Exploring the Impact of Chatbot Integration on Cybersecurity Awareness and Behaviour : A Multifactorial Analysis

Wael Sh. Basri

College of Business Administration, Northern Border University, ArAr. Saudi Arabia.
Email: wael.basri@nbu.edu.sa

Hilal H. Ali

College of Business Administration, Marketing, Northern Border University, ArAr. Saudi Arabia. Email: Hilal.Ali@nbu.edu.sa

Abstract

The study investigates the substantial mediating role and moderating impact of user proficiency levels on the relationship between pivotal factors and the acknowledgment and behavioural patterns concerning computer security within the framework of organizational environments. Two sets of questionnaires were administered: one targeted customers who had conducted online transactions (n=250), while the other was distributed to staff members of agencies involved in online commerce (n=200). These surveys probed the association with chatbots, expended effort, organizational cybersecurity culture, readiness for cyberattacks, users' evaluations of chatbots and their expertise levels, as well as users' cyber behaviour and cyber awareness. Structural Equation Modelling (SEM) with Partial Least Squares (PLS) was employed for data analysis. The results indicate that user confidence in chatbots significantly influences the relationship between chatbot availability, user proficiency in chatbot interaction, formulation of cyber threat models, organizational cybersecurity culture, and cybersecurity awareness and behaviours. Notably, robust moderation effects were observed concerning the expertise level of users in the cybersecurity associations related to threat model assessment, organizational cybersecurity culture, and cybersecurity behaviour and awareness. These findings underscore the paramount importance of fostering user trust in chatbots to advance cybersecurity awareness and behaviours facilitated by chatbot usage. Moreover, tailoring cybersecurity initiatives to accommodate varying user expertise levels and designing diverse options for user engagement may represent pivotal strategies for enhancing organizational cybersecurity in the long term. The primary focus of this researcher pertains to the examination of literature concerning the mediating function of trust in chatbots and the moderating influence of user expertise level on cybersecurity within organizational contexts. This research contributes to a more comprehensive understanding of the dynamics among the implicated factors and offers practical insights aimed at enhancing cybersecurity measures.

Keywords: Chatbots, Cybersecurity, User Trust, User Expertise, Artificial Intelligence (AI), Cybersecurity Culture.

Introduction

In recent years, chatbots have emerged as versatile tools, demonstrating proficiency across various domains of assistance and information dissemination. These AI-powered conversational agents exhibit significant potential in enhancing the efficiency and comprehensiveness of cybersecurity initiatives by introducing novel, user-centric communication channels. Leveraging natural language processing (NLP) and machine learning algorithms, chatbots deliver personalized guidance, address inquiries, and simulate real-world scenarios, thereby equipping users with insights into cyber risks and best practices.

In the contemporary digital era, cybersecurity awareness and behaviour represent pivotal components of cybersecurity practices. Awareness encompasses an individual's comprehension of vulnerabilities to cyber threats, recognition of the necessity to safeguard critical data, and adherence to recommended safety protocols. Zwilling et al. (2022) notes that while internet users generally possess considerable knowledge regarding cyber threats, their adoption of security measures remains at a basic level. Similarly, Shukla et al. (2022) observes a reluctance to implement significant security measures despite prior awareness. Li et al. (2019) underscores the significance of organizational policies in shaping employees' cybersecurity behaviours, while (BANDI, 2016) highlights individual variances in factors such as risk inclination and decision-making styles, which impact online security behaviours.

The primary objective of cybersecurity training initiatives is to educate individuals on prevalent cyber threats, including phishing schemes, malware incursions, and data breaches, while equipping them with the ability to identify and mitigate such risks. These efforts encompass security awareness training, dissemination of informational materials, and cultivation of a security-oriented culture within organizations. By enhancing awareness regarding the ramifications of cyber-attacks and the imperative for proactive risk management, individuals gain the knowledge necessary to safeguard themselves and their data against potential harm.

Ting et al. (2024) asserts that the level of cybersecurity behaviour among Malaysian university students exhibits parity across genders, emphasizing the necessity for equitable education and training for both sexes. Al-Dean Qawasmeh, AlQahtani, and Khurram Khan (2024) provides a comprehensive examination of cybersecurity training methodologies, emphasizing the importance of staying abreast of evolving trends in the field. Hakimi, Quchi, and Fazil (2024) underscores the significance of humanizing cybersecurity endeavours, recognizing the pivotal role of the human element in both operational efficacy and strategic decision-making processes. Carminati, Ponsford, and Gould (2024) has devised a scale to assess vulnerability to cyber scams among individuals with acquired brain injuries, catering to the unique needs of this specific population cohort.

The establishment of user trust in chatbots constitutes a fundamental prerequisite for their effective utilization across various domains, including cybersecurity. Trust serves as the cornerstone of human-computer interactions, shaping users' perceptions, cognitions, and behaviours towards chatbots. Particularly within the cybersecurity domain, where users depend on chatbots for information and assistance, fostering and maintaining trust is paramount to facilitating efficient interactions and collaborations. Extensive research on user trust in chatbots has delineated several critical factors. Følstad, Nordheim, and Bjørkli (2018) concluded that the quality of human-robot interaction significantly influences trust levels, encompassing factors such as the chatbot's comprehension of requests, its semblance of human-like qualities, self-presentation, and professional demeanour. Nordheim, Følstad, and Bjørkli (2019) expanded on this by emphasizing perceived expertise and responsiveness, alongside brand perception, as pivotal contributors to trust in chatbot technology. Burri (2018) suggested that incorporating voice output capabilities can enhance trust within chatbot interactions. Additionally, Wang and Siau (2018) highlighted the multifaceted roles of personality traits, institutional reputation, cognitive factors, knowledge dissemination, and calculative considerations in cultivating trust, particularly in the context of health-oriented chatbots.

The reliability, transparency, security, responsiveness, consistency, user experience, and accountability of chatbots collectively represent pivotal factors that

influence user trust. By prioritizing these aspects during the design and implementation phases, organizations can bolster user trust and confidence, fostering meaningful interactions and attaining desired outcomes, such as heightened cybersecurity awareness and behaviour. Rana, Jain, and Nehra (2024) emphasized the significance of trust while acknowledging that it is not the sole determinant of consumer attitudes in online shopping. Church (2024) underscored the importance of human oversight in chatbot interactions to mitigate the dissemination of misinformation. Solomovich and Abraham (2024) found a positive association between trust in ChatGPT and perceived usefulness, with ease of use acting as a mediating factor in this relationship. Simas and Ulbricht (2024) highlighted the importance of anthropomorphism in enhancing user interaction, trust, and acceptance, while also acknowledging ethical considerations inherent in such design choices.

