International Journal of Safety and Security Engineering
Vol. 14, No. 2, April, 2024, pp. 487-498
Journal homepage: http://iieta.org/journals/ijsse

The Impact of Call Spoofing on Trust and Communication: A User Perception Study

Amitabh Verma

Business Department, Sohar University, Sohar 311, Oman

Corresponding Author Email: vermainfo123@gmail.com

Copyright: ©2024 The author. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.140216

Received: 5 December 2023
Revised: 26 January 2024
Accepted: 31 January 2024
Available online: 26 April 2024

Keywords:
call spoofing, communication security, user perceptions, knowledge, trust, demographic variations

ABSTRACT

This study explores the complex field of phone spoofing in the context of India's digital revolution, examining how people react to and perceive dishonest communication techniques. The study examines the interconnected dynamics of Knowledge of Call Spoofing, Perceived Threat, and Trust in Phone Communication, with a focus on the Indian context, where traditional values collide with rapid technological advancements. This study employs a mixed-methods approach, integrating both qualitative and quantitative data. Quantitative data is gathered through a structured survey questionnaire distributed to a demographically diverse sample, and qualitative insights are obtained through in-depth interviews and focus groups. The results show a strong and positive correlation between call spoofing knowledge and phone communication trust, indicating that knowledgeable users are more likely to have confidence in their phone interactions. These views are further shaped by demographic subtleties, which include differences in gender, age, education, and occupation. The results offer a basis for developing proactive and culturally aware approaches to boost user confidence, guaranteeing a safe and robust digital communication environment catered to the various demands of the enormous Indian populace. In addition to that, this research has real-world consequences for educators, technology companies, and governments who are involved in determining India's digital future.

1. INTRODUCTION

The communication landscape has changed recently in India due to the country's rapid digitization and extensive usage of mobile phones, providing unmatched connections. But amid the ease of seamless communication, a growing worry has surfaced: call spoofing is a constant menace. In the Indian context, call spoofing-the dishonest practice of falsifying caller ID information. Song et al. [1] poses a serious threat to the security and confidence of phone communication.

The incidence of call spoofing events has increased sharply as smartphone usage and internet connectivity in India sees an unparalleled upsurge. In addition to calling into question users' susceptibility, this problem also begs investigation into the complex factors that influence people's feelings of trust in phone communication [2]. Sustaining confidence in phone communication is essential for personal, professional, and financial relationships in India, where mobile phones have become an indispensable component of everyday life. Call spoofing undermines the conventional trust that consumers have in caller identification systems by introducing a degree of doubt [3].

In the context of India, this study aims to investigate the complex effects of call spoofing on user confidence in phone communication. In particular, the study looks at how people view this increasing threat and investigates whether or not call spoofing information is correlated with trust [4]. Furthermore, considering the heterogeneous demographic makeup of India, the study aims to detect differences in user opinions among various demographic subgroups.

It's critical to comprehend how users view call spoofing for several reasons. First of all, it clarifies how well people are being informed about this issue by existing awareness campaigns and educational initiatives. Second, investigating the relationship between trust and knowledge sheds light on the psychological effects of call spoofing on user behavior [5]. Last but not least, recognizing demographic variances enables treatments and countermeasures to be tailored to certain user groups, addressing the particular difficulties encountered by various Indian population segments [6].

2. THEORETICAL BACKGROUND

In light of the growing concern over dishonest activities in the telecommunications industry, research on call spoofing and its effects on user trust in phone communication has gained significance in recent years [7]. Numerous investigations have explored the technological nuances of phone spoofing, providing insight into the changing strategies used by spoofers and the countermeasures intended to stop them [8]. These pieces not only analyze spoofers' techniques but also show how these practices change throughout time. Recent statistics highlight the alarming prevalence of call spoofing in India. According to a report by the Telecom Regulatory Authority of India (TRAI), there has been a

noticeable rise in the number of complaints regarding call spoofing and related fraudulent activities over the past few years. TRAI's data indicate that call spoofing incidents have increased by over 25% annually, underscoring a growing trend in telecommunication fraud (Telecom Regulatory Authority of India, 2022). Moreover, a study conducted by the Indian Computer Emergency Response Team (CERT-In) revealed that in 2021 alone, there was a 30% increase in cybercrimes related to call spoofing, compared to the previous year (Indian Computer Emergency Response Team, 2021). This upsurge is particularly concerning given India's extensive mobile phone user base, which exceeds 900 million subscribers, as reported by the Ministry of Electronics and Information Technology. An application of voice biometric, namely voice recognition or speaker recognition refers to the process of recognizing the person who is speaking [9]. This study adds a significant understanding of the variables influencing user trust by taking familiarity, prior experiences, and perceived dependability into account. The rising trend of call spoofing in India is further corroborated by data from cybersecurity firms operating in the region. For instance, a report by Kaspersky Labs indicated that India ranked among the top five countries globally for the highest number of detected call spoofing and phishing attempts, suggesting a widespread and growing problem. An intricate study of the psychological effects of dishonest activities on user behavior is made possible by this interdisciplinary approach [10]. These investigations seek to offer a thorough grasp of the complex effects of phone spoofing. Although stronger security measures are increasingly developed, promoted and deployed, the number of security breaches is still increasing [11]. Deep fakes-artificial but hyper-realistic video, audio, and images created by algorithms-are one of the latest technological developments in artificial intelligence. Amplified by the speed and scope of social media, they can quickly reach millions of people and result in a wide range of marketplace deceptions. However, extant understandings of deepfakes' implications in the marketplace are limited and fragmented [12]. Social engineering relies heavily on human interaction and often involves using psychological tricks aimed at making victims agree to things they would not have done normally. By exploiting humans' limited security knowledge or awareness, phishers deceive online users into disclosing their sensitive information [13]. Attackers use enhanced gadgets to record users' voices, replay them for the ASV system, and be granted access for harmful purposes [14]. Automatic speaker verification (ASV) systems are susceptible to malicious attacks. It discredit the performance of a standard ASV system by increasing its false acceptance rates [15]. Despite a growing momentum to develop spoofing countermeasures for automatic speaker verification, now that the technology has matured sufficiently to support mass deployment in an array of diverse applications, greater effort will be needed in the future to ensure adequate protection against spoofing [16]. The Telecom Regulatory Authority of India (TRAI) has established guidelines and regulations aimed at curbing unsolicited commercial communications, which often involve call spoofing. These regulations mandate telemarketers to register and adhere to specific norms, including the use of pre-registered caller IDs. Efforts have been made to implement caller ID authentication protocols. These protocols, such as STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted Information Using to KENs), are designed to validate and certify the authenticity of caller IDs, making it difficult for spoofers to mask their real numbers. Law enforcement agencies have established cyber cells that deal with digital fraud, including call spoofing. Reporting mechanisms via helplines and online portals have been set up for victims to report spoofing incidents.

While regulatory frameworks exist, their implementation can be challenging due to the vast and complex telecommunications network in India. Monitoring and enforcement can be inconsistent across different regions. Spoofers often use advanced technologies and tactics to bypass existing safeguards, making some measures less effective. The continuous evolution of spoofing techniques poses a significant challenge. The effectiveness of awareness campaigns varies. In some cases, lack of widespread reach and continuous public engagement limits their impact, especially in rural or less digitally literate populations. While there is collaboration between the government and telecom providers, gaps can exist in information sharing, technological upgrades, and coordinated action against call spoofing. The literature on call spoofing and related topics is extensive, as this review of the literature indicates. Existing measures against call spoofing in India and their effectiveness provides a critical baseline for this study. It allows for a comprehensive understanding of the current landscape and helps in identifying the gaps that this research address, thereby contributing valuable insights for enhancing anti-spoofing strategies. This customized empirical study investigates demographic differences in call spoofing user perceptions, knowledge, and trust. By offering a complex and context-specific explanation of the effect of call spoofing on user trust in phone conversations, the proposed research seeks to close this knowledge gap.

3. RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

3.1 Research model

With an emphasis on the Indian context, this study offers a thorough research model intended to clarify the complex dynamics underlying users' views of how call spoofing affects their confidence in phone conversations [17]. The independent variable "Knowledge of Call Spoofing (K)," which measures users' awareness and comprehension of the dishonest activity, is the fundamental component of our model. We propose that there is a negative connection (H1) between this information and "Trust in Phone Communication (T)," meaning that users' trust in phone communication is likely to decline as they become more aware of call spoofing. Our model acknowledges the need for a more nuanced understanding and adds a mediating variable called "Perceived Threat (PT)" to capture users' subjective perceptions of call spoofing as a security and privacy risk [18]. The second hypothesis (H2) of this study is based on the hypothesis that PT mediates the beneficial effect of knowledge on trust. In addition, the present study used demographic variables, including Age, Gender, Education, and Occupation, as moderating factors (H3) to investigate how these attributes impact the associations among knowledge, perceived danger, and trust. With the use of this structured model, the study hopes to shed light on the intricate interactions that exist between perceived threat, trust, and user knowledge. It also hopes to offer a comprehensive viewpoint

that is suited to the various demographic groups that make up the Indian populace. This study aims to clarify the complex aspects of users' experiences with call spoofing by empirical analysis and statistical modeling, providing insightful recommendations for legislation, public awareness initiatives, and technology advancements in the Indian telecom sector [19].

3.2 Knowledge of call spoofing

As a crucial independent variable in this study, "Knowledge of Call Spoofing" is essential to comprehending users' awareness and understanding of call spoofing, a dishonest activity that compromises the accuracy of caller identification [20]. This variable captures the degree to which people are aware of the methods that bad actors use to spoof caller ID information so they can hide who they are. The purpose of this study is to determine how much consumers know about call spoofing and investigate whether higher awareness is associated with a measurable decline in phone communication trust. Researchers want to investigate the possible adverse effect of informed awareness on consumers' trust in the legitimacy of incoming calls [21] by using Knowledge of Call Spoofing (K) as an independent variable. This variable captures the basic knowledge that consumers have about call spoofing, which paves the way for investigating the effects of call spoofing on trust levels and developing effective countermeasures and awareness campaigns as a result.

An important component of this study examines the relationship between "Knowledge of Call Spoofing (K)" and "Trust in Phone Communication (T)," i.e., how consumers' understanding of call spoofing affects their confidence in the veracity of phone conversation [22]. It is anticipated that as customers become more aware of call spoofing and its deceptive tactics, their confidence in phone conversations will decline. This predicted negative association implies that a knowledgeable user who is aware of the possibility of criminal intent and caller ID manipulation may become more wary or circumspect when answering incoming calls [23]. User perception and trust impacts that how users perceive the risks associated with call spoofing and the degree of trust they place in telephonic communications in the face of potential security threats. The reliance on caller ID as a trust factor is problematic in the context of spoofing and suggest that users need to be educated about these vulnerabilities [4]. Individuals who possess a thorough understanding of the techniques utilized by spoofers can become more cognizant of the dangers involved, which could ultimately result in a reduction in their general confidence in the data transmitted over the telephone [24]. Knowledge of telecommunication fraud significantly diminish user trust, recommending enhanced security measures to mitigate this effect [3]. Psychological aspects that make individuals vulnerable to social engineering in telephony, including call spoofing. Factors like authority bias and urgency as key elements exploited by attackers and suggests integrating psychological awareness into user education programs [13]. The findings [7] that how users perceive caller ID authentication technologies and their impact on overall trust in mobile security reveal that while such technologies are welcomed, there is still skepticism about their effectiveness in preventing spoofing attacks. Digital literacy also influences user trust and ability to navigate telecommunication security risks, including call spoofing. It enhances users' ability to identify and respond to security threats effectively [25]. Understanding the complex interactions between knowledge and trust in the context of call spoofing requires an examination of this relationship, which will also provide insights into user behavior, risk perception, and the wider ramifications for communication practices in the digital age [26].

Hypotheses 1 (H1): There is a significant positive relationship between Knowledge of Call Spoofing and Trust in Phone Communication.

3.3 Perceived threat

According to the hypothesis, "Perceived Threat mediates the relationship between Knowledge of Call Spoofing (K) and Trust in Phone Communication," users go through a psychological process when they learn about phone spoofing. Users are likely to experience a heightened perception of threat (PT) about call spoofing tactics as their understanding of these fraudulent practices grows (K) [27]. Users assess the dependability of phone conversation via this lens of perceived threat. The mediated relationship implies that users' subjective perceptions of the possible threats provided by call spoofing are deeply entwined with the influence of knowledge on trust, rather than being purely direct [28]. In real life, individuals who are aware of phone spoofing may be wary of incoming calls because they perceive a threat due to their comprehension of possible manipulation [29]. As a result, their general trust in phone communication is impacted by this perceived danger. About call spoofing, the mediation process provides a detailed insight into the psychological dynamics at work, emphasizing the significance of perceived threat in influencing the link between knowledge and trust [13]. This mediation model is essential to understanding how users negotiate the trust environment in a time when call spoofing is a danger to the veracity of phone conversations. The study intends to provide important insights into user behavior, risk perception, and the wider implications for promoting trust in phone communication despite the difficulties presented by dishonest activities such as call spoofing by dissecting the complexities of these relationships.

Hypotheses 2 (H2): Perceived Threat mediates the relationship between Knowledge of Call Spoofing and Trust in Phone Communication.

3.4 Moderating variables

This research adds a layer of complexity and richness to our knowledge of how consumers manage the complicated landscape of call spoofing, perceived threat, and trust in phone communication by incorporating demographic characteristics as moderators. A more detailed analysis of the subtle ways in which age, gender, education, and occupation may influence people's reactions to call spoofing knowledge is made possible by acknowledging the variability inherent [30] in these characteristics. According to the study, age-related variances in generational familiarity with technology may have an impact on one's level of understanding regarding call spoofing. Younger people, who are frequently more accustomed to modern technologies, might interact between knowledge and trust differently than older people do [31]. Contrarily, gender dynamics raise the prospect of different call spoofing experiences and perceptions, which may have varying effects

on trust levels. It is anticipated that educational backgrounds will have a significant impact on how people perceive and evaluate the risks connected to call spoofing [32]. A more comprehensive knowledge of technology risks may be fostered by higher education, which could influence the perceived threat mediation process. Additionally, the occupation-specific lens recognizes that experts in particular professions could face particular difficulties and display particular trust dynamics during phone conversations, indicating the possible impact of occupational context [33]. Through the incorporation of demographic variables into the study's hypotheses, the research aims to reveal not only general patterns but also subtle differences in how various demographic groups deal with call spoofing. In light of the difficulties presented by call spoofing, this method recognizes the diversity within the study population and seeks to capture the various ways in which people, depending on their demographic traits, may understand, react to, and trust phone conversations [34]. As the research progresses, it aims to provide focused insights that can guide customized actions and tactics, promoting a more robust and trustworthy phone communication environment across various demographic groups.

Hypothesis 3 (H3): Demographic Variables Age, Gender, Education, and Occupation moderate the relationship between Knowledge of Call Spoofing, Perceived Threat, and Trust in Phone Communication.

