International Journal of Information Security (2025) 24:44
https://doi.org/10.1007/s10207-024-00954-5

SPECIAL ISSUE PAPER

# How do gender and age similarities with a potential social engineer influence one's trust and willingness to take security risks?

Israa Abuelezz[1] · Mahmoud Barhamgi[1] · Sameha Alshakhsi[2] · Ala Yankouskaya[3] · Armstrong Nhlabatsi[1] · Khaled M. Khan[1] · Raian Ali[2]

Accepted: 1 December 2024

## Abstract

This study investigates how age and gender similarity between individuals and potential social engineers affect the individuals' trust and risk-taking behaviors. We crafted and face validated 16 personas, varying in demographics and visual cues, and inquired whether participants would agree to use each persona's offer to connect to the internet via their personal mobile hotspot, as well as the degree of trust they placed in the persona's intentions. Individuals were informed about the potential risks associated with using another person's mobile hotspot and that the person offering can be, but not necessarily, malicious. Data from 635 participants (322 Arabs and 313 British) were collected through an online survey. Participants were categorized by gender into male and female groups, and by age into two groups: early adulthood (18–35 years) and middle adulthood (36–59 years). Our results showed a correlation between trust and offer acceptance across all participant groups except for British females in middle adulthood. Additionally, participants, regardless of their gender and age groups, exhibited greater trust and acceptance towards personas who were female or older. Arab sample did not indicate a significant gender preference in aged personas; however, the British early adulthood group displayed a significant inclination towards accepting the offer from aged female personas over aged male personas. While demographic similarity between the potential manipulator personas and participants did not significantly impact the participants trust and risk-taking, our study uncovered differences in trust and offer acceptance when both age and gender demographics were considered together, suggesting nuanced effects of demographic matching and mismatching on taking security risks. These findings underscore the importance of incorporating bias awareness and debiasing techniques to reduce high reliance on demographic or cultural stereotypes.

**Keywords** Social engineering · Bias · Gender · Age · Cybersecurity · Risk-taking · Risk perception · Arab · UK

## 1 Introduction

With the recent technological advances in computer systems and software, the potential for technical vulnerability has increased for both individuals and businesses, leading to an increase in cybersecurity attacks [1, 2]. The "human" factor emerges as the most susceptible component within the interconnected chain of cybersecurity [3]. Cybersecurity encompasses a spectrum of threats, with social engineering (SE) being recognized as one of the human-centric methods for exploiting security vulnerabilities. Building target trust plays a central role in the success of a SE attack, as the primary objective of a social engineer, regardless of their chosen approach, is to persuade the individual to trust them with sensitive data.

Prior research has shown that individuals exhibit differences in risk perception and susceptibility to cybersecurity attacks across different gender and age groups. A simulated phishing study revealed that females showed greater susceptibility to phishing attacks, while individuals aged 18 to 25 demonstrated higher susceptibility compared to older age groups [4]. Despite the importance of understanding how age and gender of potential manipulators affect the deception of individuals in the context of cybersecurity, research

✉ Israa Abuelezz
israa.saad@qu.edu.qa

✉ Raian Ali
raali2@hbku.edu.qa

[1] College of Engineering, Qatar University, Doha, Qatar

[2] College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar

[3] Department of Psychology, Bournemouth University, Poole, UK

Published online: 16 December 2024

in this area is limited. One study discussed that the profile of a cybercriminal is formed by amalgamating elements including their personal traits, behavioral patterns, and demographic data, all reflective of the nature of cybercrimes they commit [5]. However, the study did not explicitly address the behavioral tendencies of attackers based on gender or age groups. Notably, the dynamics of trust in social interaction have been explored in various contexts, albeit scarcely in cybersecurity. Prior research has indicated that trust dynamics between demographic groups, such as age and gender, are influenced by a complex interplay of factors, including not only individual psychology but also cultural and societal norms, which extend the understanding of trust well beyond mere demographics [6]. This highlights a complex interplay where factors such as cultural nuances and individual risk-taking behaviors also shape trust propensities.

Prior research has demonstrated that individuals tend to trust those who have similar demographic attributes to them [7]. Yet, no research to date has investigated the effect of gender and age matching/mismatching between manipulator and target on persuasion and trust in the context of SE, especially in face-to-face interaction. This study is part of a broader research initiative exploring how demographic and visual cues of potential social engineers affect trust and security risk acceptance among Arab and UK participants. The findings from the broader research identified a tendency among participants to more likely accept security risk from, and exhibit greater trust towards, female and elderly potential manipulators [8].

This paper examines a specific SE situation where a person in urgent need could be exploited by a potential manipulator. In our scenario, a stranger approaches an individual (the participant in our study) in a public place who has lost internet connectivity, and the stranger offers the use of their mobile internet hotspot. In this situation, the persona (the stranger offering a mobile hotspot) is positioned as a potential manipulator, which could expose the target to cybersecurity risks when they are connected to the stranger's hotspot, while keeping participants informed of the security risk involved. By focusing on this example, we explore how the age and gender of potential manipulator influence the trust and risk-taking of individuals across different gender and age groups (whether matching or differing) to fall victim to SE during face-to-face interactions. Additionally, this study also investigates the role of cultural nuances in shaping the individual propensities for trust and risk-taking behaviors. Our contribution to the literature includes incorporating samples from both the UK and the Arab region, thus addressing the commonly raised critique of overreliance on WEIRD samples (Western, Education, Industrialized, Rich, and Democratic) [9]. The cultural dimension of individualism versus collectivism has been identified as one of the most significant cultural differences [10]. These differences were particularly evident when comparing Arab cultures with British cultures, as Hofstede and other studies have highlighted [11, 12].

The key contributions of this paper are delineated as follows:

1. *Investigation of Trust and Risk-taking Relationship*: The paper explores the intricate dynamics of trust and risk-taking behaviors across different age and gender groups.
2. *Assessment of the Impact of Age and Gender Similarity*: The study examines the role of similarity in age and gender between potential social engineers and individuals, exploring how these similarities may influence the individual's trust in cybersecurity contexts.
3. *Examination of the Role of Culture*: This research investigates how cultural factors shape individual differences in trust and risk-taking behaviors, by involving participants from both the UK and Arab backgrounds.

## 2 Related work

According to Social Role Theory, age and gender exert considerable influence on shaping social interactions and communication patterns [13]. The theory states that individuals are typically socialized into specific gender roles early in life, impacting their behavior, communication styles, and interactions with others. Gender, as one of the most essential social categories, is likely to significantly shape an individual's perceptions, attitudes, and behaviors [14]. Moreover, age-related roles and expectations similarly affect how individuals engage with others and perceive themselves in social settings [13]. In light of this context, gender and age can play pivotal roles in influencing individuals' responses during attempts at SE, especially in face-to-face interactions.

### 2.1 Cybersecurity behaviors: gender and age differences

Existing research reveals marked disparities in the susceptibility to cybersecurity threats based on gender and age [4, 15, 16]. For example, Kircanski et al., found that older and younger adults are vulnerable to cyberthreats particularly when induced emotionally [17]. Another study highlighted that individuals within the young adult demographic, specifically those aged 18–25, exhibit greater vulnerability to phishing attacks [4]. Contrasting findings from another study, however, observed that there was no significant difference in susceptibility to cyberthreats across different age groups [18]. Despite these findings, it has been suggested that awareness of and caution toward security risks increases with age, potentially decreasing their vulnerability to phishing attacks. This is supported by the observation that older adults display a more robust Information Security Awareness (ISA) and a heightened aversion to security risk, with ISA scores that appear to increase with advancing age [15, 19]. The uniformity of cybersecurity risk susceptibility across different age groups is being challenged, suggesting that the range of cybersecurity behaviors requires further detailed investigation [20].

Similarly, gender differences in information security behaviors show nuanced patterns. While some research indicated no gender differences in vulnerability to phishing attacks [21], other studies have found that women tend to be more vulnerable to phishing attacks [15] and demonstrate less secure password management [22]. Conversely, research has also found that women are more concerned about information privacy, more likely to adapt privacy measures [23] and exhibit better InfoSec practices than men [4, 15]. This complexity is further nuanced among young women, who have shown to be more concerned about their privacy on social networks than young men, and more likely to use privacy measure [24]. As a result, the interplay of age and gender distinctly affects InfoSec behaviors, highlighting the critical necessity to integrate these considerations into cybersecurity strategies. A study examining the combined effects of age and gender on email phishing susceptibility suggests that the susceptibility to phishing varies across age groups and genders. Specifically, it reveals that older women are more susceptible to phishing than younger women, and younger men are more susceptible than older men [25]. Yet, investigations into this specific intersection of demographic factors remain scarce.

Cybersecurity behaviors are shaped by various factors beyond gender and age, including technical expertise, training, and social attributes such as personality traits and cultural background. Research utilizing the Big Five personality model demonstrates that personality impacts security practices consistently across different age groups, indicating that traits like openness, conscientiousness, agreeableness, extraversion, and neuroticism influence individuals similarly, regardless of age [26]. In addition, technical knowledge and training are significant factors that mediate gender differences in cybersecurity, particularly in phishing susceptibility. Women, on average, have been found to have less technical training and knowledge, leading to higher vulnerability [4]. This suggests that enhancing technical education could help in mitigating these gender-related disparities. Moreover, cultural factors may serve as potential influencers when assessing the differences in vulnerability to cybersecurity threats and security behaviors across age and gender groups. A study comparing employees in Sweden, the U.S., and India found that the efficacy of security behaviors was influenced by cultural disparities among the employees. Nonetheless, age and gender were less impactful on the employees resistance to phishing [27]. Another study in Qatar highlighted that trust, technology overconfidence, and religious beliefs markedly increased email phishing vulnerability, underscoring the need for culture-specific cybersecurity education [28].

