduce opportunities for women to learn how to protect themselves in cyberspace. This finding underscores the importance of specific cybersecurity training targeted toward this population.

We also evaluated whether these data were associated with the EDSMC20. A statistically significant but weak correlation was identified with the EACC ($r = 0.225$, $p < 0.001$), which was expected. Given the low degree of correlation, responses to the EACC do not appear to reflect social desirability. For questions about antivirus use ($r = 0.066$, $p = 0.230$), privacy protection ($r = -0.025$, $p = 0.646$), cookie blockers ($r = -0.014$, $p = 0.803$), phishing protection ($r = 0.011$, $p = 0.836$), and fingerprinting blockers ($r = -0.083$, $p = 0.132$), no relevant associations with the EDSMC20 were found.

5.4 PP04 – To what extent are personality traits associated with cybersecurity knowledge and behaviors?

We then examined the possible relationships between personality, cybersecurity knowledge, and cybersecurity behaviors. To this end, Table 3 presents a correlation matrix involving these variables, with specific correlations calculated for women (below the diagonal) and for men (above the diagonal). Additionally, correlations for the complete dataset (men and women combined) are included below the first matrix.

Regarding the correlations for the entire sample, we observed small yet expected associations among personality variables, suggesting that, in this sample, consistent with other studies, the IGFP-5 accurately measured the big five

Correlation coefficients for men (above the diagonal) and for women (below the diagonal)								
Variable	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1. Openness	—	0.08	0.38***	0.21**	0.03	-0.08	-0.03	-0.10
2. Conscientiousness	0.17*	—	0.08	0.19*	-0.19*	-0.001	-0.05	-0.10
3. Extraversion	0.20**	0.00	—	0.23**	-0.01	-0.08	-0.11	0.05
4. Agreeableness	0.15	0.22**	0.20*	—	-0.23**	0.03	-0.14	-0.05
5. Neuroticism	-0.08	-0.39***	-0.15	-0.12	—	-0.03	0.08	0.04
6. I2C Hits	0.03	-0.14	-0.19*	-0.15	-0.01	—	0.15	0.19*
7. I2C Security	0.09	-0.01	0.01	0.15	-0.09	0.15	—	0.27***
8. EACC	0.28***	0.11	-0.10	0.02	-0.13	0.19*	0.27***	—
Correlations coefficients for the whole sample								
Variable	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1. Openness	—							
2. Conscientiousness	0.13*	—						
3. Extraversion	0.29***	0.05	—					
4. Agreeableness	0.18***	0.22***	0.22***	—				
5. Neuroticism	-0.02	-0.27***	-0.07	-0.13*	—			
6. I2C Hits	0.04	-0.03	-0.14*	-0.03	-0.09	—		
7. I2C Security	0.1	0	0.05	0.07	-0.19***	0.21***	—	
8. EACC	0.19***	0.1	-0.05	0.06	-0.18**	0.22***	0.34***	—

Note. * p < .05, ** p < .01, *** p < .001. Below the diagonal = Women; Above = Men.

Table 3. Entropy and characterization passwords created by participants (n = 329).

traits. We also identified a statistically significant correlation between the level of knowledge and the level of security, which aligned with expectations. For cybersecurity knowledge and behaviors, a correlation was anticipated, albeit not of great magnitude, as it is well known that many users, despite recognizing the correct conduct, may not exhibit secure behaviors due to factors such as response costs. Cain *et al*. [2018], for instance, noted that even experiencing attacks or receiving security training does not guarantee the adoption of best practices.

We found it noteworthy that a moderate association emerged between the level of confidence in one's own knowledge and cybersecurity behavior (Overall: $r = 0.34$, $p < 0.001$; Women or Men: $r = 0.27$, $p < 0.001$). One possible explanation for this result is that, beyond exposure to security training, it is crucial to assess how effectively the training enables individuals to feel confident in their mastery of the subject and their practical ability to handle virtual threats. In this regard, Alanazi *et al*. [2022] noted that secure behavior is more closely related to the practical ability to implement it (e.g., knowing how to update software) than to an understanding of security concepts or a general awareness of being vulnerable to threats.

Regarding the association between personality and knowledge, we found only one statistically significant correlation, which was negative, between extraversion and knowledge ($r = -0{,}14$, $p = 0{,}011$). This suggests that more extroverted individuals tend to know less about cybersecurity, and vice versa. This result may be explained by the fact that, in this sample, those with greater knowledge of cybersecurity were from the computing field and exhibited lower levels of extraversion (Correlation between having a degree in computing and extraversion: $r = -0.21$, $p < 0.001$).