4. RESEARCH METHODOLOGY

4.1 Research design

With an emphasis on the moderating effects of demographic characteristics and the mediating effect of perceived threat, the technique used for this study seeks to provide a thorough knowledge of how consumers perceive the impact of call spoofing on their trust in phone communication. A mixed-methods design has been selected as the comprehensive research technique [35] for this study to investigate the complex links among users' perceptions of threat, awareness of call spoofing, trust in phone communication, and the moderating influence of demographic characteristics [36]. This comprehensive strategy combines qualitative and quantitative methodologies to obtain a detailed insight into user experiences within the Indian environment [37]. The qualitative and quantitative methods in our study complement each other in a way that allows for a more comprehensive understanding of the issue at hand. The quantitative data gives us the breadth of information, reaching a wide range of participants to understand the general perception of call spoofing. The qualitative data, meanwhile, adds depth to these findings, exploring the 'why' behind the trends observed in the quantitative phase. This combination enables us to not only quantify the extent of the issue but also to understand the underlying reasons, motivations, and attitudes. In this study research design follows a sequential explanatory strategy, where quantitative data collection and analysis are followed by qualitative data collection and analysis. This approach is particularly beneficial in this context as it allows the findings from the quantitative phase to guide and inform the focus of the qualitative phase. It helps in exploring and interpreting the quantitative results in greater depth, thereby providing a more nuanced understanding of the research questions. Although this approach has certain limitations and potential biases. Mixed-methods research can be more complex and resource-intensive than single-method studies. Balancing qualitative and quantitative data collection, analysis, and integration requires considerable time and resources. In qualitative aspects of mixed-methods research, the researcher's perspectives or preconceptions can influence data collection and interpretation. This subjectivity can skew the findings, particularly in interviews and focus group. Researcher implemented systematic approaches for data analysis, especially in qualitative research, which can mitigate interpretation biases and add rigor and transparency to the process.

In the quantitative phase, a standardized survey questionnaire is given to a sample of participants that is representative of different demographic groups. Quantitative data on users' perceptions of threats, trust in phone communication, understanding of call spoofing, and demographics can be gathered using this method [38]. To guarantee the authenticity and dependability of the data gathered, the survey instrument will contain validated scales [39]. To evaluate the proposed hypotheses and determine how important factors interact, in-depth statistical studies such as regression, mediation, and moderation analyses will be used.

In-depth interviews and focus groups are used by the qualitative component to supplement the quantitative phase by delving further into the subjective experiences and perceptions of the participants. To guarantee variation in demographic features and enable a thorough examination of individual viewpoints, purposeful sampling will be used [40]. An open and exploratory discourse will be facilitated via semi-structured interview protocols and thoughtfully planned focus group discussions [41], capturing the nuances of how users navigate trust in phone contact amidst the difficulties presented by call spoofing. The application of thematic analysis to qualitative data will enhance the quantitative results and offer a more profound comprehension of the participants' lived experiences.

4.2 Measurement items

The survey instrument was initially composed of two parts and written in English. Component A, the initial step, was to collect respondents' data, such as their gender, age, education, and occupation. Component B of the questionnaire was the next piece that measured respondents' perceptions. The Likert scale, which has five points-1 for strongly disagreeing and 5 for strongly agreeing-was examined by the constructs [42]. Three telecommunications industry professionals were consulted to verify the face validity of the scale, and their assessments of the measurement's suitability were solicited using a questionnaire (Table 1). Additionally, a pilot study was conducted to verify the utility and comprehensibility of the questionnaire.

4.3 Research sample

As a thorough overview, the demographic profile Table 2 provides insightful information about the makeup of the population that was surveyed. The data displayed here, which describes the sample characteristics for a study including 680 participants, offers helpful information about the demographic and experience makeup of the research subjects [43]. The

profile provides systematic details on gender, age, education, and occupation using percentages and frequencies. This allows for a more nuanced assessment of the individuals' varied traits. According to the gender distribution, 67.06% of the respondents are men, suggesting that men make up the majority of the sample. The remaining 32.94% of the population is female. An overview of the gender representation in the study is given by this breakdown. The age distribution of the participants shows a wide range of ages and life stages. Remarkably, 32.06% of the sample's participants are in the 35-44 age range, representing the majority. Other noteworthy age groups are 25-34 years old (17.65%) and 45-55 years old (27.06%). This comprehensive analysis facilitates comprehension of the age distribution within the sample. Respondents are categorized in the educational background section according to their academic accomplishments. A significant percentage (40.29%) have a Bachelor's degree, whereas others have a High School Diploma (16.18%), a Diploma (24.71%), or a Master's degree or above (18.82%). The distribution reveals the range of educational backgrounds in the sample. Occupational roles shed light on the respondents' professional environments. At 44.41%, workers make up the largest category, followed by officers at 31.03%. The percentages of managers and supervisors are 11.47% and 13.09%, respectively. The distribution of occupations within the population polled is shown by this breakdown. This detailed summary provided by the demographic profile table enables readers and researchers to understand the wide range of participant characteristics. Understanding gender representation, age diversity, educational backgrounds, and occupational positions in greater detail is made possible by the frequencies and percentages, which also support a more nuanced interpretation of study findings within the given demographic context.

Table 1. Measurement items

Item No.	Measurement Items	References
1	**Knowledge of Call Spoofing (K)**	
1.1	K1.1: How much do you know about popular call spoofing tactics like speech distortion or tampering with caller ID information?	[4, 44, 45]
1.2	K1.2: How well aware are you of the possible dangers of call spoofing, such as the compromise of your privacy and personal information?	
1.3	K1.3: How certain are you that you can tell when a call is probably being spoofed? Please rate your capacity to spot call spoofing indicators during phone calls.	
2	**Perceived Threat (PT)**	
2.1	PT2.1: How much worry do you have about call spoofing operations violating your privacy? Please rank how concerned you are about privacy.	[46, 47]
2.2	PT2.2: To what extent do you consider call spoofing to be a security risk, including worries about possible fraud or illegal access to private data?	
2.3	PT2.3: How much, in your opinion, does call spoofing affect your level of confidence in the security and veracity of phone conversations? Kindly share your evaluation with me."	
3	**Trust in Phone Communication (T)**	
3.1	T3.1: In light of call spoofing, how much faith do you have in the accuracy of caller ID information presented during phone calls? Kindly rank your level of confidence.	[22, 48, 49]
3.2	T3.2: How much do you feel secure that your phone conversations are secure overall, considering the potential weaknesses caused by call spoofing?	
3.3	T3.3: Given a range of characteristics such as communication security and caller ID dependability, kindly rate your overall level of trust in phone communication.	

Table 2. Sample characteristics

Demographic Profile	Categories	Frequencies (N=680)	Percentage (%)
Gender	Male	456	67.06
	Female	224	32.94
Age	18-24 years	75	11.03
	25-34 years	120	17.65
	35-44 years	218	32.06
	45-55 years	184	27.06
	55 years and above	83	12.21
Education	High School Diploma	110	16.18
	Diploma	168	24.71
	Bachelor	274	40.29
	Master and above	128	18.82
Occupation	Manager	78	11.47
	Supervisor	89	13.09
	Officer	211	31.03
	Worker	302	44.41

5. DATA ANALYSIS AND RESULT

Advanced statistical methods are applied in this study's data analysis methodology, specifically the Heterotrait-Monotrait (HTMT) ratio and Partial Least Squares Structural Equation Modeling (PLS-SEM) [50]. To investigate the intricate links between the constructs of Perceived Threat (PT), Knowledge of Call Spoofing (K), and Trust in Phone Communication (T), PLS-SEM will be utilized. Because it allows for the consideration of latent variables and allows for the

simultaneous investigation of structural and measurement models, PLS-SEM is a good fit for this research [51]. This method makes it possible to thoroughly examine how Perceived Threats and Trust in Phone Communication are affected by Knowledge of Call Spoofing. Furthermore, to evaluate discriminant validity and make sure that the constructs in the model are different and do not measure the same underlying notion, the Heterotrait-Monotrait ratio of correlations will be employed [52]. By combining the advantages of HTMT for validity assessment and PLS-SEM for structural modeling, this multifaceted data analysis approach offers a thorough and reliable investigation of the relationships within the conceptual framework.