## 2.2 Trust and risk-taking: insights from cybersecurity and beyond

Research in various domains has examined the association between trust and risk-taking behaviors, highlighting the role of trust in influencing risky decision-making. In cybersecurity, for example, Li et al. (2008) found a strong relationship between trust in online technologies and whether users will willingly engage in riskier online activities, such as sharing personal information or performing transactions with unfamiliar vendors [29]. The research also observed that with the increase of trust, users cognitive and emotional barriers to risk diminish, leading to a greater willingness to disclose sensitive information even in ambiguous online environments. Similarly, Thatcher et al. (2011) found that individuals with higher trust in information technology systems are more likely to engage in postadoption exploratory behaviors, such as using more features of the system [30]. In SE contexts, attackers exploit trust to elicit risky behavior from their targets. Workman (2007) observed that trust in interpersonal relationships is vital for phishing attacks, as it lowers the perceived risk and allows the manipulation of individuals [31]. After trust is established, victims are more likely to act in a way that compromises security, reinforcing the idea that trust supposedly reduces perceived risk in cybersecurity contexts.

Beyond cybersecurity, trust's influence on risk-taking is well-documented in economics and workplace settings. Studies by Colquitt et al. (2007) and Mayer et al. (1995) demonstrate that increased trust leads to risky decision-making, particularly in organizational settings [32, 33]. Colquitt et al. (2007) highlight several risk-taking behaviors in organizational setting influenced by trust, such as engaging in challenging tasks (task performance), helping others beyond assigned duties (citizenship behavior), and reducing counterproductive behaviors [32]. As trust increases, individuals are more willing to accept vulnerability in decision-making. This willingness extends to taking on tasks or challenges with uncertain outcomes. Findings from e-commerce research (Gefen, 2000; Jarvenpaa et al., 2000) also show that trust in online stores reduces perceived risks and thus makes consumers willing to provide personal details or participate in financial transactions [34, 35]. Gefen (2000) further highlights that familiarity with an e-commerce platform and its processes builds trust, even without extensive prior interaction, which encourage users to make inquiries or purchases [34].

### 2.3 The role of gender and age in trust and interpersonal influence

Studies across various fields indicate that age and gender have a significant impact on how effectively individuals can build trust and rapport [36–38], highlighting potential areas for exploitation by social engineers. Despite limited research on the role of age and gender in persuasion within the realm of cybersecurity attacks, related findings from marketing, education, and health suggest their significant influence. It is important to consider how the matching of these characteristics between the communicator and the receiver can impact the trust. Educational research shows that gender-matched teacher-student pairs often yield better student performance, with female students benefiting from female teachers [38–40]. Likewise, teacher-student gender matching modestly enhances academic outcomes, with female teachers slightly outperforming male teachers in promoting progress for all students [39]. While gender matching in teacher-student relationships may not always rely explicitly on persuasion, trust and relationship building that arise from gender matching can influence outcomes and provide insights into how social engineers can use these factors to manipulate trust in cybersecurity.

In healthcare, gender matching impacts patient outcomes and satisfaction. One study using virtual consultations showed patient satisfaction hinged on physician–patient gender matching, especially for female patients with female physicians [41]. The findings also revealed that female patients expressed higher satisfaction levels when paired with female physicians who employed a caring communication approach, as opposed to those who did not. This reflects how gender-specific communication styles can enhance trust. In security-related decision-making, the modality of interaction could be a critical factor in influencing the target's trust and the overall success of a cybersecurity attack. In marketing, gender and age matching's impact on sales is debated. Dwyer et al. found that opposite-gender pairings improved sales, whereas age similarity didn't affect outcomes [37]. Conversely, Stros et al. reported that female salespeople were preferred by female customers, suggesting an advantage for female sales representatives in sales interactions [36]. The study also suggested that employing female salespeople may potentially enhance sales interactions and increase sales success.

In light of this literature, numerous studies across marketing, education, and healthcare have explored how communicator-recipient gender and age matching affects perceptions and attitudes of individuals. However, communication and influence approaches studied in these domains typically does not encompass risks, or they involve a type of risk-taking that differs from the risks associated with manipulation in cybersecurity context. In marketing, risk-taking often includes the practical or pleasant benefits associated with a product and its contractual terms. It also involves the possibility of not making a sale, which can lead to financial losses, missed incentives, or reduced rewards for the salesperson. However, in our study, the focus of perceived risk is from the perspective of the recipient, not the communicator. The risks we examine are those taken by the potential target of manipulation (the recipient), rather than the risk experienced by the person attempting the persuasion (the salesperson or communicator). Risk-taking in marketing, which mainly involves personal economic consequences, therefore differs from the far-reaching risks in cybersecurity. In cybersecurity, by contrast, risk-taking involves traversing the digital landscape, which can have a wide impact that extends beyond financial losses to breaches of privacy and damage to one's reputation. Building on this foundation, we formulate our research questions for the current study as follows:

*RQ1*: Does matching the age and gender of an individual with that of a potential social engineer, within the context of face-to-face interactions, affect the individual's willingness to trust and take cybersecurity risks?

**Hypothesis 1** *We hypothesize that participants will exhibit greater trust and a higher propensity to take security risks when the age and gender of the potential social engineer match their own.*

*RQ2*: Does the willingness to accept security risks correlate with the level of trust perceived in the potential social engineer?

**Hypothesis 2** *We hypothesize that there will be a significant positive correlation between the level of trust perceived in the potential social engineer and the participant's willingness to take security risks.*

## 3 Method

This section of the manuscript outlines the methodology utilized, commencing with the creation of the personas and the procedure implemented in face-validation. We developed personas to simulate a real SE scenario and improve ecological validity. The use of visual personas instead of textual descriptions (e.g. aged, female) allows participants to engage with a more immersive, lifelike interaction. We wanted to create a realistic scenario in which participants' trust and risk-taking behaviors are assessed more naturally and reflect real-life encounters. The personas were carefully designed based on the factors assessed, as explained in the subsequent section. The following sections also illustrate the data set and the group of participants involved in the study, as well as the measures used in the analysis. The approaches used for statistical analysis will be discussed.

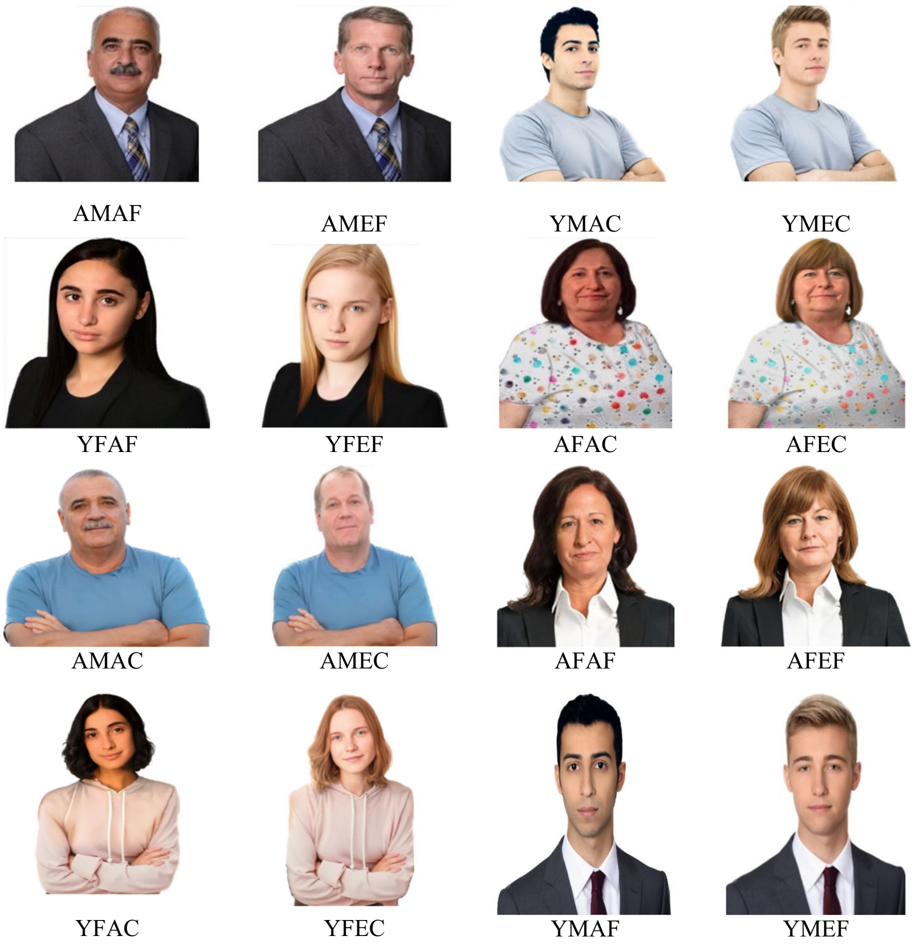

**Fig. 1** The 16 personas used in the study < **A**ged | **Y**oung, **M**ale | **F**emale, **A**rab | **E**uropean, **F**ormal | **C**asual >

### 3.1 Personas development

The study presented a scenario mirroring a common real-world experience where an individual loses internet connectivity in a public setting. In this scenario, a stranger, referred to as a "persona" in our study, offers an internet connection through their mobile hotspot, a situation that could potentially expose one to cybersecurity threats and positions the persona as a possible manipulator. These personas were designed with varied demographic and visual attributes, including age groups (aged and young adults), genders (female and male), ethnic appearances (Arab and European facial features), and attire formality (formal or casual). This process yielded 16 unique persona profiles. A shorthand notation was employed to represent each persona's attributes: < **A**ged | **Y**oung, **M**ale | **F**emale, **A**rab | **E**uropean, **F**ormal | **C**asual >. For instance, 'YMEF' denotes a Young Male European with Formal attire. These personas were created using FaceApp's artificial intelligence feature [42]. It is imperative to note that these personas were carefully designed to reflect the specific attributes being examined—age, gender, ethnicity, and look formality—while intentionally omitting extraneous elements such as religious cues. Style consistency was maintained within age groups for both formal and informal attire categories. Figure 1 in the manuscript represents the 16 personas used in the study.