User expertise level plays a pivotal role in shaping the design and effectiveness of chatbots, particularly within the cybersecurity domain. This level of expertise encompasses users' knowledge, skills, and experience pertaining to cybersecurity principles, techniques, and technologies. Awareness of the varying expertise levels among users enables chatbot developers to tailor interactions and content according to the specific needs of different user groups. Consequently, users benefit from a more personalized experience, leading to heightened awareness of cybersecurity practices and responsible behaviours. Carreno-Medrano, Dahiya, Smith, and Kulić (2019) introduced an approach to estimate users' skill levels based on task performance, demonstrating a strong correlation with actual performance levels. Hafeez et al. (2021) proposed a methodology utilizing EEG signals to accurately identify gamers' expertise levels, achieving an impressive accuracy rate of up to 98.04%. The spectrum of user expertise in cybersecurity ranges from novices with limited knowledge and experience to experts possessing advanced skills and technical proficiency. Recognizing this diversity is essential for developing chatbots capable of accommodating users across the proficiency spectrum and effectively addressing their specific requirements. Sudirjo, Gugat, Utama, Utami, and Martis (2023) conducted research on the User Experience Questionnaire, indicating favourable overall user

experiences with travel applications. Hernando and Aguilera-Venegas (2024) proposed a novel approach to developing expert systems capable of handling infinite-valued attributes, thereby enhancing the problem-solving capabilities of these systems. Mildner et al. (2024) explored ethical design challenges in conversational user interfaces, advocating for a human-centred approach. Cachola et al. (2024) developed a unified technique for creating and evaluating template views of documents, demonstrating high effectiveness through human evaluations.

This study offers a distinctive contribution to the field of cybersecurity through a thorough examination of the impact of chatbot integration on cybersecurity awareness and behaviour, employing multifactor analysis. By rigorously evaluating factors such as ease of access to chatbots, usability, threat model assessment, and organizational cybersecurity culture, this comprehensive investigation delineates crucial elements influencing user engagement with and response to cybersecurity initiatives. Beyond merely advancing our understanding of chatbots and cybersecurity, this research provides actionable insights for enhancing cybersecurity efficacy in an increasingly digitized environment.

Literature Review and Hypotheses

The degree of trust individuals place in chatbots significantly influences how the availability of chatbot access fosters their awareness and behaviour in cybersecurity. The user-chatbot relationship denotes the frequency or availability of opportunities for interaction. Cybersecurity awareness and behaviour encompass users' understanding of cybersecurity principles and their corresponding actions or practices. User trust in a chatbot serves as a metric of users' confidence or reliability in chatbot systems, encompassing aspects such as functionality, reliability, and security features. Research has demonstrated that user confidence in chatbots constitutes a major determinant of their acceptance and efficacy (Müller, Mattke, Maier, Weitzel, & Graser, 2019); (Przegalinska, Ciechanowski, Stroz, Gloor, & Mazurek, 2019), reflecting a combination of personality traits, system attributes, and user characteristics (Min, Fang, He, & Xuan, 2021). Nevertheless, there exists a need for nuanced inquiry to elucidate the specific role of trust within the broader relationship between cybersecurity awareness and

behaviour and access to chatbots. Empirical evidence suggests that user trust in chatbots plays a pivotal role in mediating the association between access to chatbots and cybersecurity awareness and behaviour (Alawida et al., 2024); (Arpaci, 2023). This trust is influenced by factors such as the chatbot's proficiency in discerning cybersecurity-related content, as well as its utility, usability, and credibility within the online customer journey. However, further enhancements in chatbot capabilities, particularly in tasks such as cybersecurity entity recognition, are warranted (Shafee, Bessani, & Ferreira, 2024). The issue of trust could be explored by investigating users' perceptions of security and safety measures when interacting with a chatbot. By positing that perceived trust in chatbots serves as an intermediary between information access and cybersecurity awareness and behaviour, the hypothesis suggests a mediating role of users' trust perceptions. Through their interactions with chatbots, users are inclined to bolster their trust in these systems, consequently contributing to their cybersecurity awareness and behaviour.

H1. *User trust in chatbots mediates the relationship between access to chatbot and cyber security awareness and behaviour*

The perceived ease of use of chatbots exerts influence on users' trust in them, subsequently shaping their attitudes towards cybersecurity and associated behaviours. Simplicity and responsiveness, synonymous with ease of use, pertain to users' perceptions of interaction with chatbots. Cybersecurity awareness and behaviour encompass users' knowledge of fundamental cybersecurity concepts and their adoption of cybersecurity precautions and actions. User trust in chatbots encapsulates the level of confidence users place in them concerning efficacy, reliability, and security performance. Research indicates that ease of use, cybersecurity awareness, and behaviour are positively associated with user trust in chatbots (De Cosmo, Piper, & Di Vittorio, 2021); (Prakash, Joshi, Nim, & Das, 2023); (Toader et al., 2019). Features such as input cues, user attitudes toward technology, and conversational capabilities impact trust in chatbots (Prakash et al., 2023), whereas glitches encountered during chatbot interactions may compromise credibility (Toader et al., 2019). Thus, in order to enhance user credibility and, consequently, bolster cybersecurity awareness and behaviour, careful consideration of these features in chatbot design and implementation is imperative. Studies on chatbots have identified factors influencing user acceptance and

intentions to use these systems. Goli, Sahu, Bag, and Dhamija (2023) found that purchasing intent hinges on perceived ease of use, usefulness, innovativeness, information quality, and customization of chatbots. Mehta et al. (2022) underscored the significant impact of consumer trust on attitudes and behavioural intentions towards chatbots, highlighting perceived security, traceability, and social presence of AI-based chatbots as primary determinants of usage extent. Hasan, Chowdhury, Rahman, Syed, and Ryu (2023) observed optimism and innovativeness as positive influencers, while discomfort and insecurity exerted negative influences on perceived ease of use and usefulness. This hypothesis posits that user trust in chatbots acts as a mediator, suggesting that although ease of use positively impacts cybersecurity awareness and behaviour, a portion of this effect is attributed to users' trust perceptions. Therefore, heightened ease of use of chatbots correlates with increased user trust in these systems, resulting in elevated levels of cybersecurity awareness and more favourable cybersecurity behaviours among users.

H2. *User trust in chatbots mediates the relationship between ease of use and cyber security awareness and behaviour.*

The extent of users' trust in chatbots dictates the degree to which they are influenced by threat model evaluations facilitated through these systems, subsequently impacting their awareness and behaviours concerning cybersecurity. Threat model evaluation entails the systematic assessment of potential cybersecurity threats and vulnerabilities within a system. Cybersecurity awareness and behaviour encompass users' comprehension of cybersecurity principles and their corresponding actions or practices in upholding cybersecurity measures. Numerous studies have identified key factors influencing user trust in chatbots. Wen, Lingdi, Kuijun, and Xiaoping (2009) proposed a trust model that considers both direct and indirect trust, with the latter being more significant and influenced by interactions. System attributes such as personalization and media richness, along with user characteristics and prior experience, may positively influence trust in chatbots (Min et al., 2021) Conversely, (Yang, Chen, Por, & Ku, 2023) acknowledged the security risks and vulnerabilities inherent in chatbots and emphasized the importance of instilling user trust and addressing privacy concerns. Additionally, individuals' perceived knowledge and trust in the internet may influence threat appraisal and coping processes, consequently

shaping cybersecurity behaviours (De Kimpe, Walrave, Verdegem, & Ponnet, 2022). This proposition suggests that the impact of threat model evaluation on cybersecurity awareness and behaviour is moderated by users' trust beliefs. In essence, through threat model evaluations conducted via chatbots, users' trust in these systems guides their interpretation and response to provided information, thereby affecting their cybersecurity awareness and conduct.