In the particular setting of this research on call spoofing and its effect on communication trust, bootstrap resampling becomes an essential technique for enhancing the statistical soundness of your results. Because of the intricacy of PLS-SEM and the possibility of multiple relevant elements [53] in this research dataset, bootstrap resampling provides a means of evaluating the robustness and stability of the predicted connections. Because bootstrap resampling produces several resampled datasets that closely resemble the original sample, it is very useful when working with small sample sizes [54]. This procedure offers a more thorough grasp of the distribution of model parameters while also assisting in mitigating the inherent variability in smaller datasets. Additionally, the process of bootstrap resampling facilitates the identification of possible outliers or significant examples that may have an outsized influence on the model estimations. By drawing random samples (6000 and 7000 samples, respectively) frequently with replacement, the method helps to estimate the model's parameters more reliably and accounts for the unpredictability brought by these circumstances. Bootstrap resampling stands out as a non-parametric method in PLS-SEM, where assumptions about the underlying distribution do not always hold [55]. This feature guarantees that the statistical conclusions obtained from the model are reliable and independent of particular distributional assumptions, which is in line with the flexibility needed in structural equation modeling.

The study strengthens the validity of its findings by employing bootstrap resampling. A more sophisticated understanding of the uncertainties surrounding the correlations between Knowledge of Call Spoofing, Perceived Threat, and Trust in Phone Communication is offered by the distribution of parameter estimates that are produced as well as the resultant confidence intervals. In the end, this method helps to produce a more thorough and trustworthy evaluation of the study model, strengthening the research findings and expanding their applicability.

Table 3 provides a thorough analysis of the measurement features for the Knowledge of Call Spoofing (K), Perceived Threat (PT), and Trust in Phone Communication (T) constructs in your structural model. The degree to which the Knowledge of Call Spoofing (K) loading values for K1.1, K1.2, and K1.3 are related to the latent construct is indicated. Interestingly, K1.2 has the highest loading (0.784), suggesting that it plays a significant role in assessing call spoofing knowledge. The responses' central tendency and variability are shown by the mean (5.421) and standard deviation (1.234) for this construct. Excessive values of AVE (0.576), CR (0.847), rho_A (0.845), and Cronbach's Alpha (0.823) indicate strong convergent validity and internal consistency. Items PT2.1, PT2.2, and PT2.3 related to a perceived threat (PT) show high loadings, with PT2.2 being the most significant (loading=0.856). An overview of the answer distribution is provided by the mean (4.789) and standard deviation (1.378). Strong internal consistency and convergent validity are indicated by the high values for Cronbach's Alpha (0.889), rho_A (0.898), CR (0.921), and AVE (0.753) for perceived threat. Items T3.1, T3.2, and T3.3 in the Trust in Phone Communication (T) category show strong loadings; T3.2 has the greatest loading (loading=0.778). The replies' central tendency and dispersion are indicated by the mean (4.287) and standard deviation (1.342). Cronbach's Alpha (0.786), rho_A (0.797), CR (0.843), and AVE (0.578) values all suggest adequate internal consistency and convergent validity. The in-depth analysis of loadings, means, standard deviations, and reliability metrics improves the comprehension of latent constructs' measurement characteristics [52]. Reliability coefficients and high loadings indicate that the chosen items successfully capture the intended structures [56]. Furthermore, satisfactory AVE values show that latent variables rather than measurement errors account for a sizable percentage of the variance [57]. Together, these results strengthen the validity and robustness of your measurement model, providing a strong basis for the structural analysis that follows in this study.

Table 3. Measurement model evaluation

Construct	Item	Loading	Mean	Standard Deviation	Cronbach's Alpha	rho_A	CR	AVE
K	K1.1	0.756						
	K1.2	0.784	5.421	1.234	0.823	0.845	0.847	0.576
	K1.3	0.734						
PT	PT2.1	0.812						
	PT2.2	0.856	4.789	1.378	0.889	0.898	0.921	0.753
	PT2.3	0.886						
T	T3.1	0.817						
	T3.2	0.778	4.287	1.342	0.786	0.797	0.843	0.578
	T3.3	0.769						

Table 4. Correlations (HTMT) and the square root of AVE

	K	PT	T
K	**0.759**		
PT	0.546(0.632)	**0.868**	
T	0.552(0.613)	0.378(0.415)	**0.76**

The links between the constructs of Perceived Threat (PT), Knowledge of Call Spoofing (K), and Trust in Phone Communication (T) are revealed by the correlation matrix displayed in Table 4. The diagonal elements, as indicated, stand in for the self-correlations, which are always 1. The

pairwise correlations between the constructs are shown in the off-diagonal elements. A moderately positive link is implied by the correlation coefficient of 0.546 between Perceived Threat (PT) and Knowledge of Call Spoofing (K). This implies that a rise in perceived threat is correlated with a greater understanding of call spoofing. When considering the impact of Trust in Phone Communication (T), the parenthesized result (0.632) can suggest a partial link. Likewise, a moderately favorable link is shown by the correlation value of 0.552 between Knowledge of Call Spoofing (K) and Trust in Phone Communication (T). This implies that trust in phone communication tends to rise with increased information about call spoofing. A partial association may be implied by the parenthesized result (0.613), given the impact of perceived threat (PT). Perceived Threat (PT) and Trust in Phone Communication (T) have a weakly positive link, as indicated by their correlation coefficient of 0.378. This implies that confidence in phone conversations tends to increase modestly with perceived threat. The figure that has been parenthesized (0.415) could indicate a partial correlation that takes Knowledge of Call Spoofing (K) into consideration. The correlation matrix in this study gives a quantitative summary of the relationships between the constructs and offers insightful information about how changes in one concept might affect changes in others [58]. Partial correlations provide a more nuanced view of the relationship between Knowledge of Call Spoofing, Perceived Threat, and Trust in Phone Communication by assisting in the control of the impact of other factors.

5.1 Research model and hypotheses testing

Once the validity and reliability of the constructs were established, the researcher looked at the conceptual model. The theory and concept of the path model were initially examined to assess how effectively the theory and concept might be supported by empirical data [59]. This analysis was done for the conceptual model shown in Figure 1. Advanced statistical methods like Structural Equation Modeling (SEM) were used to thoroughly examine these hypotheses, and a sizable sample size was used to guarantee the validity and generalizability of the results [60]. Extensive hypothesis testing was conducted on the hypotheses, encompassing the analysis of path coefficients, R-square values, and significance levels [61]. This allowed for a comprehensive comprehension of the model's explanatory capacity as well as the importance of specific interactions within the suggested framework (Figure 2). SEM's application made it possible to evaluate the interdependencies between the variables holistically, which advanced our understanding of call spoofing, threat perception, and telecom trust.