Regarding confidence in one's own knowledge, we found only a weak negative correlation with neuroticism ($r = -0.19$, $p < 0.001$), suggesting that individuals with higher emotional instability feel less confident about their knowledge. Based on the construct measured by neuroticism, it is expected that more emotionally unstable individuals feel generally less secure. We also observed that emotionally unstable individuals engage less in cybersecurity behaviors ($r = -0.18$, $p = 0.001$).

Since confidence in one's own knowledge increases the likelihood of engaging in these behaviors, it is understandable that individuals who trust their actions less are less likely to adopt secure practices. On the other hand, we observed a correlation between openness and cybersecurity behavior ($r = 0.19$, $p < 0.001$), suggesting that a willingness to engage with new stimuli may be directly linked to the adoption of secure practices. This may relate to the fact that cybersecurity behaviors require exploring information that evolves over time, such as how to protect oneself and how technologies work.

Regarding women's data, we observed in Table 3 that extraversion showed a negative correlation with cybersecurity knowledge ($r = -0.19$, $p < 0.05$). We also noted that women who were more open to new experiences exhibited more cybersecurity behaviors, contradicting previous literature findings ($r = 0.28$, $p < 0.001$). Kennison and Chan-Tin [2020] found a positive association between sensation seeking, which is related to openness, and risk-taking behavior. Additionally, for women, higher conscientiousness and lower neuroticism were associated with a lower degree of risk-taking behavior, which we did not verify in our data. Despite this, the associations we found, although not statistically significant, reflect the same direction of correlations, i.e., more conscientious individuals exhibit more cybersecurity behaviors ($r = 0.11$) and less neurotic individuals exhibit more cybersecurity behaviors ($r = -0.13$).

For men, we did not find statistically significant associations between personality and cybersecurity knowledge, security, or behavior. However, we observed a possible relationship between higher levels of extraversion and lower security (r = -0.11), higher levels of agreeableness and lower security (r = -0.14), higher levels of openness and lower cybersecurity behaviors (r = -0.10), and higher levels of conscientiousness and lower cybersecurity behaviors (r = -0.10). In all these cases, the findings may be related to specific characteristics of the sample, and we need to collect more data to find a robust pattern of association between personality measures and the constructs assessed in this study.

Strictly speaking, we expected to find that cybersecurity behaviors would be positively associated, at least, with conscientiousness. According to Alanazi *et al*. [2022], social norms and risk awareness increase the likelihood of cybersecurity behaviors. Social norms are linked to the duty facet of the conscientiousness factor. Risk awareness is directly related to conscientiousness in general. According to Egelman and Peer [2015], cybersecurity behaviors are related to long-term thinking, which requires risk awareness and disciplined conduct to mitigate risks.

Overall, despite the few and weak correlations, we found preliminary evidence of an association between Big Five traits and the variables examined in this study, with particular emphasis on openness, extraversion, and neuroticism. It would be important to continue investigating this phenomenon, as we need to make interventions to promote cybersecurity knowledge and behaviors more effective. Kennison and Chan-Tin [2020] suggest that cybersecurity training programs can reduce the frequency of insecure behaviors but should incorporate personality profiles for a more effective approach. To do so, we first need to better understand this relationship by conducting other studies like this one, with larger and more diverse samples, since we were not able to corroborate all the findings in the existing literature. Thus, we noticed that there is divergence regarding the findings. Certainly, the measures used have a direct impact on this divergence, and therefore, psychometric studies on such measures are recommended.

6 Conclusion

The aim of this study was to characterize cybersecurity knowledge and behaviors, assessing their relationship with personality. In the present sample, we observed higher scores in agreeableness and openness, accompanied by low levels of neuroticism. Knowledge scores about cybersecurity were "moderate to good", with a slight advantage for participants in the computer science field. Regarding cybersecurity behavior, we noted a moderate frequency and again a positive highlight for those in the computer science field.

When examining the relationships between these variables, we identified evidence of a weak association between personality traits and the dimensions of cybersecurity knowledge and behavior, mainly, for women. This may be useful in guiding future studies, which may contribute to customized training, as well as in building models to recommend behaviors based on the user's personality traits. Finally, we gathered evidence that women should be prioritized in educational campaigns to promote cybersecurity behavior. As literature points out, our culture does not stimulate girls to study technology or pursue careers in computer science. One possible consequence of this is that women feel less secure about its own knowledge concerning cybersecurity and may engage less in cybersecurity behavior, which is a risky attitude.