H3. *User trust in chatbots mediates the relationship between threat model evaluation and cyber security awareness and behaviour.*

Organizational cybersecurity culture encompasses a shared set of attitudes, values, and practices regarding cybersecurity within a specific organization. Cybersecurity awareness and behaviour refer to users' understanding of cybersecurity concepts and their actions or practices related to cybersecurity techniques. Studies investigating user trust in chatbots and its connection to cybersecurity awareness and behaviour have identified several key factors. Liang et al. (2021) highlighted user concerns regarding the use of data by chatbot developers, particularly emphasizing the necessity to safeguard personal information from misuse. Recent research has shed light on cybersecurity risks associated with chatbots, including potential vulnerabilities such as those observed in Chat GPT (Sebastian, 2023). These risks include the creation of malware and phishing emails, which malicious actors could exploit (Qammar et al., 2023). However, chatbots can also serve as valuable tools for detecting and predicting cybercrime, particularly on social media platforms through sentiment analysis (Arora, Arora, & McIntyre, 2023). Integrating chatbots in such contexts can enhance the development of sustainable strategies and contribute to a more secure cyber environment. Nevertheless, while chatbots have the potential to bolster cybersecurity, it is essential to monitor and address associated drawbacks and vulnerabilities. With user trust in chatbots serving as a mediator, the hypothesis posits that the influence of organizational cybersecurity culture on cybersecurity knowledge and practices is partially explained by users' confidence in chatbot utilization. This suggests that enhanced awareness and actions occur when users trust chatbots as intermediaries in cybersecurity efforts.

H4. *User trust in chatbots mediates the relationship between organizational cyber security culture and cyber security awareness and behaviour.*

Moderation Hypotheses

Chatbot accessibility refers to the feasibility and frequency of interaction with chatbot systems. Cybersecurity awareness and behaviour concern users' proficiency in managing cybersecurity concepts and their engagement in cybersecurity practices. El Hajal, Daou, and Ducq (2021) and Hamad and Yeferny (2020) have both illustrated the utilization of AI chatbots to enhance cybersecurity awareness, with Hajal's study particularly emphasizing the role of AI-based chatbots in augmenting user awareness. Research on user expertise in cybersecurity-related contexts has identified several primary factors. Rajivan, Moriano, Kelley, and Camp (2017) proposed a framework for assessing end-user security expertise, encompassing security skills, rules, and knowledge. Inibhunu et al. (2016) developed Focal Point, an adaptive level of detail rendering system for cybersecurity operations aimed at enhancing user performance. Carlton and Levy (2015) delineated the principal platform-independent cybersecurity skills for non-IT professionals, validated by subject matter experts. Moustafa, Bello, and Maurushat (2021) underscored the significance of user behaviour in cybersecurity management, highlighting cognitive disparities that may contribute to susceptibility to cyberattacks. This hypothesis posits that the relationship between chatbot accessibility and cybersecurity awareness and behaviour varies depending on the user's level of expertise. In essence, the impact of chatbot availability on cybersecurity outcomes is more pronounced for users with limited knowledge compared to those with extensive expertise.

H5: *User expertise level moderates the relationship between access to chatbot and cyber security awareness and behaviour.*

Cybersecurity awareness and behaviour encompass users' capacity to comprehend cybersecurity principles and enact behaviours conducive to cybersecurity measures. Research suggests that user proficiency, particularly in computer security skills, might act as a moderator in the relationship between ease of use and cybersecurity awareness and behaviour (Reddy & Rao, 2016). The role of internet security awareness as a moderating factor in university students' perception of cybersecurity, particularly in the context of using learning management systems, has also been underscored (Alfalah, 2023). Furthermore, the significance of user awareness

in information system security has been emphasized, with considerable implications for overall security levels (Galba, Šolić, & Lukić, 2015). Consequently, digital literacy functions as a mediator between perceived ease of use and the intention to utilize e-commerce applications (FAQİH, 2020). Additionally, Wijayanti, Al-Banna, and Nurdany (2024) noted that perceived risk assurance mediates the relationship between attitude and behavioural intentions in digital banking. The hypothesis introducing user expertise level as a moderator suggests that the relationship between ease of use and cybersecurity awareness and behaviour may vary depending on users' proficiency levels. In other words, the impact of perceived ease of use of chatbots on cybersecurity outcomes may differ among individuals with varying levels of cyber skills.

H6: *User expertise level moderates the relationship between ease of use and cyber security awareness and behaviour.*

Through the moderator of user expertise level, the proposed hypothesis posits that threat model evaluation and cybersecurity awareness and behaviour are contingent upon the user's level of proficiency. In essence, the outcomes of scanning threat model evaluations by users with varying levels of expertise in cybersecurity may significantly differ. Research investigating the association between user skills and threat model evaluation underscores the role of expertise as a moderator in this relationship. Anell, Gröber, and Krombholz (2020) underscores in her study that while end-users and security experts may hold divergent threat models, end-users often overlook certain attackers, suggesting that users' knowledge levels can influence the intricacies of threat model evaluation. Similarly, Deng (2015) proposed a threat assessment model comprising both objective and subjective factors, which are shaped by the experiences of commanders or experts, indicating that the assessor's knowledge can impact the assessment process. Meland, Tøndel, and Jensen (2010) and Williams and Yuan (2015) highlight the importance of experts in threat model evaluation, demonstrating that reusable threat models facilitate a more thorough identification of threats and mitigations. Williams employs these models to assess the efficacy of a threat modelling tool, which aids non-experts. Additionally, Giovacchini et al. (2024) and Görmez, Arslan, IŞIK, and Gündüz (2024) shed light on the role of user expertise in threat model evaluation.

H7: *User expertise level moderates the relationship between threat model evaluation and cyber security awareness and behaviour.*

The organizational cybersecurity culture encompasses shared values, behaviours, and practices related to cybersecurity within an organization, while cybersecurity awareness and behaviour reflect individuals' understanding of cybersecurity fundamentals and their corresponding actions. Goode, Levy, Hovav, and Smith (2018) underscores the significance of security education, training, and awareness programs in fostering cybersecurity behaviours. Halevi et al. (2016) elucidates how cultural and psychological factors, including user expertise, influence cybersecurity behaviour. Onumo, Ullah-Awan, and Cullen (2021) demonstrates how certain cybersecurity technologies mitigate negative perceptions of compliance with cybersecurity control procedures among employees. Trim and Upton (2016) emphasizes the role of staff training and organizational learning in shaping a cybersecurity culture tailored to different levels of expertise. Corradini and Nardelli (2019) highlights the impact of a robust organizational culture on risk, influenced by users' understanding and experience in cybersecurity, as well as their risk perception. This hypothesis posits that the relationship between organizational cybersecurity culture and cybersecurity awareness and behaviour is moderated by users' expertise levels, suggesting varying effects on cybersecurity outcomes among users with different levels of experience.