The research methodology that examines the complex links between Knowledge of Call Spoofing (K), Perceived Threat (PT), and Trust in Phone Communication (T) is presented in Table 5 along with the results of two crucial hypotheses, H1 and H2. The first hypothesis looks at the direct correlation between trust in phone communication (T) and knowledge of call spoofing (K). Regarding the first hypothesis, the beta coefficient (β) of 0.192 indicates that trust in phone communication and knowledge of call spoofing have a positive and statistically significant association. At $p<0.001$, the corresponding t-value of 3.546 suggests a high degree of statistical significance. This lends credence to the idea that people who are more knowledgeable about call spoofing are inclined to have greater levels of confidence while communicating over the phone. The second hypothesis investigates an indirect relationship, positing that the association between Knowledge of Call Spoofing (K) and Trust in Phone Communication (T) is influenced by Perceived Threat (PT). According to Hypothesis 2, Perceived Threat has a positive and statistically significant indirect effect on the link between Knowledge of Call Spoofing and Trust in Phone Communication, as indicated by the beta coefficient of 0.234 and the t-value of 3.665 ($p<0.001$). This shows that people who feel more threatened are more prone to rely on their call spoofing expertise, which in turn affects their degree of trust when communicating over the phone. The strength and dependability of the observed associations are highlighted by the significance level of $p<0.001$. The level of statistical significance is made evident in a straightforward manner. Collectively, these results add to a more complex understanding of how call spoofing knowledge and perceived threat interact to influence phone communication trust, offering insightful information for both theoretical and applied purposes in the context of digital communication security.

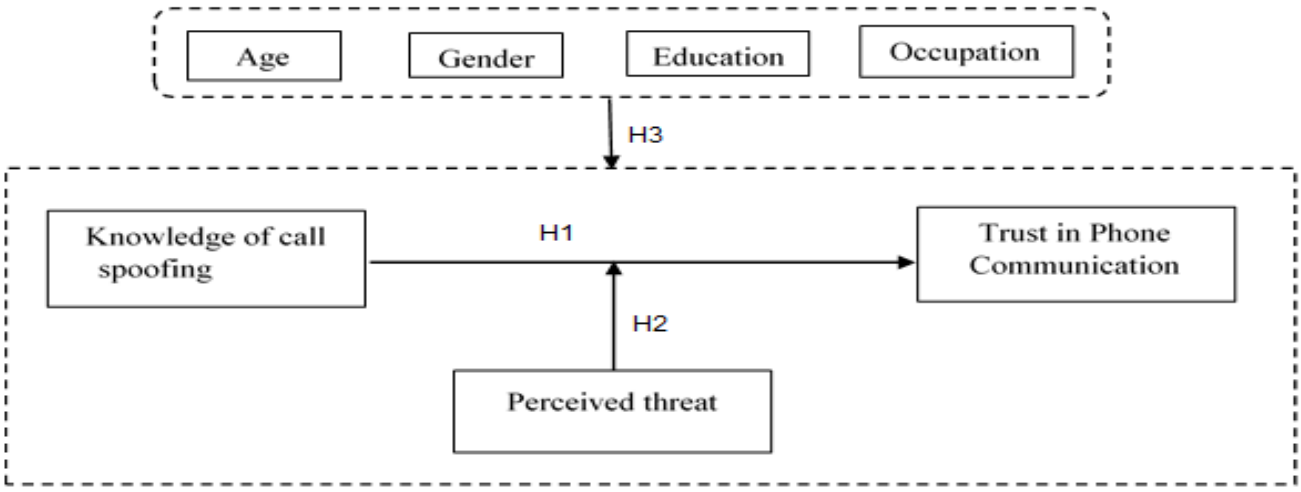

Figure 1. Proposed research framework

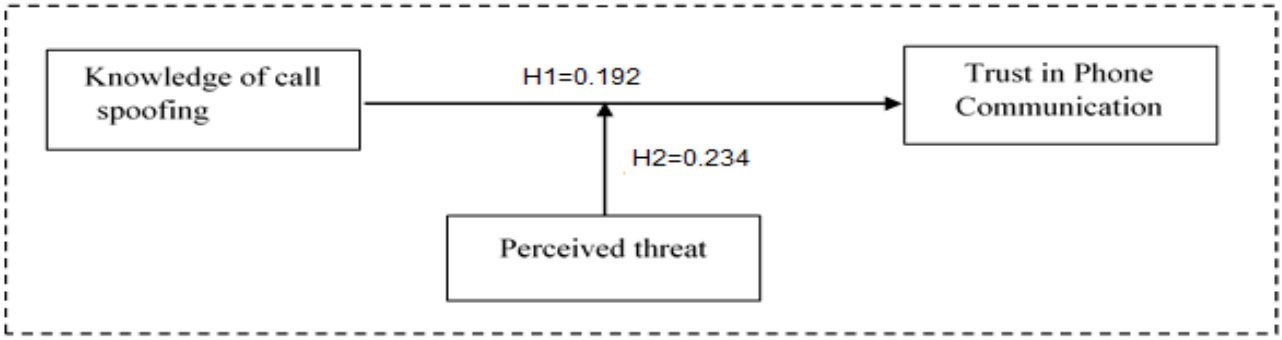

Figure 2. Research hypotheses

Table 5. Hypotheses testing

Model	Path Coefficients (β)	T-Value	Hypotheses	Decision	Significance
K→T	0.192	3.546	H1	Supported	p<0.001
PT→(K→T)	0.234	3.665	H2	Supported	p<0.001

Note: **p<0.01. *p<0.05

5.2 Moderating effects of gender, age, education, and occupation on knowledge of call spoofing, perceived threat, and trust in phone communication

Including demographic variables as moderators can improve the predictive accuracy of this research model. By accounting for these variables, researcher can more accurately predict how knowledge of call spoofing and perceived threats influence trust in phone communication within specific demographic groups. Treating these variables as moderators, this study reflects the differential impact of call spoofing across various segments of the population. This approach recognizes that the experience and perception of call spoofing are not uniform but vary according to these demographic factors. As different demographic groups may require different communication strategies and interventions. For instance, younger individuals who are more tech-savvy might be more aware of call spoofing but also more exposed to it due to higher technology use. In contrast, older adults may require more education and awareness campaigns. By understanding how different demographics modulate the relationship between call spoofing knowledge and trust, targeted and more effective interventions can be developed. The coefficients for Hypothesis H3, which attempts to investigate the moderating effects of demographic variables (Gender, Age, Education, and Occupation) on the associations between Perceived Threat, Knowledge of Call Spoofing, and Trust in Phone Communication, are shown in Table 6. The positive values found in the gender coefficients for both the male and female categories imply that gender does, in fact, impact how users perceive things. The coefficient for men is 0.643, which is slightly higher than the coefficient for women (0.577), suggesting that, generally speaking, men may have a more noticeable positive influence on user impressions. Regarding the Age coefficients, the downward trajectory from 18-24 to less than 55 suggests that age moderates the associations under investigation. The moderation impact decreases with age [62], indicating that, in comparison to older people, younger people may be more influenced by knowledge of call spoofing, perceived threats, and trust in phone communication. The coefficients corresponding to various degrees of education indicate that education serves as a moderator. Individuals with lower educational attainment may perceive call spoofing, perceived threat, and trust in phone communication more strongly due to the higher coefficients for lower education levels, especially the positive impact of a high school diploma (0.617). The moderating effect of various employment positions is further shown by occupation coefficients. The moderating effect experienced by those in worker positions appears to be favorable, as indicated by the positive coefficient of 0.432 for workers, and a negative one of -0.092 for managers. This suggests that, in comparison to managers, employees may, on average, feel a stronger favorable impact on their trust in phone communication. This research on how demographic variables influence the complex dynamics of user perceptions in the setting of call spoofing is enhanced by Hypotheses H3 and the comprehensive coefficients. These findings offer practical implications for the customization of communication security measures depending on demographic traits, acknowledging that various groups might react differently to tactics aimed at fostering trust, perception of threat, and knowledge. A more comprehensive understanding of user views regarding call spoofing and communication security is made possible by Hypotheses H3 and the corresponding coefficients, which provide insightful information about the moderating influences of gender, age, education, and occupation.