A face validation process was carried out to confirm ethnic representation and face validity of the personas. We recruited individuals from diverse cultural backgrounds for this evaluation to ensure that the personas not only accurately represented European or Arab ethnic characteristics, but also were perceived as ordinary in terms of likability and conventional appearance. The participants examined the 16 personas and evaluated each one for age, ethnicity (European or Arab), formality attire, and provided additional observations. Based on this feedback, modifications were made. For instance, personas in formal attire originally shown smiling had their smiles toned down to better suit formal standards. Additionally, for the casual female personas, sleeveless tops were deemed not suitable for some Arab nations, so we opted for short sleeves. Additionally, in order to increase authenticity, we made adjustments to the hair colors to align with typical regional characteristics. This included opting for lighter shades of blonde for European and darker shades for

Arab personas. The sequence in which personas were presented to participants was randomized to prevent order bias, reduce learning effect, and limit fatigue effects from influencing the ratings.

## 3.2 Dataset

Participants were drawn from the Arab Gulf Cooperation Council (GCC) and the United Kingdom (UK) through the data collection service of TGM Research, a company specializing in data collection for research [43]. These two cultural contexts were selected based on their divergent moral principles and societal values, offering a diverse terrain for comparative examination. To evaluate these cultural differences, a country comparison was conducted using the GLOBE (Global Leadership and Organizational Behavior Effectiveness) study framework, which illustrated prominent disparities in aspects like Power Distance and Collectivism between the UK and GCC countries [44]. The survey was constructed using SurveyMonkey, a platform designed for creating and managing questionnaires [45]. The study was conducted between November 2023 to December 2023, during which participants were recruited, screened, and completed the survey on the platform. To ensure comprehensibility and eliminate potential misunderstandings or ambiguous language, a trial run of the survey was conducted with a small sample before its full deployment.

Eligibility for survey participation was determined by factors including age (over 18), country of birth and current residence within the GCC (Saudi Arabia, Qatar, Bahrain, Kuwait, Oman, and the UAE) or the UK (England, Scotland, Wales, and Northern Ireland). Participants were required to self-identify with the cultural norms and practices of either the Arab GCC or the UK. A prerequisite for participation was a basic understanding and previous use of mobile Internet hotspots. All participants provided informed consent and were given the option to withdraw from the survey at any time. To ensure data quality, attention checks were incorporated into the survey. Participants who failed these checks or completed the survey hastily (less than 50% of the median duration calculated after removing lengthy duration outliers) were excluded from the analysis. Ethical approval for this study was obtained from the Institutional Review Board (IRB) at Hamad Bin Khalifa University. Participants who indicated a non-binary gender were omitted from both the Arab and UK datasets because their sample size was small, with each group containing fewer than five participants. Individuals aged 60 and above were excluded from both the Arabic and English datasets as we received no responses from Arab participants in this age group. The final dataset comprised 635 participants, with 322 from the Arab GCC and 313 from the UK. The dataset used in this study, which was part of a larger study, is available via the Open Science Framework (OSF) link provided in the Data Availability section.

## 3.3 Measures

### 3.3.1 Demographic measures

Participants provided their age and gender, with age recorded as an exact number of years and gender specified in a free-text format. Completion of both the age and gender fields was mandatory.

### 3.3.2 Risk-taking intention and trust

In the given scenario, participants' inclination to engage in risk-related behavior was quantified by questioning their willingness to accept a mobile internet hotspot connection from an unknown individual depicted as 'persona' in the study. Participants were asked to provide their likelihood of accepting such an offer by responding to the following question: '*How likely would you accept the offer of this person to use his/her mobile Internet hotspot*?' Additionally, to understand their perception of risk, participants rated their trust towards the 'persona' with the question: '*How likely do you think this person may try to compromise your data privacy and security while you are connected through his/her mobile internet hotspot?*' Responses to both queries were recorded using a six-point Likert Scale, where 1 indicated 'very unlikely' and 6 indicated 'very likely'. It is worth noting that prior to the assessment, participants were informed of the potential risks associated with using third-party hotspots, particularly the risk of unauthorized data access. Further details of the complete survey design can be found at the OSF link mentioned in the Data Availability section of this manuscript.

## 3.4 Data analysis

The analysis was conducted using JASP software version 0.18.3 [46]. Participants' ages were categorized into two groups to reflect stages of adulthood: early adulthood (18–35) and middle adulthood (36–59), in line with recognized developmental periods as outlined in a prior sources [47, 48]. This categorization also mirrored the age groups of the personas presented to participants, namely 'young' and 'aged'. In this study, the variable concerning the formal or casual appearance of the personas was omitted, allowing for the consolidation of acceptance and trust scores within the personas' respective gender and age groupings of the same ethnicity. For example, acceptance and trust scores for the 'AMAF' (Aged Male Arab Formal) persona were combined with those for the 'AMAC' (Aged Male Arab Casual). Notably, responses to the risk perception question, indicative of trust, were reverse-coded; a greater perceived risk of a data privacy breach by the stranger indicated lower trust.

Focusing on demographic assessment, we compared participants' acceptance and trust levels with personas sharing their ethnicity; Arab participants were evaluated against Arab personas, and UK participants against European personas. The combined acceptance and trust scores resulted in eight separate columns for each ethnic group (Arab and European personas), with four columns assigned to each measure. Totals for each column ranged from 2 to 12. For a detailed breakdown of these columns, please refer to the dataset file attached in the OSF link provided in the Supplementary Material section. The explanation is displayed under the Data Dictionary tab of the dataset.

To address the first research question, a one-way repeated measures ANOVA was employed to examine within-subjects variance across the four persona characteristics—Aged Male (AM), Aged Female (AF), Young Female (YF), and Young Male (YM). Given the robustness of repeated measures ANOVA to violations of normality with non-normal data and large sample size, as discussed by Blanca et al. [49], we proceeded without non-parametric tests despite the ordinal nature of our data. Sphericity assumption, as tested by Mauchly's test ($p$ < 0.001), was not met for most of the within-subjects effects. Therefore, degrees of freedom were corrected using Greenhouse–Geisser estimate. Detailed results from the sphericity assumption tests are available in Tables 1S and 2S in the supplementary material referenced in the Data Availability section. To mitigate the risk of Type I errors from multiple comparisons, Bonferroni correction was applied. Post-hoc comparisons on trust and risk-taking participants were performed to further explore the specific differences between age and gender categories (e.g., early adulthood females vs. middle adulthood females) of each participant group (Arab and British). This analysis allowed us to identify and interpret significant variations in trust and risk-taking behavior based on demographic similarities between the personas and participants.

To explore the second research question, a Spearman's rho correlation analysis was utilized to examine the relationship between acceptance and trust scores. The analysis examined the relationship between acceptance and trust ratings among participant age and gender groups, focusing on the four personas (AM, AF, YM, and YF) that corresponded to the participants' own ethnicity in both datasets.

## 4 Results

### 4.1 Descriptive statistics

The descriptive statistics for the demographic characteristics of participants' age and gender are displayed in Table 1. The gender distribution shows differences between the participant groups, with a higher percentage of females in the British sample (57.19%) than in the Arab sample (45.03%). Specifically in the middle adulthood group, the British participants showed a disparity in gender representation with 48.6% females and 62.69% males, similarly to Arab participants who have 27.59% females and a notably higher percentage of males at 55.37%. Regarding age, the British participants exhibit a slightly higher mean age (M) of 37.93 years compared to the Arab participants' mean age of 34.64 years, with both groups demonstrating comparable age ranges.

**Table 1** Participant demographics

| Variables | Participants (N = 635) | |
|---|---|---|
| | Arab (N = 322) | British (N = 313) |
| Gender (%) | | |
| Female | 145 (45.03) | 179 (57.19) |
| Early Adulthood | 105 (72.41) | 92 (51.40) |
| Middle Adulthood | 40 (27.59) | 87 (48.60) |
| Male | 177 (54.97) | 134 (42.81) |
| Early Adulthood | 79 (44.63) | 50 (37.31) |
| Middle Adulthood | 98 (55.37) | 84 (62.69) |
| Age | | |
| M (SD) | 34.64 (9.82) | 37.94 (11.98) |
| Range | 18–57 | 18–59 |

### 4.2 ANOVA results on the acceptance and trust

This section will address RQ1 and Hypothesis 1. Table 2 displays the within-subjects effects of the Persona Age-Gender Repeated Measures (RM) Factor on the acceptance and trust scores among the age-gender groups of participants in both Arab and British samples. The age-gender groups of participants are defined as follows: early adulthood females (EA-F), middle adulthood females (MA-F), early adulthood males (EA-M), and middle adulthood males (MA-M). The RM Factor corresponds to the persona age-gender groups, namely: AM, AF, YM, YF. Each sample was assessed by the RM Factor with personas' ethnicity matching the participants' own ethnicity. The table reports mean scores for acceptance ($M_a$) and trust ($M_t$), in addition to p-values for acceptance ($p_a$) and trust ($p_t$), and effect sizes represented by partial eta squared (${\eta_p}^2$) for acceptance (${\eta_p}^2{}_a$) and trust (${\eta_p}^2{}_t$), for each group comparison.