H8: *User expertise level moderates the relationship between organizational cyber security culture and cyber security awareness and behaviour.*

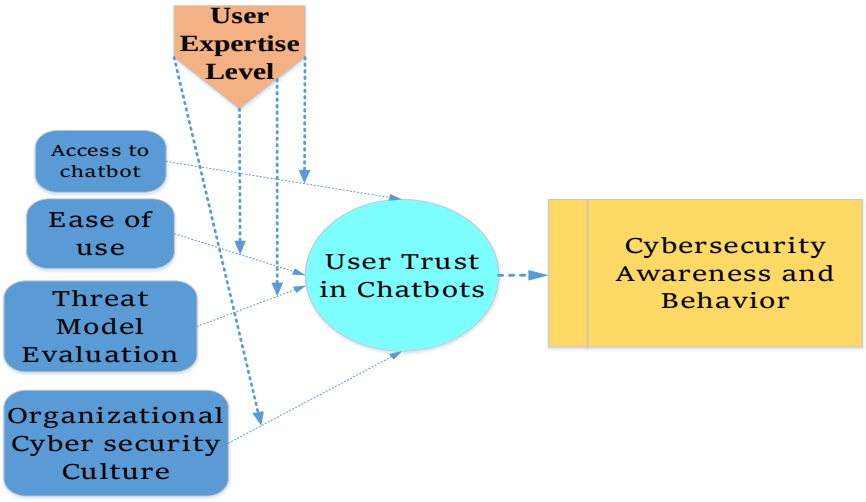

Figure 1: Conceptual Framework

Methodology

The research design entails the creation and dissemination of two distinct surveys, each aimed at specific segments of society engaged in online activities. Targeted participants include customers already involved in online purchasing. The survey aims to explore customer experiences and opinions regarding chatbots and cybersecurity. It comprises inquiries pertaining to key aspects such as chatbot availability, user-friendliness, trust in chatbots, and user knowledge levels. These factors significantly influence individuals' interactions with virtual sales assistants and their perceptions of online safety during the online purchasing process. Feedback from 250 online customers will provide insights across a diverse range of opinions.

Targeting Employees of Organizations Engaged in Online Business. This questionnaire is intended for individuals employed within organizations participating in various forms of online commercial activities. It delves into areas such as organizational cybersecurity culture, threat assessment and modelling, and cybersecurity awareness and behaviour. With a sample size of 200 employees, the questionnaire seeks to elucidate the organizational stance on cybersecurity protocols, employee awareness, and behaviours pertinent to online business endeavours. Its design aims to capture the organizational perspective on employees' cybersecurity practices, levels of awareness, and behavioural patterns that may impact online business operations.

Data Collection and Analysis

The questionnaires are distributed either via email or through online survey platforms. Participants receive detailed instructions outlining the purpose of the study, ensuring confidentiality, and clarifying their roles as subjects. Data collection occurs over a specified period to ensure an adequate sample size is attained. Quantitative analysis can be conducted on both types of questionnaire data. Descriptive statistics may be employed to summarize the characteristics of each participant and their responses to questionnaire items. SEM with PLS was utilized for data analysis.

Descriptive Statistics and Results

The Constructs column delineates the metrics of the variables or constructs utilized in the study. Subsequently, the constructs are defined, encompassing factors such as Access to Chatbot (AC), Ease of Use (EU), Organizational Cybersecurity Culture (OCSC), Threat Model Evaluation (TME), Cybersecurity Awareness and Behaviour (CAB), User Trust in Chatbots (UTC), and User Expertise Level (UEL).

Table 1. Descriptive Statistics

Constructs	Mean	Std. Deviation	Minimum	Maximum
AC	3.01	0.79	1	5
EU	3.25	0.82	1	5
OCSC	3.67	0.83	1	5
TME	3.27	0.73	1	5
CAB	2.98	0.91	1	5
UTC	3.54	0.82	1	5
UEL	3.69	0.86	1	5

Measurement Model

Factor loading elucidates the correlations between the indicator (item) and the latent construct it reflects in the model of latent variables. High factor loadings indicate a stronger relationship, suggesting that the item effectively reveals its association with the underlying construct. Differences ranging from -0.6 to -0.9 typically denote evidence of strong confirmatory validity in this table. On the other hand, Cronbach's alpha serves as a measure of internal consistency, indicating the extent to which participant responses within a construct are interrelated. A higher alpha value (often applying a threshold of 0.7 and above) enhances the reliability of the test indicator. It assesses whether the observations effectively reflect both global and local similarity.

Another criterion akin to Cronbach's Alpha is composite reliability, which evaluates the extent to which sub-theory indicators accurately describe the latent structure. Generally, composite reliability values of 0.7 and above are deemed acceptable. Additionally, AVE represents the proportion of variance in the indicators explained by the construct, excluding measurement error. The study aims to correlate construct reliability with the ratio of variance in the response indicators to variance

attributable to measurement error. An AVE value of 0.5 or higher signifies acceptable construct convergence validity.

From the data presented in Table 2, it is evident that all factors exhibit strong convergent validity, as indicated by their high factor loadings, acceptable factor loadings, composite reliability values, and AVE values exceeding 0.5. Conversely, it is prudent to scrutinize any indicators with low factor loadings or reliability, as these may necessitate further examination and potential refinement for future projects. Therefore, the robustness of the measurement model, which encompasses convergent validity, affirms that the items therein effectively measure the specified constructs.

Table 2. Convergent Validity

	Loadings	Alpha	Composite Reliability	AVE
AC1	0.754	0.794	0.811	0.754
AC2	0.701			
AC3	0.831			
EU1	0.861	0.801	0.823	0.768
EU2	0.839			
EU3	0.901			
EU4	0.769			
OCSC1	0.790	0.758	0.796	0.734
OCSC2	0.648			
OCSC3	0.597			
OCSC4	0.743			
OCSC5	0.786			
OCSC6	0.769			
OCSC7	0.846			
OCSC9	0.794			
TME1	0.869	0.819	0.857	0.786
TME2	0.847			
TME3	0.760			
TME5	0.783			
TME6	0.842			
TME7	0.760			
TME8	0.837			
TME9	0.722			
TME10	0.781			
CAB1	0.834	0.768	0.788	0.811
CAB2	0.864			
CAB5	0.689			
CAB6	0.766			
CAB7	0.811			
CAB9	0.758			

UTC1	0.687	0.857	0.867	0.812
UTC2	0.795			
UTC3	0.833			
UEL1	0.860	0.790	0.827	0.761
UEL2	0.719			
UEL3	0.758			
UEL4	0.837			
UEL5	0.849			

Discriminant Validity

VIF is a statistical measure assessing multicollinearity, which indicates the extent to which the estimated regression coefficient of a variable is inflated due to collinearity among predictor variables. VIF values exceeding 1 signify the presence of multicollinearity, wherein redundant information is present in multiple independent variables, potentially diminishing the validity and interpretability of models. Typically, VIF values below 5 are deemed satisfactory, although some researchers adopt a more conservative threshold of 3.