Table 6. Correlations between Hypotheses H3 and demographic variables

Hypotheses	Gender		Age					Education			Occupation				
	Male (N=456)	Female (N=224)	18-24 (N=75)	25-34 (N=120)	35-44 (N=218)	45-55 (N=184)	<55 (N=83)	High school diploid (N=110)	Diploma (N=168)	Bachelor (N=274)	Master and above (N=128)	Manager (N=78)	Supervisor(N=89)	Officer (N=211)	Worker (N=302)
H3	0.643	0.577	0.514	0.479	0.456	0.412	0.432	0.617	0.453	-0.092	-0.017	-0.012	-0.016	0.411	0.432

The summary of the main findings are:

Correlation between Call Spoofing Knowledge and Trust in Phone Communication: The research uncovers a significant positive relationship between an individual's awareness of call spoofing techniques and their trust in phone communications. It suggests that individuals who are more knowledgeable about call spoofing are likely to place greater trust in their telephonic interactions.

Impact of Demographic Variables: The study highlights that demographic factors such as age, gender, education level, and occupation play a moderating role in how knowledge of call spoofing influences perceived threat and trust in phone communication. These demographic subtleties shape the impact and perception of call spoofing differently across various segments of the population.

Perceived Threat as a Mediator: The research illustrates that perceived threat mediates the relationship between the knowledge of call spoofing and trust in phone communication. As individuals become more aware of call spoofing, their perception of threat increases, which, in turn, influences their level of trust in phone communications.

The broader implications of these findings, the research has several important consequences. The positive correlation between call spoofing knowledge and trust in phone communication emphasizes the need for increased awareness and education about call spoofing tactics. By enhancing knowledge, users can be better prepared to identify and avoid fraudulent calls, thereby reinforcing trust in telephonic communications.

The significant role of demographic variables suggests that any measures to combat call spoofing, such as awareness campaigns or educational programs, should be tailored to address the specific needs and characteristics of different demographic groups. This targeted approach can help in effectively mitigating the risks associated with call spoofing for various segments of the population.

Lastly, the mediating role of perceived threat highlights the psychological impact of call spoofing on individuals. Understanding this aspect can aid in developing strategies that not only focus on imparting knowledge but also address the users' concerns and fears related to phone communication security. This holistic approach can contribute to building a more secure and trustworthy telecommunication environment. Overall, this study provides crucial insights into the dynamics of call spoofing in India, offering a foundation for developing more effective strategies to enhance communication security and user trust in the digital age.

6. DISCUSSION AND CONCLUSIONS

The research's conclusions are especially pertinent given how quickly and dynamically communication patterns are changing in India. India offers a unique setting for investigating consumer perceptions of call spoofing and communication security, as it is home to one of the largest and fastest-growing digital populations globally. The Indian context is particularly relevant to the positive link between Knowledge of Call Spoofing and Trust in Phone Communication, as the country's user population is diverse due to the widespread usage of smartphones and rising levels of digital literacy. Through programs like Digital India, consumers are learning more about the issues surrounding technology, such as dishonest communication [25] techniques. The positive correlation implies that Indian consumers' confidence in phone communication may increase as they learn more about call spoofing, resulting in a more secure digital communication environment. Examining the moderating impacts of age, occupation, gender, and education is especially important [63] given India's complex sociocultural milieu. In India, a nation with a rich tapestry of cultures, traditions, and social norms, these cultural elements play a significant role in shaping how individuals perceive and respond to call spoofing. Indian culture is often characterized by a high level of trust and familiarity in social and family networks. This intrinsic trust can extend to phone communications, making individuals more susceptible to call spoofing, as they might be less skeptical of unknown callers. Additionally, the cultural norm of showing respect to authority figures or those claiming to be in positions of power can lead to a higher likelihood of falling prey to spoofed calls. India's vast linguistic diversity means that call spoofing tactics might be tailored to exploit language-specific nuances. Spoofers could use regional languages or dialects to build credibility and trust. People might lower their guard when communicated with in their native language, perceiving such calls as more trustworthy. Disparities in education, gender dynamics, age-related technology adoption trends, and vocational diversity in the Indian workforce are all important factors that influence how users view and react to communication security challenges. In India, where fast technical improvements meet with traditional values, it is critical to comprehend how various demographic groups perceive and react to call spoofing. The results point to possible differences in user perceptions between genders, age groups, educational backgrounds, and professional responsibilities. This emphasizes the necessity for customized communication security measures that are sensitive to the distinct features of various Indian demographic groups.

There are numerous practical ramifications for India's communication security protocols. Education programs can be made more effective by customizing them to appeal to a wider range of demographic groups. By identifying the age-related patterns and educational gaps in the impact of call spoofing knowledge, tailored interventions can be implemented to bridge the digital literacy gap. Recognizing the variations in occupations also helps in developing security plans that address the diverse requirements and worries of the Indian labor force. Several cultural subtleties in the Indian environment affect communication attitudes and practices. To provide a more thorough knowledge of user perceptions, future research could go deeper into regional variances, cultural factors, and linguistic considerations. Studies that follow the development of communication practices in response to evolving technology and security measures in the Indian setting throughout time could provide important insights for strategy adaptation.

This study adds to the conversation around communication security in India's digital environment. The results demonstrate the relationship between perceived threat, trust, and knowledge, with demographic factors serving as important moderators. As this study is conducted within the context of India, which may limit the generalizability of the findings to other cultural or regional contexts. Although the study considers demographic variations, the representation of certain groups (like rural populations or specific age groups) may not be comprehensive enough to generalize the findings across all demographics in India. In this research mixed

method design employed which is more complex and resource-intensive than single-method studies. Balancing qualitative and quantitative data collection, analysis, and integration requires considerable time and resources. In this study researcher applied multiple data sources for cross-verification helps to balance subjective biases inherent in qualitative data. Triangulation can enhance the credibility and validity of the research findings. In qualitative aspects of mixed-methods research, the researcher's perspectives or preconceptions can influence data collection and interpretation. This subjectivity can skew the findings, particularly in interviews and focus group discussions. Future research could aim to include these underrepresented areas, providing a more holistic understanding of the impacts of call spoofing.

From a methodological standpoint, the study predominantly addresses the psychological and social facets of call spoofing, leaving a gap in the exploration of technological aspects. Conducting longitudinal studies could help in understanding how perceptions and impacts of call spoofing evolve over time, especially as new technologies emerge. Utilizing big data analytics and AI could help in understanding patterns and trends in call spoofing, and in developing predictive models for better prevention strategies. These suggestions aim to address the limitations and expand the scope of research in understanding and mitigating the impacts of call spoofing on trust and communication.

ACKNOWLEDGMENT

The author would like to extend warm gratitude to all colleagues at Sohar University, Oman, for the time and effort spent reviewing and providing feedback on this article. This feedback contributed a lot to finalizing the quality of the manuscript.