Significant influences of the RM factor were evident across all participant groups. In the groups of the female participants, early adulthood females (EA-F) within the Arab sample exhibited significant effects on acceptance ($p_a$ < 0.001) and trust ($p_t$ < 0.001), with the largest effect size for

**Table 2** Within-subjects effects showing the influence of the persona age-gender RM factor on acceptance and trust scores for each participant age-gender group within Arab and British samples

| Participant age-gender group | Persona age-gender RM factor | Participants (N = 635) | | | | | |
|---|---|---|---|---|---|---|---|
| | | Arab (N = 322) | | | British (N = 313) | | |
| | | $M_a/M_t$ | $p_a/p_t$ | $\eta_p{}^2{}_a/\ \eta_p{}^2{}_t$ | $M_a/M_t$ | $p_a/p_t$ | $\eta_p{}^2{}_a/\ \eta_p{}^2{}_t$ |
| EA-F | AM | 6.71/6.81 | < .001/ < .001 | 0.192/0.105 | 5.71/7.30 | < .001/ < .001 | 0.237/0.271 |
| | AF | 7.30/7.11 | | | 7.39/8.72 | | |
| | YM | 5.71/5.74 | | | 6.15/7.09 | | |
| | YF | 7.83/6.92 | | | 7.10/8.01 | | |
| MA-F | AM | 6.70/6.55 | 0.027/0.005 | 0.077/0.120 | 4.87/7.56 | < .001/ < .001 | 0.095/0.134 |
| | AF | 7.35/6.80 | | | 5.51/8.01 | | |
| | YM | 6.25/5.93 | | | 4.59/7.01 | | |
| | YF | 7.28/7.33 | | | 5.13/7.31 | | |
| EA-M | AM | 8.85/8.22 | < .001/ < .001 | 0.094/0.243 | 6.38/7.04 | < .001/ < .001 | 0.215/0.239 |
| | AF | 8.92/8.44 | | | 8.22/8.94 | | |
| | YM | 7.53/6.08 | | | 6.48/7.20 | | |
| | YF | 8.38/7.30 | | | 7.88/8.34 | | |
| MA-M | AM | 7.41/6.66 | < .001/ < .001 | 0.145/0.216 | 6.07/7.66 | < .001/ < .001 | 0.070/0.119 |
| | AF | 7.42/6.87 | | | 6.38/8.05 | | |
| | YM | 6.01/5.16 | | | 5.73/7.12 | | |
| | YF | 6.94/5.94 | | | 6.31/7.63 | | |

**p* < .05, ** *p* < .01, *** *p* < .001

[Persona: < Aged | Young, Male | Female >]; [Participant: EA-F: Early Adulthood Female, MA-F: Middle Adulthood Female, EA-M: Early Adulthood Male, MA-M: Middle Adulthood Male]. The persona's ethnic appearance (Arab or European) matches the ethnicity of the participant group

acceptance ($\eta_p{}^2{}_a = 0.192$) observed among all Arab participant groups. A similar pattern emerged in the British sample, where EA-F showed the most pronounced effects on acceptance ($p_a < 0.001$, $\eta_p{}^2{}_a = 0.237$) and trust ($p_t < 0.001$, $\eta_p{}^2{}_t = 0.271$), reflecting the highest effect sizes reported in the British sample. For MA-F, the Arab cohort showed significant effects on acceptance ($p_a = 0.027$, $\eta_p{}^2{}_a = 0.077$) and trust ($p_t = 0.005$, $\eta_p{}^2{}_t = 0.120$), although with smaller effect sizes compared to the British cohort, which exhibited larger effect sizes for acceptance ($p_a < 0.001$, $\eta_p{}^2{}_a = 0.095$) and trust ($p_t < 0.001$, $\eta_p{}^2{}_t = 0.134$).

In the groups of male participants, significant RM factor effects were noted for EA-M and MA-M on acceptance and trust across Arab and British participants ($p_a$, $p_t < 0.001$). The Arab EA-M group had a moderate effect on acceptance ($\eta_p{}^2{}_a = 0.094$) and a large effect on trust ($\eta_p{}^2{}_t = 0.243$), while the British EA-M group showed similar effect sizes on both acceptance and trust ($\eta_p{}^2{}_a = 0.215$, $\eta_p{}^2{}_t = 0.239$), which were accompanied by the highest mean scores for acceptance and trust across all persona factor levels (AM: $M_a = 6.38$, $M_t = 7.04$; AF: $M_a = 8.22$, $M_t = 8.94$; YM: $M_a = 6.48$, $M_t = 8.20$; YF: $M_a = 7.88$, $M_t = 8.34$).

In order to determine if participants exhibited a significant preference for one demographic combination of persona (age x gender) over another, post-hoc analyses were conducted, categorizing gender by age groups, as presented in Tables 3 and 4. The tables report *pbonf*, indicating Bonferroni-adjusted p-values for acceptance (*pbonf_a*) and trust (*pbonf_t*), and Cohen's d, representing the effect size for acceptance (Cohen's $d_a$) and trust (Cohen's $d_t$).

Table 3 reveals significant differences in how the female participants in early adulthood (EA-F) from both Arab and British groups perceived the personas. Among EA-F, Arab participants demonstrated a significant preference for YF personas over AM personas in terms of acceptance (*pbonf_a* < 0.001, Cohen's $d_a = 0.434$). However, this preference was not observed in trust where the difference was not significant (*pbonf_t* = 1.000). In contrast, British EA-F participants displayed a significant preference for YF over AM personas on both acceptance and trust with notable effect sizes (*pbonf_a* < 0.001, Cohen's $d_a = 0.533$; *pbonf_t* < 0.001, Cohen's $d_t = 0.348$). Additionally, within the Arab EA-F cohort, a significant difference favored AM over YM personas in both acceptance and trust (*pbonf_a* < 0.001, *pbonf_t* < 0.001), while in the British EA-F group, these comparisons did not

**Table 3** Post-hoc comparisons of acceptance and trust scores between Arab and British female participants categorized by age group across the persona age-gender RM factor

| Persona age-gender RM factor | | Female participants | | | |
|---|---|---|---|---|---|
| | | Early adulthood (N = 197) | | | |
| | | Arab (N = 105) | | British (N = 92) | |
| | | Acceptance | Trust | Acceptance | Trust |
| | | pbonf_$_a$/Cohen's $d_a$ | pbonf_$_t$/Cohen's $d_t$ | pbonf_$_a$/Cohen's $d_a$ | pbonf_$_t$ /Cohen's $d_t$ |
| AM | AF | 0.152/−0.226 | 1.000/−0.140 | < .001/−0.646 | < .001/−0.696 |
| | YF | < .001/−0.434 | 1.000/−0.052 | < .001/−0.533 | < .001/−0.348 |
| | YM | < .001/0.393 | < .001/0.489 | 0.210/−0.171 | 1.000/0.107 |
| AF | YF | 0.240/−0.208 | 1.000/0.087 | 0.984/0.112 | < .001/0.348 |
| | YM | < .001/0.620 | < .001/0.629 | < .001/0.475 | < .001/0.804 |
| YF | YM | < .001/0.828 | < .001/0.541 | < .001/0.362 | < .001/0.455 |
| Persona age-gender RM factor | | Middle adulthood (N = 127) | | | |
| | | Arab (N = 40) | | British (N = 87) | |
| | | Acceptance | Trust | Acceptance | Trust |
| | | pbonf_$_a$/ Cohen's $d_a$ | pbonf_$_t$ /Cohen's $d_t$ | pbonf_$_a$/ Cohen's $d_a$ | pbonf_$_t$ /Cohen's $d_t$ |
| AM | AF | 0.666/−0.242 | 1.000/−0.111 | 0.004/−0.253 | 0.040/−0.194 |
| | YF | 0.949/−0.215 | 0.190/−0.345 | 1.000/−0.101 | 0.746/0.110 |
| | YM | 1.000/0.168 | 0.492/0.278 | 0.718/0.115 | 0.005/0.239 |
| AF | YF | 1.000/0.028 | 0.859/−0.234 | 0.242/0.152 | < .001/0.304 |
| | YM | 0.046/0.410 | 0.093/0.390 | < .001/0.368 | < .001/0.433 |
| YF | YM | 0.076/0.382 | < .001/0.624 | 0.022/0.216 | 0.418/0.130 |

*$p < .05$, **$p < .01$, ***$p < .001$

< Aged | Young, Male | Female >. The persona's ethnic appearance (Arab or European) matches the ethnicity of the participant group

yield significant results (*pbonf_*$_a$ = 0.210, *pbonf_*$_t$ = 1.000). Furthermore, within the young personas (YM vs. YF), the Arab EA-F group showed a significant bias towards YF (*pbonf_*$_a$ < 0.001, Cohen's $d_a$ = 0.828), a trend that was mirrored in the British EA-F group but with a smaller effect size (*pbonf_*$_a$ < 0.001, Cohen's $d_a$ = 0.362).

The post-hoc comparisons within the middle adulthood female (MA-F) group did not yield as many significant results. In the Arab cohort, MA-F participants did not exhibit significant differences when comparing AM with AF, YF, or YM personas in terms of acceptance and trust. In contrast, the British MA-F cohort showed significant differences, with a preference for AF over AM in acceptance and trust (*pbonf_*$_a$ = 0.004, *pbonf_*$_t$ = 0.040) and a significant preference for AM over YM in trust (*pbonf_*$_t$ = 0.005). Furthermore, the British MA-F group did not show significant differences in acceptance when comparing AF with YF (*pbonf_*$_a$ = 0.242); however, trust was significantly higher for AF compared to YF (*pbonf_*$_t$ < 0.001, Cohen's $d_t$ = 0.304). Among the younger personas within the Arab MA-F group, no significant difference in acceptance was found between YF and YM (*pbonf_*$_a$ = 0.076), whereas the British MA-F group showed a significant preference for YF over YM (*pbonf_*$_a$ = 0.022). Conversely, trust was significantly higher for YF compared to YM in the Arab cohort (*pbonf_*$_t$ < 0.001), a pattern not observed in the British cohort (*pbonf_*$_t$ = 0.418).