Table 3 presents the interrelations between pairs of variables. Each cell contains a correlation coefficient, which quantifies the strength of the relationship between two constructs. These coefficients indicate the extent of positive or negative association, ranging from -1 to 1, with -1 and 1 representing extreme negative and positive correlations, respectively, while zero signifies no relationship. Conversely, discriminant validity refers to a measurement that exhibits low correlations with other constructs, signifying that each construct measures distinct concepts and related notions.

The VIF error messages do not appear for the diagonal elements, which represent the variance inflation factors of each latent construct. These factors are not pertinent to discriminant validity assessment. Conversely, off-diagonal cells display correlation coefficients between pairs of constructs, serving as indicators of the strength of causal relationships between underlying concepts. Ensuring low correlations between constructs is the final component of discriminant validity, affirming that each construct is distinct from others and not redundant.

Table 3. Discriminant Validity

	VIF	AC	EU	OCSC	TME	UTC	UEL	CAB
AC	2.31							
EU	1.94	0.431						
OCSC	1.84	0.358	0.567					
TME	1.68	0.284	0.673	0.547				
UTC	1.64	0.564	0.648	0.466	0.466			
UEL	……	0.461	0.469	0.587	0.576	0.499		
CAB	…..	0.543	0.342	0.682	0.549	0.527	0.524	

Note: AC- Access to Chatbot, EU- Ease of Use, OCSC- Organizational Cybersecurity Culture, TME- Threat Model Evaluation, UTC- User Trust in Chatbots, UEL- User Expertise Level, CAB- Cybersecurity Awareness and Behaviour

Structural Model Results

This list enumerates the endogenous variables within the structural model. These variables are deemed endogenous as they are elucidated or impacted by other variables within the model. The values above the R-Squared metrics depict the percentage of total variance in each endogenous variable, elucidated by the independent variables within the model. For instance, an R-Squared value of 0.824 for the exogenous variable UTC indicates that approximately 82.4% of its variance is accounted for by the independent variables utilized in the model.

• The endogenous regressors in the model comprise UTC and CAB.

• The R^(Al-Dean Qawasmeh et al. 2024) value for UTC is 0.824, which suggests about 82.4% of the variance in users' trust in chatbots is caused by the model independent variables.

• The presented R-Squared value for CAB is 0.431, indicating that approximately 43.1% of the variance in cybersecurity awareness and behaviour is explained by the independent variables in this model.

These R-Squared values in table 4 offer insights into the predictive capability of the structural model concerning the endogenous variables. Elevated R-Squared values signify a closer fit of the model to the data, indicating that a greater proportion of the variance in the dependent variables is explained by the independent variables. Nevertheless, it is imperative to interpret these values alongside other model fit

statistics and theoretical considerations to assess the overall adequacy of the structural model.

Table 4. R –Square

Endogenous Variable	R Square
UTC	0.824
CAB	0.431

Mediating Effect

The beta coefficient, denoting the association between the indirect effects of the independent variable (IV) on the dependent variable (DV) through the mediator (Med), signifies the magnitude and direction of this relationship between the IV and DV. A positive beta coefficient denotes a positive indirect effect, while a negative coefficient indicates a negative indirect effect.

The standard error serves as an indicator of the variability or precision of the estimated beta coefficient. Reduction in standard errors signifies enhanced precision in inferring the indirect effect. T-statistics assess the significance of the beta coefficient, with higher values indicating greater certainty that the results are not random. P-values offer a measure of the significance of the beta coefficient, with values below a predetermined threshold (commonly 0.05) indicating statistical significance of the indirect effect. Evaluating the p-value determines the significance of a mediating effect. If the p-value falls below the significance level (e.g., 0.05), the effect is deemed a significant mediating influence. However, the mere presence of a small p-value does not ensure a sustainable mediation.

• The study examines the mediating roles of access to the chatbot (AC), ease of use (EA), threat model evaluation (TME), and organizational cybersecurity culture (OCSC) in the relationship between predictor variables and cybersecurity awareness and behaviour (CAB), mediated by users' attitudes towards the chatbots (UTC).

• All mediating effects are accompanied by reported beta coefficients, standard errors, t-statistics, and p-values.

• As indicated by the p-values for all aforementioned mediating effects (all values below 0.05), support is provided for all four mediating pathways: AC -> UTC -> CAB, EA -> UTC -> CAB, TME -> UTC -> CAB, and OCSC -> UTC -> CAB.

The findings of this study suggest that users' trust in chatbots could potentially serve as a mediator in the relationship among presence, ease of use, threat focus, organizational cybersecurity culture, and cybersecurity awareness and practices. This highlights the pivotal role of trust in shaping cybersecurity outcomes.

Table 5. Mediating Effect Results

	BETA	Standard Error	T Statistics	P Values	Decision
AC -> UTC -> CAB	0.125	0.028	3.54	0.012	Supported
EA -> UTC -> CAB	0.057	0.031	2.69	0.000	Supported
TME -> UTC -> CAB	0.068	0.049	4.68	0.019	Supported
OCSC -> UTC -> CAB	0.046	0.019	3.87	0.024	Supported

Moderating Effect Results

The beta weight signifies the strength and direction of the moderating influence exerted by the moderator variable (UEL) on the relationship between the IV and the Med. Positive coefficients indicate that the respective factor reinforces a choice or enhances confidence in the candidate, whereas negative coefficients signify the opposite effect. The standard error reflects discrepancies that may arise in the estimated beta coefficient. Essentially, smaller standard errors indicate more precise estimation of the impact of the moderation effect. T-tests ascertain the significance of beta coefficients. Increasing T-values provide evidence that the observed moderating effect is highly unlikely to occur by chance. Their robust association with the observed moderating effect diminishes the probability of chance occurrence.

The p-value served as the test statistic determining the statistical significance of the beta coefficient. Interpreting a p-value below a significance level, such as 0.05, denotes a significant moderating effect with a high level of confidence. Ultimately, the calculated data are utilized to derive the p-value, guiding the determination of moderation effect significance. It can be inferred that a moderation effect is statistically significant and supported if the p-value falls below the specified significance level (e.g., 0.05). However, this outcome should be interpreted cautiously.

• The aim of this study is to investigate the mediating effect of user expertise level (UEL) on the relationship between access to chatbot (AC), ease of use (EU), threat model evaluation (TME), and organizational cybersecurity culture (OCSC) and user

trust in chatbots (UTC).