REFERENCES

[1] Song, J., Kim, H., Gkelias, A. (2014). iVisher: Real-time detection of caller ID spoofing. ETRI Journal, 36(5): 865-875. https://doi.org/10.4218/etrij.14.0113.0798

[2] Waluyo, A., Cahyono, M.S., Mahfud, A.Z. (2022). Digital forensic analysis on caller ID spoofing attack. In 2022 7th International Workshop on Big Data and Information Security (IWBIS), Depok, Indonesia, pp. 95-100. https://doi.org/10.1109/IWBIS56557.2022.9924733

[3] Mustafa, H., Xu, W., Sadeghi, A.R., Schulz, S. (2014). You can call but you can't hide: Detecting caller id spoofing attacks. In 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Atlanta, GA, USA, pp. 168-179. https://doi.org/10.1109/DSN.2014.102

[4] Bidgoli, M., Grossklags, J. (2017). "Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing. In 2017 APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, USA, pp. 57-69. https://doi.org/10.1109/ECRIME.2017.7945055

[5] Abdallah, A., Maarof, M.A., Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68: 90-113. https://doi.org/10.1016/j.jnca.2016.04.007

[6] Muhammad, Z., Anwar, Z., Javed, A.R., Saleem, B., Abbas, S., Gadekallu, T.R. (2023). Smartphone security and privacy: A survey on APTs, sensor-based attacks, side-channel attacks, google play attacks, and defenses. Technologies, 11(3): 76. https://doi.org/10.3390/technologies11030076

[7] Azad, M.A., Morla, R. (2013). Caller-rep: Detecting unwanted calls with caller social strength. Computers & Security, 39: 219-236. https://doi.org/10.1016/j.cose.2013.07.006

[8] Zhao, Q., Chen, K., Li, T., Yang, Y., Wang, X. (2018). Detecting telecommunication fraud by understanding the contents of a call. Cybersecurity, 1: 1-12. https://doi.org/10.1186/s42400-018-0008-5

[9] Tan, C.B., Hijazi, M.H.A., Khamis, N., Nohuddin, P.N.E.B., Zainol, Z., Coenen, F., Gani, A. (2021). A survey on presentation attack detection for automatic speaker verification systems: State-of-the-art, taxonomy, issues and future direction. Multimedia Tools and Applications, 80(21-23): 32725-32762. https://doi.org/10.1007/s11042-021-11235-x

[10] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2(1): 1-22. https://doi.org/10.1186/s42400-019-0038-7

[11] Albladi, S.M., Weir, G.R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-Centric Computing and Information Sciences, 8(1): 1-24. https://doi.org/10.1186/s13673-018-0128-7

[12] Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., Dwivedi, Y.K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. Journal of Business Research, 154: 113368. https://doi.org/10.1016/j.jbusres.2022.113368

[13] Aleroud, A., Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68: 160-196. https://doi.org/10.1016/j.cose.2017.04.006

[14] Zhou, J., Hai, T., Jawawi, D.N., Wang, D., Ibeke, E., Biamba, C. (2022). Voice spoofing countermeasure for voice replay attacks using deep learning. Journal of Cloud Computing, 11(1): 51. https://doi.org/10.1186/s13677-022-00306-5

[15] Rahmeni, R., Aicha, A.B., Ayed, Y.B. (2019). Speech spoofing countermeasures based on source voice analysis and machine learning techniques. Procedia Computer Science, 159: 668-675. https://doi.org/10.1016/j.procs.2019.09.222

[16] Wu, Z., Evans, N., Kinnunen, T., Yamagishi, J., Alegre, F., Li, H. (2015). Spoofing and countermeasures for speaker verification: A survey. Speech Communication, 66, 130-153. https://doi.org/10.1016/j.specom.2014.10.005

[17] Bokharaei, H.K., Sahraei, A., Ganjali, Y., Keralapura, R., Nucci, A. (2011). You can SPIT, but you can't hide: Spammer identification in telephony networks. In 2011 Proceedings IEEE INFOCOM, Shanghai, China, pp. 41-45. https://doi.org/10.1109/INFCOM.2011.5935195

[18] Murray, C.J., Vos, T., Lozano, R., et al. (2012). Disability-adjusted life years (DALYs) for 291 diseases and injuries in 21 regions, 1990-2010: A systematic analysis for the global burden of disease study 2010. The Lancet, 380(9859): 2197-2223.