In the analysis of male participants' preferences for different persona demographic combinations, Table 4 details the post-hoc comparisons. Early adulthood males (EA-M) from the Arab cohort showed a significant preference for AM persona over YM persona, both in acceptance (*pbonf_*$_a$ < 0.001, Cohen's $d_a$ = 0.497) and trust (*pbonf_*$_t$ < 0.001, Cohen's $d_t$ = 0.889). No such preferences were observed in the British EA-M sample for this comparison (*pbonf_*$_a$ = 1.000, *pbonf_*$_t$ = 1.000). However, British EA-M participants demonstrated a pronounced preference for AF and YF personas over AM in acceptance (AM vs. AF: *pbonf_*$_a$ < 0.001, Cohen's $d_a$ = 0.668; AM vs. YF: *pbonf_*$_a$ < 0.001,

**Table 4** Post-hoc comparisons of acceptance and trust scores between Arab and British male participants categorized by age group across the persona age-gender RM factor

| Persona age-gender RM factor | | Male participants | | | |
|---|---|---|---|---|---|
| | | Early adulthood (N = 129) | | | |
| | | Arab (N = 79) | | British (N = 50) | |
| | | Acceptance<br>pbonf_$_a$/ Cohen's $d_a$ | Trust<br>pbonf_$_t$ /Cohen's $d_t$ | Acceptance<br>pbonf_$_a$/ Cohen's $d_a$ | Trust<br>pbonf_$_t$ /Cohen's $d_t$ |
| AM | AF | 1.000/−0.029 | 1.000/−0.095 | < .001/−0.668 | < .001/−0.893 |
| | YF | 0.853/0.177 | 0.018/0.379 | < .001/−0.544 | < .001/−0.611 |
| | YM | < .001/0.497 | < .001/0.889 | 1.000/−0.036 | 1.000/−0.075 |
| AF | YF | 0.530/0.205 | 0.001/0.473 | 1.000/0.123 | 0.425/0.282 |
| | YM | < .001/0.525 | < .001/0.984 | < .001/0.631 | < .001/0.817 |
| YF | YM | 0.049/0.320 | < .001/0.510 | 0.001/0.508 | 0.004/0.536 |
| Persona age-gender RM factor | | Middle adulthood (N = 182) | | | |
| | | Arab (N = 98) | | British (N = 84) | |
| | | Acceptance<br>pbonf_$_a$/ Cohen's $d_a$ | Trust<br>pbonf_$_t$ /Cohen's $d_t$ | Acceptance<br>pbonf_$_a$/ Cohen's $d_a$ | Trust<br>pbonf_$_t$ /Cohen's $d_t$ |
| AM | AF | 1.000/−0.004 | 1.000/−0.086 | 0.385/−0.110 | 0.092/−0.181 |
| | YF | 0.255/0.170 | 0.004/0.304 | 0.923/−0.084 | 1.000/0.011 |
| | YM | < .001/0.506 | < .001/0.629 | 0.235/0.122 | 0.006/0.247 |
| AF | YF | 0.229/0.173 | < .001/0.389 | 1.000/0.025 | 0.061/0.192 |
| | YM | < .001/0.509 | < .001/0.714 | < .001/0.232 | < .001/0.427 |
| YF | YM | < .001/0.336 | 0.002/0.325 | 0.003/0.207 | 0.010/0.236 |

**p* < .05, ***p* < .01, ****p* < .001

< Aged | Young, Male | Female > . The persona's ethnic appearance (Arab or European) matches the ethnicity of the participant group

Cohen's $d_a = 0.544$) and trust (AM vs. AF: *pbonf_$_t$* < 0.001, Cohen's $d_t = 0.893$; AM vs. YF: *pbonf_$_t$* < 0.001, Cohen's $d_t = 0.611$), with substantial effect sizes. The British EA-M group also showed a significant preference for YF over YM in acceptance (*pbonf_$_a$* = 0.001, Cohen's $d_a = 0.508$) and trust (*pbonf_$_t$* = 0.004, Cohen's $d_t = 0.536$). In the Arab EA-M cohort, a similar trend was observed, favoring YF over YM, with a lower significance in acceptance (*pbonf_$_a$* = 0.049, Cohen's $d_a = 0.320$) but higher significance in trust (*pbonf_$_t$* < 0.001, Cohen's $d_t = 0.510$).

For middle adulthood male (MA-M), the Arab participants did not show significant preferences when comparing AM with AF (*pbonf_$_a$* = 1.000, *pbonf_$_t$* = 1.000). However, there was a significant preference for AM over YM in both acceptance (*pbonf_$_a$* < 0.001, Cohen's $d_a = 0.506$) and trust (*pbonf_$_t$* < 0.001, Cohen's $d_t = 0.629$) with moderate effect sizes. Unlike the British EA-M group, the British MA-M participants did not exhibit a statistical preference in acceptance or trust when comparing AM with AF and YF (AM vs. AF: *pbonf_$_a$* = 0.385, *pbonf_$_t$* = 0.092; AM vs. YF: *pbonf_$_a$* = 0.923, *pbonf_$_t$* = 1.000). Nevertheless, both Arab and British MA-M participants displayed a significant preference for AF over YM in acceptance (Arab: *pbonf_$_a$* < 0.001; British: *pbonf_$_a$* < 0.001) and trust (Arab: *pbonf_$_t$* < 0.001, Cohen's $d_t = 0.714$; British: *pbonf_$_t$* < 0.001, Cohen's $d_t = 0.427$), with the Arab cohort showing more pronounced effect sizes. Furthermore, a significant preference for YF over YM was evident in both acceptance and trust among Arab and British MA-M participants, confirming a consistent favorability towards female personas across age groups (Arab: *pbonf_$_a$* < 0.001, *pbonf_$_t$* = 0.002; British: *pbonf_$_a$* = 0.003, *pbonf_$_t$* = 0.010).

## 4.3 Spearman's rho correlation between acceptance and trust in personas

This section will address RQ2 and Hypothesis 2. Tables 5 and 6 detail the correlations between acceptance of the hotspot

**Table 5** Correlation between acceptance and trust scores among female participants categorized by age group

| Persona variable | Female participants | |
|---|---|---|
| | Early adulthood (N = 197) | |
| | Acceptance-trust correlation | |
| | Arab (N = 105) | British (N = 92) |
| | $p_{value}$/Spearman's $\rho$ | $p_{value}$/ Spearman's $\rho$ |
| AM | < .001/0.480 | .019/0.244 |
| AF | < .001/0.483 | < .001/0.486 |
| YM | < .001/0.377 | .001/0.328 |
| YF | < .001/0.432 | < .001/0.431 |
| Persona variable | Middle adulthood (N = 127) | |
| | Acceptance-trust correlation | |
| | Arab (N = 40) | British (N = 87) |
| | $p_{value}$/Spearman's $\rho$ | $p_{value}$/Spearman's $\rho$ |
| AM | < .001/ 0.520 | 0.738/0.036 |
| AF | < .001/ 0.601 | 0.187/0.143 |
| YM | < .001/ 0.520 | 0.778/0.031 |
| YF | 0.002/0.467 | 0.150/0.156 |

*$p$ < .05, **$p$ < .01, ***$p$ < .001

< Aged | Young, Male | Female > . The persona's ethnic appearance (Arab or European) matches the ethnicity of the participant group

**Table 6** Correlation between acceptance and trust scores among male participants categorized by age group

| Persona variable | Male participants | |
|---|---|---|
| | Early adulthood (N = 129) | |
| | Acceptance-trust correlation | |
| | Arab (N = 79) | British (N = 50) |
| | $p_{value}$/Spearman's $\rho$ | $p_{value}$/Spearman's $\rho$ |
| AM | < .001/0.494 | < .001/0.476 |
| AF | < .001/0.602 | < .001/0.474 |
| YM | < .001/0.524 | < .001/0.554 |
| YF | < .001/0.496 | < .001/0.545 |
| Persona Variable | Middle Adulthood (N = 182) | |
| | Acceptance-trust correlation | |
| | Arab (N = 98) | British (N = 84) |
| | $p_{value}$/Spearman's $\rho$ | $p_{value}$/Spearman's $\rho$ |
| AM | < .001/0.617 | < .001/0.485 |
| AF | < .001/0.583 | < .001/0.459 |
| YM | < .001/ 0.620 | < .001/0.580 |
| YF | < .001/0.514 | < .001/0.490 |

*$p$ < .05, **$p$ < .01, ***$p$ < .001

< Aged | Young, Male | Female > . The persona's ethnic appearance (Arab or European) matches the ethnicity of the participant group

offer and trust in personas by female and male participants in Arab and UK datasets. The tables display both the $p_{value}$ and Spearman's rho correlation coefficient (Spearman's $\rho$) for each group.

As evidenced in Table 5, a significant correlation pattern is discernible among female participants, with Spearman's $\rho$ indicating the strength and direction of the relationships. For early adult Arab females (N = 105), acceptance of the offer significantly correlated with trust in personas across all personas, with Spearman's $\rho$ values of 0.480 for AM, 0.483 for AF, 0.377 for YM, and 0.432 for YF. British female participants (N = 92) showed a moderate positive correlation for AF ($p < 0.001$, Spearman's $\rho = 0.486$) and YF ($p < 0.001$, Spearman's $\rho = 0.431$), and a weaker positive correlation for AM (Spearman's $\rho = 0.244, p = 0.019$) and YM (Spearman's $\rho = 0.328$, $p = 0.001$).

In the middle adulthood, Arab female participants continued to show a strong positive correlation between acceptance of the offer and trust in personas (AM: $p < 0.001$, Spearman's $\rho = 0.520$; AF: $p < 0.001$, Spearman's $\rho = 0.601$; YM: $p < 0.001$, Spearman's $\rho = 0.520$; and YF: $p = 0.002$, Spearman's $\rho = 0.467$). Contrastingly, no significant correlation was observed between acceptance and trust among female British participants in this age group for all personas (AM: Spearman's $\rho = 0.036$, $p = 0.738$; AF: Spearman's $\rho = 0.143$, $p = 0.187$); YM: Spearman's $\rho = 0.031$, $p = 0.778$; YF: Spearman's $\rho = 0.156, p = 0.150$). These results indicate that, particularly in middle adulthood, the Arab female participants' acceptance of hotspot offers is closely intertwined with their trust in the persona, a trend not mirrored among their British counterparts.

As presented in Table 6, a significant correlation between acceptance of the offer and trust in personas is observed among male participants. Among early adult Arab males (N = 79), the correlations are notably moderate to strong (AM: Spearman's $\rho = 0.494$, AF: Spearman's $\rho = 0.602$, YM: Spearman's $\rho = 0.524$, and YF: Spearman's $\rho = 0.496$, all $p < 0.001$). Early adult British males (N = 50) displayed significant positive correlations as well, with Spearman's $\rho$ values of 0.476 for AM, 0.474 for AF, and 0.554 for YM and a notably higher Spearman's $\rho$ value of 0.545 for YF (all $p < 0.001$).

For males in middle adulthood, Arab participants demonstrated very strong positive correlations (AM: Spearman's $\rho = 0.617$, AF: Spearman's $\rho = 0.583$, YM: Spearman's $\rho = 0.620$, YF: Spearman's $\rho = 0.514$, all $p < 0.001$). Their British counterparts also showed significant positive correlations, though slightly lower (AM: Spearman's $\rho = 0.485$, AF: Spearman's $\rho = 0.459$, YM: Spearman's $\rho = 0.580$, YF: Spearman's $\rho = 0.490$, all $p < 0.001$).