• Table 6 presents the moderating relationships through beta coefficients, standard errors, t statistics, and p-values.

• The results support the idea that moderating the user expertise level influences the relationships between TME and OCSC, as well as UTC, as indicated by their statistically significant p-values (below 0.05).

• However, the mediating effects of user expertise level on the relationship between accessibility to chatbots (AC) and EU, as well as UTC, appear weak, as evidenced by their non-significant p-values.

The findings indicate that the user's expertise level plays a significant role in mediating the relationships between threat model evaluation and organizational cybersecurity culture, as well as between access to chatbot and ease of use. However, it does not reveal significant associations between threat model evaluation and ease of use, or between access to chatbot and organizational cybersecurity culture, in influencing user trust in chatbots.

Table 6. Moderating Effect Results

	Beta	Standard Error	T Statistics	P Values	DECISION
UEL-> AC-> UTC	0.137	0.010	1.02	0.219	Not Supported
UEL-> EU-> UTC	0.164	0.024	1.25	0.120	Not Supported
UEL-> TME-> UTC	0.138	0.020	3.54	0.014	Supported
UEL-> OCSC-> UTC	0.166	0.034	2.67	0.000	Supported

Discussion

The incorporation of chatbots into cybersecurity awareness and behaviour, facilitated by multifactorial analysis, unveils several pivotal variables. Firstly, access to chatbots influences user engagement and involvement in cybersecurity initiatives. Secondly, ease of use directly impacts users' capacity to comprehend and implement cybersecurity information. Additionally, the evaluation of threat models is essential to ensure chatbots effectively identify and respond to cybersecurity threats. Furthermore, organizational cybersecurity culture significantly influences users' preferences regarding chatbot-based interventions. By considering these factors, organizations can enhance accessibility, usability, threat detection capabilities, and

cybersecurity culture to improve cybersecurity education and behaviour. Ultimately, integrating chatbot technology can promote greater user engagement, enhanced cybersecurity knowledge resilience, improved threat detection, and adherence to cybersecurity practices, thereby bolstering cybersecurity in both individual and business contexts.

The research outcomes underscore the pivotal role of user trust in mediating various factors including accessibility, ease of use, threat model evaluation, organizational cybersecurity culture, and cybersecurity awareness and behaviour. This emphasizes the fundamental significance of user trust in shaping cybersecurity practices. Users' trust in chatbots motivates compliance with security protocols and enhances vigilance towards cybersecurity issues. The results of the mediation analysis underscore the critical importance of reliability and trustworthiness in chatbot systems development as the initial step towards ensuring cybersecurity within an organization.

Evidently, the study did not uncover any substantial moderator effects of user expertise level on the correlation between chatbot usage and cybersecurity awareness and behaviour, as well as user ease of use and cybersecurity indicators. Such incongruent findings suggest that the overall frequency of chatbot interaction, driven by convenience rather than specific knowledge, appears to exert a lasting impact on cybersecurity practices regardless of internet users' cybersecurity literacy level. The moderation analysis revealed a noteworthy interaction between the user's expertise level and variables such as the evaluation of organizational cybersecurity culture and threat model, or the level of cybersecurity awareness. This underscores the significant influence of user knowledge on the acceptance and enactment of cybersecurity measures. With higher levels of expertise, individuals are more likely to interpret threat models differently and be receptive to initiatives aimed at fostering organizational cybersecurity culture. Consequently, this is expected to result in heightened cybersecurity consciousness and behaviour.

Hypothesis 1 posits that user trust plays a pivotal role in leveraging chatbots as effective tools for enhancing cybersecurity awareness and fostering desired behaviours among users. Establishing a coherent rationale elucidating the mediated

association between user trust and chatbots would facilitate the development of strategies and designs applicable in cybersecurity education systems and training environments. The findings of the analysis indicate a significant contribution of user trust to the cultivation of cybersecurity awareness and behaviour. Increased access to chatbots correlates positively with enhanced user trust, thereby exerting a favourable influence on their cybersecurity consciousness and behaviour.

Hypothesis 2 underscores the pivotal role of usability and trust in shaping the design of chatbot systems for cybersecurity training and education. Understanding the mediating role of user trust can inform efforts aimed at enhancing the usability of chatbots and instilling confidence in users, thereby attaining the desired level of cybersecurity. Consistently, the findings align with this theoretical framework, demonstrating a direct impact of usability on user trust in chatbots, subsequently influencing cybersecurity awareness and behaviour. When chatbots effectively convey a sense of ease of use to users, it enhances their trust, ultimately fostering improved cybersecurity practices.

Hypothesis 3 posits that user trust significantly influences the efficacy of chatbots in delivering cybersecurity-related content and fostering desired cybersecurity behaviours among users. Understanding trust as a mediator enables precise interventions in the deployment of chatbots for cybersecurity purposes. The analysis validates the hypothesis by revealing a linkage between the perceived trustworthiness of chatbots in assessing potential threats and users' cybersecurity awareness and behaviour. Awareness and assessment of various threat models positively contribute to enhancing trust in chatbot systems, consequently improving cybersecurity practices.

Hypothesis 4 underscores the imperative for organizations to cultivate trust in chatbots as integral to broader cybersecurity endeavours. Recognizing user trust as an intermediary factor can inform the formulation of strategies aimed at fostering a cybersecurity culture and promoting adherence to desired cybersecurity policies. The results robustly validate this assertion, emphasizing the pivotal role of organizational culture in engendering trust in chatbots to advance cybersecurity awareness and behaviour. Organizations with a strong cybersecurity culture garner employee

confidence in chatbot systems, thereby fostering adherence to sound cybersecurity practices.

Hypothesis 5 underscores the importance of considering users' expertise levels when designing and deploying chatbot models for cybersecurity awareness. Understanding how user expertise moderates the relationship between access to chatbots and cybersecurity outcomes can aid in identifying the most effective approaches tailored to diverse user groups. While the hypothesis did not garner support in the study, it remains a logical assumption. The findings suggest that users' proficiency levels do not significantly influence the relationship between moderate access to chatbots and cybersecurity awareness and behaviours. This implies that the cybersecurity risk remains largely consistent across user expertise levels, even with such access.

Hypothesis 6 underscores the importance of considering users' varying levels of cybersecurity knowledge when designing and evaluating the usability of chatbot systems for cybersecurity applications. Exploring how users' proficiency levels influence the interplay among these factors provides a foundation for devising suitable usability designs and interventions tailored to different user segments. However, the study findings do not appear to support this hypothesis. The intricacies of user expertise levels do not significantly impact the association between ease of use and cybersecurity awareness and behaviours. This indicates that the perceived usability of chatbots does not exhibit discernible patterns regarding users' cybersecurity outcomes based on their expertise levels.