https://doi.org/10.1016/S0140-6736(12)61689-4
[19] Williams, E.J., Hinds, J., Joinson, A.N. (2018). Exploring susceptibility to phishing in the workplace. International Journal of Human-Computer Studies, 120: 1-13. https://doi.org/10.1016/j.ijhcs.2018.06.004
[20] MacKenzie, D. (2022). Spoofing: Law, materiality and boundary work in futures trading. Economy and Society, 51(1): 1-22. https://doi.org/10.1080/03085147.2022.1987753
[21] Asongu, S.A., Nwachukwu, J.C. (2016). The mobile phone in the diffusion of knowledge for institutional quality in sub-Saharan Africa. World Development, 86: 133-147. https://doi.org/10.1016/j.worlddev.2016.05.012
[22] Müller, R., Primc, N., Kuhn, E. (2023). 'You have to put a lot of trust in me': Autonomy, trust, and trustworthiness in the context of mobile apps for mental health. Medicine, Health Care and Philosophy, 1-12. https://doi.org/10.1007/s11019-023-10146-y
[23] Möllering, G. (2020). Communicating (about) trust. Journal of Trust Research, 10(1): 1-3. https://doi.org/10.1080/21515581.2020.1804240
[24] Oliver, S. (2019). Communication and trust: Rethinking the way construction industry professionals and software vendors utilise computer communication mediums. Visualization in Engineering, 7(1): 1. https://doi.org/10.1186/s40327-019-0068-y
[25] Haleem, A., Javaid, M., Qadri, M.A., Suman, R. (2022). Understanding the role of digital technologies in education: A review. Sustainable Operations and Computers, 3: 275-285. https://doi.org/10.1016/j.susoc.2022.05.004
[26] Parlasca, M.C., Hermann, D., Mußhoff, O. (2020). Can mobile phones build social trust? Insights from rural Kenya. Journal of Rural Studies, 79: 345-360. https://doi.org/10.1016/j.jrurstud.2020.08.015
[27] Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. Technology in Society, 58: 101122. https://doi.org/10.1016/j.techsoc.2019.03.005
[28] Tams, S., Legoux, R., Léger, P.M. (2018). Smartphone withdrawal creates stress: A moderated mediation model of nomophobia, social threat, and phone withdrawal context. Computers in Human Behavior, 81: 1-9. https://doi.org/10.1016/j.chb.2017.11.026
[29] Lewis, J.A. (2014). National perceptions of cyber threats. Strategic Analysis, 38(4): 566-576. https://doi.org/10.1080/09700161.2014.918445
[30] Zhao, B., Sui, D.Z. (2017). True lies in geospatial big data: detecting location spoofing in social media. Annals of GIS, 23(1): 1-14. https://doi.org/10.1080/19475683.2017.1280536
[31] Raposo, V.L. (2023). When facial recognition does not 'recognise': Erroneous identifications and resulting liabilities. AI & SOCIETY, 1-13. https://doi.org/10.1007/s00146-023-01634-z
[32] Kelley, N.J., Hurley-Wallace, A.L., Warner, K.L., Hanoch, Y. (2023). Analytical reasoning reduces internet fraud susceptibility. Computers in Human Behavior, 142: 107648. https://doi.org/10.1016/j.chb.2022.107648
[33] Rampersad, G., Althiyabi, T. (2020). Fake news: Acceptance by demographics and culture on social media. Journal of Information Technology & Politics, 17(1): 1-11. https://doi.org/10.1080/19331681.2019.1686676
[34] Talwar, S., Dhir, A., Singh, D., Virk, G.S., Salo, J. (2020). Sharing of fake news on social media: Application of the honeycomb framework and the third-person effect hypothesis. Journal of Retailing and Consumer Services, 57: 102197. https://doi.org/10.1016/j.jretconser.2020.102197
[35] Easterday, M.W., Rees Lewis, D.G., Gerber, E.M. (2018). The logic of design research. Learning: Research and Practice, 4(2): 131-160. https://doi.org/10.1080/23735082.2017.1286367
[36] Van Griensven, H., Moore, A.P., Hall, V. (2014). Mixed methods research-The best of both worlds? Manual Therapy, 19(5): 367-371. https://doi.org/10.1016/j.math.2014.05.005
[37] Petty, N.J., Thomson, O.P., Stew, G. (2012). Ready for a paradigm shift? Part 1: Introducing the philosophy of qualitative research. Manual Therapy, 17(4): 267-274. https://doi.org/10.1016/j.math.2012.03.006
[38] Harrison, R.L., Reilly, T.M. (2011). Mixed methods designs in marketing research. Qualitative Market Research: An International Journal, 14(1): 7-26. https://doi.org/10.1108/13522751111099300
[39] Rusá, Š., Komárek, A., Lesaffre, E., Bruyneel, L. (2018). Multilevel moderated mediation model with ordinal outcome. Statistics in Medicine, 37(10): 1650-1670. https://doi.org/10.1002/sim.7605
[40] Wunsch, G., Gourbin, C. (2020). Causal assessment in demographic research. Genus, 76(1): 18. https://doi.org/10.1186/s41118-020-00090-7
[41] Connor Desai, S., Reimers, S. (2019). Comparing the use of open and closed questions for Web-based measures of the continued-influence effect. Behavior Research Methods, 51: 1426-1440. https://doi.org/10.3758/s13428-018-1066-z
[42] Carpenter, N.C., Newman, D.A., Arthur Jr, W. (2021). What are we measuring? Evaluations of items measuring task performance, organizational citizenship, counterproductive, and withdrawal behaviors. Human Performance, 34(4): 316-349. https://doi.org/10.1080/08959285.2021.1956928
[43] Cash, P., Isaksson, O., Maier, A., Summers, J. (2022). Sampling in design research: Eight key considerations. Design Studies, 78: 101077. https://doi.org/10.1016/j.destud.2021.101077
[44] Pouryousefi, S., Frooman, J. (2019). The consumer scam: An agency-theoretic approach. Journal of Business Ethics, 154: 1-12. https://doi.org/10.1007/s10551-017-3466-x
[45] Mustafa, H., Xu, W., Sadeghi, A.R., Schulz, S. (2016). End-to-end detection of caller ID spoofing attacks. IEEE Transactions on Dependable and Secure Computing, 15(3): 423-436. https://doi.org/10.1109/TDSC.2016.2580509
[46] Bastick, Z. (2021). Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation. Computers in Human Behavior, 116: 106633. https://doi.org/10.1016/j.chb.2020.106633
[47] Szóstakowski, D., Besta, T. (2023). Perceived threat, injustice appraisal and willingness to join progressive collective action. Current Psychology, 1-12. https://doi.org/10.1007/s12144-023-04926-1
[48] Azize, Ş., Cemal, Z., Hakan, K. (2012). Does brand communication increase brand trust? The empirical

research on global mobile phone brands. Procedia-Social and Behavioral Sciences, 58: 1361-1369. https://doi.org/10.1016/j.sbspro.2012.09.1120

[49] Jung, A.R., Heo, J. (2022). The effects of mobile phone use motives on the intention to use location-based advertising: the mediating role of media affinity and perceived trust and risk. International Journal of Advertising, 41(5): 930-947. https://doi.org/10.1080/02650487.2021.1974204

[50] Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M. (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31(1): 2-24. https://doi.org/10.1108/EBR-11-2018-0203

[51] Hair, J., Alamer, A. (2022). Partial least squares structural equation modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. Research Methods in Applied Linguistics, 1(3): 100027. https://doi.org/10.1016/j.rmal.2022.100027

[52] Henseler, J., Ringle, C.M., Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of The Academy of Marketing Science, 43: 115-135. https://doi.org/10.1007/s11747-014-0403-8

[53] Magno, F., Cassia, F., Ringle, C.M. (2022). A brief review of partial least squares structural equation modeling (PLS-SEM) use in quality management studies. The TQM Journal, (ahead-of-print). https://doi.org/10.1108/TQM-06-2022-0197

[54] Dahlhaus, R. (2012). Locally stationary processes. In Handbook of Statistics. Elsevier, 30: 351-413. https://doi.org/10.1016/B978-0-444-53858-1.00013-2

[55] Efron, B., Tibshirani, R. (1985). The bootstrap method for assessing statistical accuracy. Behaviormetrika, 12: 1-35. https://doi.org/10.2333/bhmk.12.17_1

[56] Shevlin, M., Miles, J.N.V., Davies, M.N.O., Walker, S. (2000). Coefficient alpha: A useful indicator of reliability? Personality and Individual Differences, 28(2): 229-237. https://doi.org/10.1016/S0191-8869(99)00093-8

[57] Cheung, G.W., Cooper-Thomas, H.D., Lau, R.S., Wang, L.C. (2023). Reporting reliability, convergent and discriminant validity with structural equation modeling: A review and best-practice recommendations. Asia Pacific Journal of Management, 1-39. https://doi.org/10.1007/s10490-023-09871-y

[58] Starmans, M.P., van der Voort, S.R., Tovar, J.M.C., Veenland, J.F., Klein, S., Niessen, W.J. (2020). Radiomics: Data mining using quantitative medical image features. In Handbook of Medical Image Computing and Computer Assisted Intervention. Academic Press, pp. 429-456. https://doi.org/10.1016/B978-0-12-816176-0.00023-5

[59] van Witteloostuijn, A., van Hugten, J. (2022). The state of the art of hypothesis testing in the social sciences. Social Sciences & Humanities Open, 6(1): 100314. https://doi.org/10.1016/j.ssaho.2022.100314

[60] Forstmeier, W., Schielzeth, H. (2011). Cryptic multiple hypotheses testing in linear models: Overestimated effect sizes and the winner's curse. Behavioral Ecology and Sociobiology, 65: 47-55. https://doi.org/10.1007/s00265-010-1038-5

[61] Hair Jr, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., Danks, N.P., Ray, S. (2021). Evaluation of the structural model. Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook, 115-138. https://doi.org/10.1007/978-3-030-80519-7_6

[62] Ifinedo, P. (2016). The moderating effects of demographic and individual characteristics on nurses' acceptance of information systems: A Canadian study. International Journal of Medical Informatics, 87: 27-35. https://doi.org/10.1016/j.ijmedinf.2015.12.012

[63] Van Dyck, D., Cerin, E., De Bourdeaudhuij, I., Salvo, D., Christiansen, L.B., Macfarlane, D., Owen, N., Mitas, J., Troelsen, J., Aguinaga-Ontoso, I., Davey, R., Reis, R., Sarmiento, O.L., Schofield, G., Conway, T.L., Sallis, J.F. (2015). Moderating effects of age, gender and education on the associations of perceived neighborhood environment attributes with accelerometer-based physical activity: The IPEN adult study. Health & Place, 36: 65-73. https://doi.org/10.1016/j.healthplace.2015.09.007