## 5 Discussion

This research contributes a unique perspective to the existing literature by exploring the interplay between age and gender similarity among potential social engineers and their targets, focusing on its influence on trust and subsequent risk-taking in face-to-face interactions. While the interaction between gender-age matching and their influence on trust and decision-making has been thoroughly explored in fields such as education [38–40], medicine [41], and marketing [36, 37], its examination within the realm of cybersecurity remains limited. Addressing this gap, our study specifically investigates whether the demographic similarities between the potential manipulator and the target have an impact on the level of trust and risk-taking exhibited by the latter towards the manipulator.

The role of trust in SE attempts isn't just shaped by personal beliefs and assumptions, but also by wider cultural and societal factors. These broader influences can drive different security-related behaviors depending on the cultural context. According to Triandis (2001), the way people interpret and respond to their surroundings varies across cultures, with elements like social norms and collectivism impacting how risk tolerance is shaped [50], with factors such as social norms and collectivism influencing risk tolerance. Statman (2015) similarly highlights that cultural environments strongly affect how risks are perceived and handled [51]. By examining both Arab and UK participants, who show marked differences in the cultural dimension of individualism versus collectivism, this research digs into these cultural nuances and sheds light on how they might inform more tailored security approaches.

Given the limited research on gender-age similarity between manipulators and targets in the cybersecurity field, our approach draws parallels with related disciplines where the persuader's profile is known to affect the efficacy of their strategies. For instance, just as previous studies [36, 37] have shown that a salesperson's demographic matching with customers can influence sales outcomes, our findings indicate that a similar dynamic may exist in the field of cybersecurity, with the demographic variances between social engineers and targets could potentially affect the success of SE tactics.

*Trust and risk-taking dynamics for gender and age groups*. Our study revealed a consistent tendency to take risks and accept the hotspot offer from female personas across all participant groups from both Arab and UK samples. These observations align with the literature suggesting that women are perceived to possess lower cybersecurity awareness than men [52–54], potentially explaining their perceived higher trustworthiness and the higher risk of accepting the offer from women more than men. Additionally, these findings resonate with trends highlighted in the literature, where female teachers and physicians are often preferred for their nurturing demeanor rather than their male counterparts [39, 41]. This pattern is further explained through Social Role Theory [13], which posits that gender expectations influence behavior and perception. Women are often viewed as more nurturing and less harmful, and this perception carries over into trust dynamics in cybersecurity contexts, as seen in our study. Nonetheless, it is important to note that the perception of females and their effectiveness may vary depending on the context.

Regarding age matching groups, our study revealed a preference among Arab participants for personas based on age, with a higher acceptance rate for older personas compared to younger personas regardless of gender. This suggests that older individuals are perceived as more trustworthy and less likely to present a risk, likely due to their lower cybersecurity awareness compared to younger generations, as demonstrated in a previous study [55], thereby posing a lower risk of executing cyber-attacks. Interestingly, this age preference pattern was not as evident in the UK sample. In this context, early adult males and females exhibited a higher inclination for risk-taking with young male personas compared to aged male personas, though this difference was not statistically significant. This difference between Arab and British participants suggests that cultural factors can play a significant role in shaping preference for individuals of different ages. According to the Social Role Theory, society attributes different roles and expectations based on the age of the individual, and these roles are shaped by cultural norms about which behaviors are considered appropriate at different stages of life [13]. For instance, some cultures place greater respect and trust in elders, leading to a higher likelihood of accepting actions or advice from older individuals. Cross-cultural psychology research supports this, showing that in some cultures, respect for elders may prompt a higher rate of acceptance for actions by older individuals [11]. Furthermore, in contrast to the Arab sample, where no significant gender preference was found for older personas, British early adult males and females showed a greater tendency to accept offers from aged female personas over aged male ones. Trust, a critical component in SE attempts, is also shaped by cultural and societal norms [6], which may explain the trust pattern differences observed between UK and Arab participants.

*The correlation between acceptance and trust*. Our study revealed a general pattern where higher trust in personas were commonly associated with increased acceptance scores, a finding that corroborates previous research emphasizing the critical role of trust in the efficacy of deceptive tactics [56]. A heightened level of perceived trust may lower the user's sense of security risk, thus increasing their willingness to accept these risks. In our study, a positive correlation between acceptance and trust was consistently observed across three participant groups: early adult females, and males in both early and middle adulthood, across both datasets. Aligning with these observations, Li, Rong, and Thatcher [57] highlighted the significant effect of trust on making decisions like purchase intentions. Noting that while their investigation centered on technology trust, its implications might parallel those of interpersonal trust, especially in environments where technology mediates interactions. In an interesting departure from the established pattern, our study observed that British females in middle adulthood did not demonstrate a significant correlation between acceptance of the hotspot offer and trust in personas. British middle adulthood females showed a notably lower acceptance rate compared to the other three British demographic groups, a significant finding confirmed by ANOVA post-hoc comparisons, with results detailed in Tables 3S and 4S in the OSF supplementary material. This aligns with the understanding that trust, a complex construct developed over time [57], may not be a decisive factor in initial acceptance for British middle adulthood females. Furthermore, a conditional variance analysis performed following the identification of 15 bivariate outliers in the correlation suggests a minimal dependency of acceptance on trust for MA-F British participants, pointing to alternative influences on their acceptance decisions beyond trust. Insights from the UK's annual media literacy report reveal a "confidence gap" among middle-aged women, indicating lower confidence in their use of digital devices. This gap is not due to a lack of competence but rather life patterns, such as career breaks and caregiving roles, which reduce exposure to technology [58]. As a result, their lower acceptance decisions in the study may be driven by factors such as comfort or familiarity with digital environments, rather than trust. Details on the correlation analysis for British MA-F, and its comparison to EA-F, are available in Fig. 1S in the OSF supplementary material.

*Variations in significant trust and acceptance*. Our study observed significant scores on trust, but not acceptance, mostly among British female and Arab male participants. Both British female and Arab male participants were significantly more trusting of AF personas compared to younger females. Interestingly, this increased trust did not extend to significant risk-taking for accepting the offer. Trust is often based on the perceived qualities of integrity, competence, and warmth in individuals. According to the Stereotype Content Model proposed by Fiske et al., these attributes are frequently associated with older individuals [59], potentially leading to a heightened level of trust towards older adults. In contrast, acceptance decisions are typically pragmatic, influenced by how the participant perceives the offer's relevance, value, or urgency within their current context [60]. It is important to note that, in our scenario, if the internet is not deemed essential by the participants, the perceived urgency of the offer may decrease, resulting in reduced acceptance rates. This holds true irrespective of the level of trust inspired by the age or gender of the persona presenting the offer.

*The impact of demographic similarity on trust and risk-taking*. Previous studies have shown that people are more likely to trust others who share similar demographic characteristics [7]. Our investigation sought to determine the compound effect of age and gender similarity between personas representing possible manipulators and participants on the trust and risk-taking levels. The results, however, did not reveal a general trend of significant differences. For example, young male participants did not exhibit a significant preference for personas within their own gender and age bracket (YM), instead, they demonstrated heightened levels of risk-taking and trust towards AF personas. Nevertheless, our findings revealed that female personas exerted a notable influence on the risk-taking scores within the early adulthood participant group from both samples when the age category of the personas matched that of the participants. Specifically, within the young adult cohort of both samples, YF personas elicited higher risk-taking and risk perception scores compared to YM personas. Conversely, such a pattern was not observed in the older adult group; participants from the middle adulthood age category (Arab MA-M, MA-F, and British MA-M) did not show significant differences in their responses to AM or AF. This finding resonates with Sprecher et al.'s insights on mate preferences, which suggests diminishing gender preferences with increasing age [61]. It's important to note the parallels drawn here are not directly from cybersecurity contexts. Nonetheless, these parallels are invoked to highlight the relevance of such demographic influences on individual's trust and engagement with potential social engineers.

*Cultural variances in trust and risk-taking*. The findings from our research pointed to notable variations in how trust and risk-taking were expressed between participants Arab and British participants, emphasizing the role that cultural context plays in shaping these behaviors. These differences were particularly evident in how participants responded to the age of personas. Among British participants in early adulthood, there was a stronger tendency to trust and take risks with younger males over older ones, and similarly, with older women rather than older men. This behavior may reflect the UK's more individualistic cultural norms [62]. Research on trust within individualistic societies indicates that trust tends to be based more on personal characteristics and achievements rather than age or seniority [63, 64]. In contrast, Arab participants exhibited a clear preference for older personas, regardless of gender, when making trust and risk-taking decisions. This may be rooted in cultural values that emphasize respect and trust for elders, which is a common trait in many non-WEIRD cultures [64]. These culturally ingrained trust dynamics highlight the need for security strategies that consider the cultural expectations of different populations.

### 5.1 Implications

The interplay of gender and age-based preferences revealed in our study highlights the significance of tailoring security awareness programs that consider demographic heuristics and stereotypes. This suggests the need for debiasing strategies that specifically address the biases individuals may have based on superficial demographic factors of potential manipulators. Debiasing strategies are cognitive techniques designed to reduce the influence of biases, such as making decisions based on stereotypes, by increasing awareness and promoting critical thinking [65]. These strategies have been successful in other disciplines, such as education and healthcare. For example, in healthcare, debiasing strategies proven effective in reducing diagnostic errors include the application of enhanced medical knowledge, structured self-explanation, and guided reflection [66]. Similarly, in education, debiasing interventions such as empathy training for teachers have been employed to reduce biases and bolster student–teacher relationships [67]. These strategies suggest a promising avenue for cybersecurity: adopting similar educational and reflective practices could potentially mitigate stereotypes biases and improve defense mechanisms against SE attempts. By mitigating these biases, particularly in face-to-face interactions, we can help individuals make more informed decisions and reduce the risk of SE exploits that take advantage of these biases. However, we are uncertain whether this can be termed bias, and further research is needed to determine whether the cognitive process is possibly driven by more objective criteria based on facts, such as the prevalence of young males among hackers.