Hypothesis 7 emphasizes the necessity of considering users' proficiency levels when formulating and executing threat model evaluations as part of diverse cybersecurity interventions. Recognizing that users' skill levels significantly shape the relationship between threat model assessment and cybersecurity outcomes can inform the targeting of interventions to better suit various user groups. Consistent with the hypothesis, the analysis strongly supports this notion. With threat model evaluation serving as a moderating factor, user expertise level notably impacts the correlation between cybersecurity awareness and behaviour. This underscores the importance of accounting for users' proficiency levels when conducting threat modelling and

devising cybersecurity strategies.

Hypothesis 8 focuses on user expertise in assessing the impact of organizational cybersecurity culture on cybersecurity outcomes. Understanding how user proficiency moderates this relationship can facilitate the cultivation of a cybersecurity culture within organizations and promote desired attitudes and behaviours among users of varying expertise levels. As anticipated, the results validate this concept. User expertise significantly influences the relationship between organizational cybersecurity culture and cybersecurity knowledge and behaviour, indicating that the impact of organizational culture may vary based on user proficiency.

Implications

The study examined the mediating role of trust in chatbots and the moderating effect of user expertise on cybersecurity awareness and behaviour. Results underscore the importance of user trust in chatbots for cybersecurity awareness and behaviour. Organizations should prioritize building trust in chatbots to promote better cybersecurity practices. Additionally, organizational cybersecurity culture plays a crucial role in establishing user trust and achieving desired cybersecurity outcomes. Aligning interventions with users' expertise levels can enhance cybersecurity protection. However, limitations such as reliance on self-reported data and response bias should be noted. Future research could explore additional motivational factors and the long-term impact of chatbots on security outcomes. Overall, this study provides insights into decision-making processes regarding cybersecurity practices and lays the groundwork for future research in the field.

Organizations are advised to prioritize initiatives aimed at fostering trust in chatbots among users. These efforts may involve transparent communication regarding chatbot capabilities and security measures, providing users with training on safe chatbot usage, and maintaining a reliable support system for addressing user concerns. Additionally, strategic interventions should be tailored to accommodate users with varying levels of expertise, considering factors such as threat model evaluation and organizational culture. The study contributes to the existing cybersecurity literature by elucidating the intertwined roles of user trust in chatbots

and user expertise levels. These findings enhance our theoretical understanding of factors influencing organizational cybersecurity effectiveness. Future research could delve deeper into the nuanced relationships between trust levels, user expertise, and contextual variables in shaping cybersecurity practices.

Limitations and Future Research Directions

While this research offers valuable insights, it faces limitations. Self-reported data may introduce bias, and the study's cross-sectional design precludes causal inference. Future research could employ longitudinal studies to assess chatbots' cybersecurity solutions. Additionally, exploring environmental factors such as industry and organizational size may provide further insights. Qualitative methods like interviews or focus groups could deepen our understanding of users' cybersecurity awareness in relation to chatbots. The study underscores the importance of transparency and expertise within the realm of cybersecurity, particularly within organizational contexts. Organizations must strive to understand and leverage these factors to effectively address cybersecurity challenges. By doing so, they can develop more efficient interventions and strategies to mitigate cyber risks.

References

Al-Dean Qawasmeh, S., AlQahtani, A. A. S., & Khurram Khan, M. (2024). Navigating Cybersecurity Training: A Comprehensive Review. arXiv e-prints, arXiv: 2401.11326. https://ui.adsabs.harvard.edu/link_gateway/2024arXiv240111326A/doi:10.48550/arXiv.2401.11326

Alawida, M., Abu Shawar, B., Abiodun, O. I., Mehmood, A., Omolara, A. E., & Al Hwaitat, A. K. (2024). Unveiling the dark side of chatgpt: Exploring cyberattacks and enhancing user awareness. Information, 15(1), 27. https://doi.org/10.3390/info15010027

Alfalah, A. A. (2023). The role of Internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study.

International Journal of Advanced and Applied Sciences, 10(4), 136-144. https://doi.org/10.21833/ijaas.2023.04.017

Anell, S., Gröber, L., & Krombholz, K. (2020). End user and expert perceptions of threats and potential countermeasures. Paper presented at the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). https://doi.org/10.1109/EuroSPW51379.2020.00038

Arora, A., Arora, A., & McIntyre, J. (2023). Developing chatbots for cyber security: Assessing threats through sentiment analysis on social media. Sustainability, 15(17), 13178. https://doi.org/10.3390/su151713178

Arpaci, I. (2023). A Multi-Analytical SEM-ANN Approach to Investigate the Social Sustainability of AI Chatbots Based on Cybersecurity and Protection Motivation Theory. IEEE Transactions on Engineering Management. https://doi.org/10.1109/TEM.2023.3339578

BANDI, S. (2016). An empirical assessment of user online security behavior: Evidence from a university. https://doi.org/10.13016/M2BJ7X

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: the motivators and barriers of employees' security behaviors. Paper presented at the 11th Symposium on Usable Privacy and Security. http://nrl.northumbria.ac.uk/id/eprint/28854

Bokolo, Z. (2023). Data security in chatbots for the insurance industry: a case study of a South African insurance company. Cape Peninsula University of Technology, https://doi.org/10.25381/cput.24440926.v1

Borsci, S., Malizia, A., Schmettow, M., Van Der Velde, F., Tariverdiyeva, G., Balaji, D., & Chamberlain, A. (2022). The chatbot usability scale: the design and pilot of a usability scale for interaction with AI-based conversational agents. Personal and ubiquitous computing, 26, 95-119. https://doi.org/10.1007/s00779-021-01582-9

Burri, R. (2018). Improving user trust towards conversational chatbot interfaces with voice output. In. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1272880

Cachola, I., Cucerzan, S., Herring, A., Mijovic, V., Oveson, E., & Jauhar, S. K. (2024). Knowledge-Centric Templatic Views of Documents. arXiv preprint arXiv:2401.06945. https://doi.org/10.48550/arXiv.2401.06945

Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. Paper presented at the SoutheastCon 2015. https://doi.org/10.1109/SECON.2015.7132932

Carminati, J.-Y. J., Ponsford, J. L., & Gould, K. R. (2024). Co-developing 'The CyberABIlity Scale'to assess vulnerability to cyberscams for people with acquired brain injury: Delphi and cognitive interviews with clinicians and people with acquired brain injury. Brain Impairment, 25(1). https://doi.org/10.1071/IB23065

Carreno-Medrano, P., Dahiya, A., Smith, S. L., & Kulić, D. (2019). Incremental estimation of users' expertise level. Paper presented at the 2019 28th IEEE International Conference on Robot and Human Interactive Communication (RO-MAN). https://doi.org/10.1109/RO-MAN46459.2019.8956320

Church, K. (2024). Emerging trends: When can users trust GPT, and when should they intervene? Natural Language Engineering, 1-11. https://doi.org/10.1017/S1351324923000578

Corradini, I., & Nardelli, E. (2019). Building organizational risk culture in cyber security: the role of human factors. Paper presented at the Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9. https://doi.org/10.1007/978-3-319-94782-2_19