For future studies, we observed that one of the limitations of this research was the low heterogeneity of the sample. For instance, it was predominantly from only two Brazilian states, which does not adequately represent either the Northern or Southeastern regions, nor the Brazilian population. Thus, we cannot generalize our findings to the Brazilian population or even to these two regions; we can only formulate hypotheses that may be more thoroughly investigated by future studies. New investigations should consider a larger and more diverse sample. Furthermore, we consider it important, responding to the call of several researchers [Egelman and Peer, 2015; Parsons *et al*., 2017; Rahman *et al*., 2021], that specific psychometric instruments for the cybersecurity field begin to be developed. They can help in evaluating the effectiveness of educational interventions to promote cybersecurity behaviors, as well as in characterizing and investigating the variables that are associated or determine them.

Declarations

Authors' Contributions

MHOH, FLL, and ELF contributed to the conception, methodology, investigation, formal analysis, and writing of this study. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Funding

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES-PROEX) - Finance Code 001. This work was partially supported by Amazonas State Research Support Foundation - FAPEAM - through the POSGRAD project 2024/2025.

Availability of data and materials

The instruments generated and/or analyzed during the current study are available upon request to the first author.

AI Use Statement. The Copilot in Microsoft Word was used to assist in translating scientific text into English. All final editorial decisions and content validations were made solely by the authors, who retain full responsibility for the accuracy and integrity of the work.

References

Alanazi, M., Freeman, M., and Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of

young adults. *Computers in Human Behavior*, 136:1–14. DOI: 10.1016/j.chb.2022.107376.

Aljohani, M., Alruqi, M., Alboqomi, O., and Alqahtani, A. (2020). An experimental study to understand how users choose password. In *Proceedings of the 4th International Conference on Future Networks and Distributed Systems (ICFNDS '20)*, pages 1–5, New York. ACM. DOI: 10.1145/3440749.3442643.

Andrade, J. M. (2008). *Evidências de Validade do Inventário dos Cinco Grandes Fatores de Personalidade para o Brasil*. PhD thesis, Universidade de Brasília. Available at:`https://repositorio.unb.br/handle/10482/1751` Tese de doutorado apresentada ao Programa de Pós-graduação em Psicologia Social, do Trabalho e das Organizações.

Banaco, R. A., Vermes, J. S., Zamignani, D. R., Martone, R. C., and Kovac, R. (2012). Personalidade. In Hübner, M. M. C. and Moreira, M. B., editors, *Temas clássicos da psicologia sob a ótica da Análise do Comportamento*, pages 144–153. Guanabara Koogan. Book.

Bishop, M., Burley, D., Buck, S., Ekstrom, J. J., Futcher, L., Gibson, D., Hawthorne, E. K., Kaza, S., Levy, Y., Mattord, H., and Parrish, A. (2017). Cybersecurity curricular guidelines. In Bishop, M., Futcher, L., Miloslavskaya, N., and Theocharidou, M., editors, *Information Security Education for a Global Digital Society*, pages 3–13, Cham. Springer International Publishing. DOI: 10.1007/978-3-319-58553-6_1.

Bošnjak, L., Sreš, J., and Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1161–1166, Opatija, Croatia. DOI: 10.23919/MIPRO.2018.8400211.

Cain, A. A., Edwards, M. E., and Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42:36–45. DOI: 10.1016/j.jisa.2018.08.002.

da Silva, M. B. F. (2023). *Cibersegurança: Uma visão panorâmica sobre a segurança da informação na Internet*. Freitas Bastos Editora. Book.

Egelman, S. and Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*, pages 2873–2882, New York. ACM. DOI: 10.1145/2702123.2702249.

Glory, F. Z., Aftab, A. U., Tremblay-Savard, O., and Mohammed, N. (2019). Strong password generation based on user inputs. In *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 416–423. DOI: 10.1109/IEMCON.2019.8936178.

Gouveia, V. V., Guerra, V. M., Sousa, D. M. F., Santos, W. S., and Costa, J. M. (2009). Escala de desejabilidade social de marlowe-crowne: evidências de sua validade fatorial e consistência interna. *Avaliação Psicológica*, 8(1):87–98. Available at:`http://bit.ly/39mRvqK`.