Our findings underscore the importance of adopting culturally sensitive interventions that target specific heuristics and stereotypes prevalent within different populations. For instance, in Arab cultures, where elder respect is highly valued, interventions addressing age-related biases may prove essential, whereas in more individualistic Western cultures, programs might need to focus on gender biases but with attention to specific age groups. Notably, British early adulthood participants demonstrated a tendency to trust and accept risk from aged females more than aged males, reflecting the nuanced interplay of age and gender in trustworthiness perceptions. Moreover, our study highlights the value of incorporating non-WEIRD samples in cybersecurity research. Additionally, incorporating non-WEIRD samples into cybersecurity research, as seen with our Arab participants, provides valuable insights into how security strategies should be adapted for non-Western contexts, where cultural norms heavily influence decision-making [68]. Supporting this, previous studies have demonstrated that culturally tailored security programs can significantly improve the effectiveness of awareness efforts. Amway, for instance, found that adjusting training to local cultures, languages, and learning styles greatly enhanced engagement and risk recognition [69]. Similarly, Brookfield Renewable showed that adapting content to incorporate regional events and cultural nuances increased participation and retention of security information [70]. These examples emphasize the need for customized security measures that reflect the diverse cultural contexts in which they are implemented, ensuring global applicability and effectiveness.

Our study's findings extend their implications to AI-driven metaverse environments. The metaverse is a collective virtual space that integrates elements of physical reality into a persistent virtual environment and is rapidly becoming a key environment for both professional and social settings [71]. In the metaverse, AI technologies are increasingly utilized to create hyper-realistic avatars and virtual agents that can replicate human behaviors and traits [72]. Given our results, malicious actors in metaverse settings could potentially exploit age and gender cues to craft avatars designed to elicit higher trust from their targets. Artificial Intelligence could assist in fine-tuning these avatars to mirror characteristics known to reduce perceived risk. This highlights the need for security measures to protect against SE threats within these virtual platforms.

Further exploration of our findings indicates that acceptance and trust should not be viewed as isolated factors in cybersecurity. The evidence of a similar pattern between these two measures suggests that an integrated framework is necessary for the development of security measures. By considering the interplay of cultural influences and human behavior, our study extends beyond traditional technical solutions, offering practical insights that align with the complexities of global cybersecurity challenges.

## 6 Limitations and future work

While our study has provided valuable insights into demographic influences on cybersecurity behavior, it has some limitations. One limitation is the potential social desirability due to self-reporting measures. This was addressed by ensuring anonymity of the collected data. Due to the exploratory nature of our study, it focused on demographic factors without considering communication styles, which previous research has shown to significantly affect outcomes, especially when combined with caring gestures [41]. Additionally, the lack of qualitative data leaves unanswered questions about the participants' reasons for trusting or preferring one persona over another. Future studies may benefit from incorporating qualitative methods, such as interviews, to explore these nuances.

Moreover, the influence of demographic similarities observed in our face-to-face scenario may extend to non-face-to-face interactions such as phishing or vishing. Future work could investigate whether phishing emails, online chat communications, or vishing calls that use personas or avatars presenting specific age or gender characteristics, could increase the target's susceptibility to these attacks. Research has already demonstrated how attackers use avatars or online personas to gain trust and manipulate their targets in phishing attacks. A study comparing text-only communication to avatar-supported interactions found that the presence of avatars significantly increased the perceived credibility and trustworthiness of the communicator, making users more susceptible to manipulation [73]. This suggests that attackers in phishing and vishing contexts could exploit these factors by using avatars or carefully crafted personas to increase their likelihood of success. Furthermore, understanding how cultural dimensions interact with demographic factors in non-face-to-face contexts could guide the development of more targeted cybersecurity interventions across different populations.

Subsequent studies could beneficially examine how individual differences, such as personality traits, impact their interaction with cybersecurity threats. Likewise, the level of technical expertise could moderate responses to cybersecurity challenges, with more knowledgeable individuals potentially better equipped to evaluate the credibility of risks and the safety of various cyber practices. It's important to note that our study's use of hypothetical scenarios may affect its ecological validity. However, we sought to mitigate this by applying pre-selection criteria, ensuring participants had familiarity with mobile hotspots and perceived at least minimal risk in using another person's hotspot. We also aimed to create a scenario that anyone could relate to and face-validating the personas for realism. While the study offers valuable insights from UK and Arab participants on trust and risk-taking, the results may not fully extend to other cultural or demographic groups. Future research involving a more diverse global population would help to better understand the broader applicability of these findings. To control for possible biases in our study, the order in which personas were presented to participants was randomized, ensuring that participants could not anticipate or recall any specific sequence. Future work should continue to balance experimental control with ecological validity to enhance the practical implications of the research findings.

As mentioned previously, the urgency and perceived value of accepting a hotspot offer to connect to the internet can greatly vary among individuals, reflecting different needs and circumstances in real-life scenarios. Future research should include varied contexts where the urgency to accept help is more pronounced, to assess how immediate demand influences trust and risk-taking behaviors. Moreover, although we did not find a strong influence of education level or socioeconomic status on trust and risk-taking behaviors across the persona age-gender RM factor, we believe these factors are still valuable to explore further. The analysis of these variables is available through the OSF link provided in the supplementary material section. It is possible that in other contexts, such as populations with varying levels of digital literacy or economic backgrounds, these factors might have a more significant impact. In addition, the exploration of these factors could yield more impactful findings in studies involving different types of risks, particularly those that are easier to recognize or more closely tied to professional expertise. Future research could investigate these variables more thoroughly, potentially using qualitative methods to better understand how different types of risks and personal backgrounds shape responses to cybersecurity risks.

## 7 Conclusion

In conclusion, this research contributes to the research of cybersecurity by analyzing how age and gender similarity between manipulators and targets influences trust and risk-taking behaviors. Although our findings did not show that similarities between these demographics had a substantial effect on trusting the potential manipulator, the combined influence of age and gender unearthed compelling patterns. These patterns highlight the importance of considering these demographics together rather than in isolation, as their combined influence, either from the perspective of the manipulator or the target, can enhance the effectiveness of persuasion employed in cybersecurity manipulation. The implications of our findings have far-reaching effects, promoting the need for a customized approach to cybersecurity awareness that takes into consideration individual and cultural biases, ultimately strengthening the defense against SE tactics. Future endeavors will delve into qualitative analyses to uncover the underlying motives and perceptions behind the demographic preferences observed.

**Acknowledgements** This research was made possible by an NPRP-14-Cluster Grant # NPRP 14C-0916-210015 from the Qatar National Research Fund (a member of Qatar Foundation). The findings herein reflect the work and are solely the responsibility of the authors. Open Access funding provided by the Qatar National Library.

**Author contributions** RA, MB, and KK designed and supervised the study and conceptualized the research. IA and RA prepared the study materials, collected, cleaned, and analyzed the data. SA and AY provided guidance on statistical analysis and verified its accuracy. AN helped the preparation of the study material and the data collection, cleaning and preparation. IA drafted the initial manuscript, and all authors critically reviewed and contributed feedback.

**Funding** Open Access funding provided by the Qatar National Library. Qatar National Research Fund, NPRP 14C-0916-210015, Qatar National Library, Open Access Fund.

**Data availability** The study design and dataset used in this study are available together with the supplementary material on the Open Science Framework at: https://osf.io/7nbgf/.

## Declarations

**Conflict of interest** The authors declare no competing interests.

## References

1. Middleton, B.: A history of cyber security attacks: 1980 to present. Auerbach Publications (2017). https://doi.org/10.1201/9781315155852
2. Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S., Lagerström, R.: Yet another cybersecurity risk assessment framework. Int. J. Inf. Secur. **22**(6), 1713–1729 (2023)
3. Lohani, S.: Social engineering: Hacking into humans. Int. J. Adv. Stud. Sci. Res. **4**, 1 (2019)
4. Sheng S., Holbrook M., Kumaraguru P., Cranor L.F., Downs J.: Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI conference on human factors in computing systems, 373–382 (2010)
5. Kipane, A.: Meaning of profiling of cybercriminals in the security context. SHS Web Conf. **68**, 01009 (2019). https://doi.org/10.1051/shsconf/20196801009
6. Singh, T.B.: A social interactions perspective on trust and its determinants. J. Trust Res. **2**(2), 107–135 (2012)
7. Clerke, A.S., Heerey, E.A.: The influence of similarity and mimicry on decisions to trust. Collabra. Psychology **7**, 05 (2021)
8. Abuelezz, I., Barhamgi, M., Nhlabatsi, A., Khan, K.M., Ali, R.: How demographic and appearance cues of a potential social engineer influence trust perception and risk-taking among targets. Inf. Comput. Secur. (2024). https://doi.org/10.1108/ICS-03-2024-0057
9. Henrich, J., Heine, S.J., Norenzayan, A.: Most people are not WEIRD. Nature **466**(7302), 29–29 (2010)
10. Greenfield, P.M.: Three approaches to the psychology of culture: Where do they come from? Where can they go? Asian J. Soc. Psychol. **3**(3), 223–240 (2000)
11. Hofstede G.: Culture's consequences: International differences in work-related values. Sage, (1984)
12. Harb C.: The Arab region: cultures, values, and identities. In: Handbook of Arab American psychology: Routledge, 3–18 (2015)
13. Eagly, A.H., Wood, W.: Social role theory. Handbook Theor. Soc. Psychol. **2**, 458–476 (2012)
14. Nosek, B.A., Banaji, M.R., Greenwald, A.G.: Harvesting implicit group attitudes and beliefs from a demonstration web site. Group Dyn. Theor. Res. Pract. **6**(1), 101 (2002)
15. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M.: Individual differences and information security awareness. Comput. Hum. Behav. **69**, 151–156 (2017)
16. Baki, S., Verma, R.M.: Sixteen years of phishing user studies: What have we learned? IEEE Trans. Depend. Secure Comput. **20**(2), 1200–1212 (2022)
17. Kircanski, K., et al.: Emotional arousal may increase susceptibility to fraud in older and younger adults. Psychol. Aging **33**(2), 325 (2018)
18. Sarno, D.M., Lewis, J.E., Bohil, C.J., Neider, M.B.: Which phish is on the hook? Phishing vulnerability for older versus younger adults. Hum. Factors **62**(5), 704–717 (2020)
19. Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D.: Factors that influence information security behavior: An Australian web-based study. In: Tryfonas, T., Askoxylakis, I. (eds.) Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings, pp. 231–241. Springer International Publishing, Cham (2015). https://doi.org/10.1007/978-3-319-20376-8_21
20. Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., Briggs, P.: Exploring age and gender differences in ICT cybersecurity behaviour. Human Behav. Emerg. Technol. **2022**, 1–10 (2022). https://doi.org/10.1155/2022/2693080
21. Moody, G.D., Galletta, D.F., Dunn, B.K.: Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. Eur. J. Inf. Syst. **26**, 564–584 (2017)
22. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A.: Correlating human traits and cyber security behavior intentions. Comput. Secur. **73**, 345–358 (2018)
23. Mohamed, N., Ahmad, I.H.: Information privacy concerns, antecedents and privacy measure use in social networking sites: evidence from Malaysia. Comput. Hum. Behav. **28**(6), 2366–2375 (2012)
24. Hoy, M.G., Milne, G.: Gender differences in privacy-related measures for young adult Facebook users. J. Interact. Advert. **10**(2), 28–45 (2010)
25. Lin, T., et al.: Susceptibility to spear-phishing emails: effects of internet user demographics and email content. ACM Trans. Comput.-Human Interact. (TOCHI) **26**(5), 1–28 (2019)
26. Warrington, C., Syed, J., Tappin, R.M.: Personality and employees' information security behavior among generational cohorts. Comput. Inf. Sci. **14**(1), 1–44 (2021)
27. Rocha Flores, W., Holm, H., Nohlberg, M., Ekstedt, M.: Investigating personal determinants of phishing and the effect of national culture. Inf. Comput. Secur. **23**, 178–199 (2015)
28. Al-Hamar M., Dawson R., Guan L.: A culture of trust threatens security and privacy in Qatar. In: 2010 10th IEEE international conference on computer and information technology, IEEE, 991–995 (2010)
29. Li, H., Sarathy, R., Xu, H.: The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decis. Support. Syst. **51**(3), 434–445 (2011)
30. Thatcher, J.B., McKnight, D.H., Baker, E.W., Arsal, R.E., Roberts, N.H.: The role of trust in postadoption IT exploration: an empirical examination of knowledge management systems. IEEE Trans. Eng. Manage. **58**(1), 56–70 (2010)
31. Workman, M.: Gaining access with social engineering: an empirical study of the threat. Inf. Syst. Secur. **16**(6), 315–331 (2007)
32. Colquitt, J.A., Scott, B.A., LePine, J.A.: Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. J. Appl. Psychol. **92**(4), 909 (2007)
33. Mayer, R.C., Davis, J.H., David Schoorman, F.: An integrative model of organizational trust. Acad. Manag. Rev. **20**(3), 709 (1995). https://doi.org/10.2307/258792
34. Gefen, D.: E-commerce: the role of familiarity and trust. Omega **28**(6), 725–737 (2000)

35. Jarvenpaa, S.L., Tractinsky, N., Saarinen, L.: Consumer trust in an Internet store: a cross-cultural validation. J. Comput.-Med. Commun. **5**(2), 0–0 (2006). https://doi.org/10.1111/j.1083-6101.1999.tb00337.x
36. Stros, M., Říha, D., Möslein-Tröppner, B.: The role of gender in salesperson perception. Mark. Sci. Inspir. **13**, 3 (2018)
37. Dwyer, S., Richard, O., Shepherd, C.D.: An exploratory study of gender and age matching in the salesperson-prospective customer dyad: testing similarity-performance predictions. J. Pers. Selling Sales Manag. **18**(4), 55–69 (1998)
38. Lim, J., Meer, J.: Persistent effects of teacher–student gender matches. J Human Res **55**(3), 809–835 (2020)
39. Hwang, N., Fitzpatrick, B.: Student–teacher gender matching and academic achievement. AERA Open **7**, 23328584211040056 (2021)
40. Egalite, A.J., Kisida, B.: The effects of teacher match on students' academic perceptions and attitudes. Educ. Eval. Policy Anal. **40**(1), 59–81 (2018)
41. Mast, M.S., Hall, J.A., Roter, D.L.: Disentangling physician sex and physician communication style: their effects on patient satisfaction in a virtual medical visit. Patient Educ. Couns. **68**(1), 16–22 (2007)
42. FaceApp: Face Editor. https://www.faceapp.com/. Accessed 13 Mar 2024.
43. Thien Phung: MOBILE Panel Sample and ONLINE Surveys TGM Research. TGM Research, https://tgmresearch.com/. Accessed 16 Mar 2024
44. House R.J., Hanges P.J., Javidan M., Dorfman P.W., Gupta V.: Culture, leadership, and organizations: the GLOBE study of 62 societies. Sage publications, (2004)
45. Waclawski, E.: How i use it: survey monkey. Occup. Med. **62**(6), 477–477 (2012)
46. JASP: A fresh way to do statistics. JASP—Free and User-Friendly Statistical Software, https://jasp-stats.org/. Accessed 16 Mar 2024
47. Stages of Human Development Psychology: Child Developmental Theories. Hello Doctor, 5 June 2020, https://hellodoctor.com.ph/parenting/stages-of-human-development-psychology/.
48. Li, S.-C., Lindenberger, U., Hommel, B., Aschersleben, G., Prinz, W., Baltes, P.B.: Transformations in the couplings among intellectual abilities and constituent cognitive processes across the life span. Psychol. Sci. **15**(3), 155–163 (2004)
49. Blanca Mena, M.J., Alarcón Postigo, R., Arnau Gras, J., Bono Cabré, R., Bendayan, R.: Non-normal data: Is ANOVA still a valid option? Psicothema **29**, 552–557 (2017)
50. Triandis, H.C.: Individualism-collectivism and personality. J. Pers. **69**(6), 907–924 (2001)
51. Statman, M.: Culture in risk, regret, maximization, social trust, and life satisfaction. J. Invest. Consult. **16**(1), 20–30 (2015)
52. Broos, A.: Gender and information and communication technologies (ICT) anxiety: male self-assurance and female hesitation. Cyberpsychol. Behav. **8**(1), 21–31 (2005)
53. He, J., Freeman, L.A.: Are men more technology-oriented than women? The role of gender on the development of general computer self-efficacy of college students. J. Inf. Syst. Educ. **21**(2), 203–212 (2010)
54. Venkatesh, V., Morris, M.G.: Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. MIS Q. **24**(1), 115 (2000). https://doi.org/10.2307/3250981
55. Daengsi, T., Pornpongtechavanich, P., Wuttidittachotti, P.: Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks. Edu Inf Technol (2022). https://doi.org/10.1007/s10639-021-10806-7
56. Albladi, S.M., Weir, G.R.: Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity **3**(1), 1–19 (2020)
57. Li, X., Rong, G., Thatcher, J.B.: Does technology trust substitute interpersonal trust? Examining technology trust's influence on individual decision-making. J. Organ. End User Comput. (JOEUC) **24**(2), 18–38 (2012)
58. Adults' Media Use and Attitudes. Ofcom, 18 Apr 2024, https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes.
59. Cuddy, A.J., Fiske, S.T., Glick, P.: Warmth and competence as universal dimensions of social perception: the stereotype content model and the BIAS map. Adv. Exp. Soc. Psychol. **40**, 61–149 (2008)
60. Authorities C.M.: Evidence review of online choice architecture and consumer and competition HarmUK government. https://www.gov.uk/government/publications/online-choice (2022)
61. Sprecher, S., Econie, A., Treger, S.: Mate preferences in emerging adulthood and beyond: age variations in mate preferences and beliefs about change in mate preferences. J. Soc. Pers. Relat. **36**(10), 3139–3158 (2019)
62. Hofstede's Six Cultural Dimensions—and Why They Matter. Verywell Mind, https://www.verywellmind.com/hofstedes-cultural-dimensions-8583990. Accessed 2 Sept 2024
63. Zeffane, R.: Gender, individualism–collectivism and individuals' propensity to trust: a comparative exploratory study. J. Manag. Organ. **26**(4), 445–459 (2020)
64. Cultural Perspectives on Aging: How the Experience of Aging Differs Around the World » Online Graduate Programs in Innovative Aging Studies » College of Medicine » University of Florida
65. Larrick, R.P.: Debiasing. In: Koehler, D.J., Harvey, N. (eds.) Blackwell handbook of judgment and decision making, pp. 316–338. Wiley (2004). https://doi.org/10.1002/9780470752937.ch16
66. Griffith, P.B., Doherty, C., Smeltzer, S.C., Mariani, B.: Education initiatives in cognitive debiasing to improve diagnostic accuracy in student providers: a scoping review. J. Am. Assoc. Nurse Pract. **33**(11), 862–871 (2021)
67. Four Ways Teachers Can Reduce Implicit Bias. Greater Good, https://greatergood.berkeley.edu/article/item/four_ways_teachers_can_reduce_implicit_bias. Accessed 13 Mar 2024
68. Alnunu, M., Amin, A., Abu-Rayya, H.M.: The susceptibility to Persuasion strategies among Arab Muslims: the role of culture and acculturation. Front. Psychol. **12**, 574115 (2021)
69. Implementing Global Security Awareness Programs: Collaboration and Cultural Relevance|Infosec. https://www.infosecinstitute.com/resources/industry-insights/implementing-global-security-awareness-programs-collaboration-cultural-relevance/. Accessed 5 Oct 2024
70. Assenza, G., Chittaro, A., De Maggio, M.C., Mastrapasqua, M., Setola, R.: A review of methods for evaluating security awareness initiatives. Eur. J. Security Res. **5**, 259–287 (2020)
71. Dionisio, J.D.N., Iii, W.G.B., Gilbert, R.: 3D virtual worlds and the metaverse: current status and future possibilities. ACM Comput. Surveys (CSUR) **45**(3), 1–38 (2013)
72. Chamola, V., et al.: A comprehensive survey on generative AI for metaverse: enabling immersive experience. Cognitive Comput. **16**(6), 3286–3315 (2024)
73. Galanxhi, H., Nah, F.F.-H.: Deception in cyberspace: a comparison of text-only versus avatar-supported medium. Int. J. Hum. Comput. Stud. **65**(9), 770–783 (2007)

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.