Guilherme, L. P., Ferreira, M. F., Fonseca, G. M., and Lazarin, N. M. (2021). Uma breve noção sobre o comportamento dos internautas em relação à segurança na rede. In *Anais da VII Escola Regional de Sistemas de Informação do Rio de Janeiro*, pages 1–7. SBC. DOI: 10.5753/ersirj.2021.16972.

Hartwig, K. and Reuter, C. (2021). Nudge or restraint: How do people assess nudging in cybersecurity - a representative study in germany. In *Proceedings of the 2021 European Symposium on Usable Security (EuroUSEC '21)*, pages 141–150. ACM. DOI: 10.1145/3481357.3481514.

Hoepers, C. (2024). A importância dos fatores humanos para a cibersegurança. *Computação Brasil*, 52:61–66. DOI: 10.5753/compbr.2024.52.4604.

Ji, S., Yang, S., Hu, X., Han, W., Li, Z., and Beyah, R. (2017). Zero-sum password cracking game: A large-scale empirical study on the crackability, correlation, and security of passwords. *IEEE Transactions on Dependable and Secure Computing*, 14(5):550–564. DOI: 10.1109/TDSC.2015.2481884.

Kennison, S. M. and Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology*, 11. DOI: 10.3389/fpsyg.2020.546546.

Lin, X., Araujo, F., Taylor, T., Jang, J., and Polakis, J. (2023). Fashion faux pas: Implicit stylistic fingerprints for bypassing browsers' anti-fingerprinting defenses. In *IEEE Symposium on Security and Privacy (SP)*, pages 987–1004, San Francisco, CA, USA. DOI: 10.1109/SP46215.2023.10179437.

Lopes, R., Maciel, B., Soares, D., Figueiredo, L., and Carvalho, M. (2023). Análise e reflexões sobre a diferença de gênero na computação: podemos fazer mais? In *Anais do XVII WIT*, pages 68–79, Porto Alegre. SBC. DOI: 10.5753/wit.2023.230819.

Mansur-Alves, M. and Saldanha-Silva, R. (2019). Teoria dos cinco fatores de personalidade (tcf): Uma introdução teórico-conceitual e aplicada para avaliação. In Baptista, M. N. e. a., editor, *Compêndio de Avaliação Psicológica*, pages 507–520. Editora Vozes. Book.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69:151–156. DOI: 10.1016/j.chb.2016.11.065.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. (2017). The human aspects of information security questionnaire (hais-q): Two further validation studies. *Computers & Security*, 66:40–51. DOI: 10.1016/j.cose.2017.01.004.

Rahman, T., Rohan, R., Pal, D., and Kanthamanon, P. (2021). Human factors in cybersecurity: A scoping review. In *Proceedings of the 12th International Conference on Advances in Information Technology (IAIT '21)*, pages 1–11, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3468784.3468789.

Ruoslahti, H., Coburn, J., Trent, A., and Tikanmäki, I. (2021). Cyber skills gaps – a systematic review of the academic literature. *Connections: The Quarterly Journal*, 20(2):33–45. DOI: 10.11610/Connections.20.2.04.

Schmitt, D. P., Allik, J., McCrae, R. R., and Benet-Martínez, V. (2007). The geographic distribution of big five person-

ality traits: Patterns and profiles of human self-description across 56 nations. *Journal of Cross-Cultural Psychology*, 38(2):173–212. DOI: 10.1177/0022022106297299.

Soares, H., Araújo, N., and de Souza, P. (2020). Privacidade e segurança digital: Um estudo sobre a percepção e o comportamento dos usuários sob a perspectiva do paradoxo da privacidade. In *Anais do I Workshop sobre as Implicações da Computação na Sociedade*, pages 97–106, Porto Alegre. SBC. DOI: 10.5753/wics.2020.11040.

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., and Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE Access*, 10:39325–39343. DOI: 10.1109/access.2022.3162594.

Teles, M., Saraiva, L., Freires, M., Rocha, M., and Marques, A. (2023). Mentoria acadêmica como aliada à integração de alunas de computação no ambiente acadêmico. In *Anais do XVII WIT*, pages 194–204, Porto Alegre. SBC. DOI: 10.5753/wit.2023.230784.

Švábenský, V., Vykopal, J., and Čeleda, P. (2020). What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences. In *The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*. DOI: 10.1145/3328778.3366816.