De Cosmo, L. M., Piper, L., & Di Vittorio, A. (2021). The role of attitude toward chatbots and privacy concern on the relationship between attitude toward mobile advertising and behavioral intent to use chatbots. Italian Journal of Marketing, 2021, 83-102. https://doi.org/10.1007/s43039-021-00020-1

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime

context. Behaviour & Information Technology, 41(8), 1796-1808. https://doi.org/10.1080/0144929X.2021.1905066

Deng, Y. (2015). A threat assessment model under uncertain environment. Mathematical Problems in Engineering, 2015. https://doi.org/10.1155/2015/878024

El Hajal, G., Daou, R. A. Z., & Ducq, Y. (2021). Human firewall: Cyber awareness using WhatApp AI chatbot. Paper presented at the 2021 IEEE 3rd International Multidisciplinary Conference on Engineering Technology (IMCET). https://doi.org/10.1109/IMCET53404.2021.9665642

FAQİH, K. M. (2020). The influence of perceived usefulness, social influence, internet self-efficacy and compatibility on users'intentions to adopt e-learning: investigating the moderating effects of culture. IJAEDU-International E-Journal of Advances in Education, 5(15), 300-320.https://doi.org/10.18768/ijaedu.593878

Følstad, A., Nordheim, C. B., & Bjørkli, C. A. (2018). What makes users trust a chatbot for customer service? An exploratory interview study. Paper presented at the Internet Science: 5th International Conference, INSCI 2018, St. Petersburg, Russia, October 24–26, 2018, Proceedings 5. https://doi.org/10.1007/978-3-030-01437-7_16

Galba, T., Šolić, K., & Lukić, I. (2015). An Information Security and Privacy Self Assessment (ISPSA) Tool for Internet Users. Acta Polytechnica Hungarica, 12(7), 149-162. https://acta.uni-obuda.hu/Galba_Solic_Lukic_63.pdf

Giovacchini, P., Borghi, L., Tartari, D., Cucci, F., Caldarelli, A., Tassinari, M., . . . Marsili, L. (2024). Applying threat analysis approach in a small forest urban park (Northern Italy): local expert-based assessment to prioritize the management actions. Folia Oecologica, 51(1), 66-74. https://doi.org/10.2478/foecol-2024-0007

Goli, M., Sahu, A. K., Bag, S., & Dhamija, P. (2023). Users' Acceptance of Artificial Intelligence-Based Chatbots: An Empirical Study. International Journal of Technology and Human Interaction (IJTHI), 19(1), 1-18. https://econpapers.repec.org/RePEc:igg:jthi00:v:19:y:2023:i:1:p:1-18

Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. Online Journal of Applied Knowledge Management (OJAKM), 6(1), 54-66. https://doi.org/10.36965/OJAKM.2018.6(1)67-80

Görmez, Y., Arslan, H., IŞIK, Y. E., & Gündüz, V. (2024). Developing Novel Deep Learning Models to Detect Insider Threats and Comparing the Models from Different Perspectives. Bilişim Teknolojileri Dergisi, 17(1), 31-43. https://doi.org/10.17671/gazibtd.1386734

Hafeez, T., Umar Saeed, S. M., Arsalan, A., Anwar, S. M., Ashraf, M. U., & Alsubhi, K. (2021). EEG in game user analysis: A framework for expertise classification during gameplay. Plos one, 16(6), e0246913. https://doi.org/10.1371/journal.pone.0246913

Hakimi, M., Quchi, M. M., & Fazil, A. W. (2024). Human factors in cybersecurity: an in depth analysis of user centric studies. Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID), 3(01), 20-33. https://doi.org/10.58471/esaprom.v3i01.3832

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., . . . Chen, J. (2016). Cultural and psychological factors in cyber-security. Paper presented at the Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services. https://doi.org/10.1145/3011141.3011165

Hamad, S., & Yeferny, T. (2020). A chatbot for information security. arXiv preprint arXiv:2012.00826. https://doi.org/10.48550/arXiv.2012.00826

Hasan, M. R., Chowdhury, N. I., Rahman, M. H., Syed, M. A. B., & Ryu, J. (2023). Analysis of the User Perception of Chatbots in Education Using A Partial Least Squares Structural Equation Modeling Approach. arXiv preprint arXiv:2311.03636. https://doi.org/10.48550/arXiv.2311.03636

Hernando, A., & Aguilera-Venegas, G. (2024). A novel way to build expert systems with infinite-valued attributes. http://dx.doi.org/%2010.3934/math.2024145

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. http://hdl.handle.net/10125/60074

Inibhunu, C., Langevin, S., Ralph, S., Kronefeld, N., Soh, H., Jamieson, G. A., . . . White, M. (2016). Adapting level of detail in user interfaces for Cybersecurity operations. Paper presented at the 2016 Resilience Week (RWS). https://doi.org/10.1109/RWEEK.2016.7573300

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Liang, K. H., Lange, P., Oh, Y. J., Zhang, J., Fukuoka, Y., & Yu, Z. (2021). Evaluation of in-person counseling strategies to develop physical activity chatbot for women. arXiv preprint arXiv:2107.10410. https://doi.org/10.48550/arXiv.2107.10410

Mehta, R., Verghese, J., Mahajan, S., Barykin, S., Bozhuk, S., Kozlova, N., . . . Dedyukhina, N. (2022). Consumers' behavior in conversational commerce marketing based on messenger chatbots. F1000Research, 11, 647. https://doi.org/10.12688/f1000research.122037.1

Meland, P. H., Tøndel, I. A., & Jensen, J. (2010). Idea: reusability of threat models–two approaches with an experimental evaluation. Paper presented at the International Symposium on Engineering Secure Software and Systems. https://doi.org/10.1007/978-3-642-11747-3_9

Mildner, T., Cooney, O., Meck, A.-M., Bartl, M., Savino, G.-L., Doyle, P. R., . . . Wenig, N. (2024). Listening to the Voices: Describing Ethical Caveats of Conversational User Interfaces According to Experts and Frequent Users. arXiv preprint arXiv:2401.14746. https://doi.org/10.48550/arXiv.2401.14746

Min, F., Fang, Z., He, Y., & Xuan, J. (2021). Research on Users' Trust of Chatbots Driven by AI: An Empirical Analysis Based on System Factors and User Characteristics. Paper presented at the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE). https://doi.org/10.1109/ICCECE51280.2021.9342098

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. Frontiers in Psychology, 12, 561011. https://doi.org/10.3389/fpsyg.2021.561011

Müller, L., Mattke, J., Maier, C., Weitzel, T., & Graser, H. (2019). Chatbot acceptance: A latent profile analysis on individuals' trust in conversational agents. Paper presented at the Proceedings of the 2019 on Computers and People Research Conference. https://doi.org/10.1145/3322385.3322392

Nordheim, C. B. (2018). Trust in chatbots for customer service–findings from a questionnaire study. http://dx.doi.org/10.1007/978-981-19-7532-5_19

Nordheim, C. B., Følstad, A., & Bjørkli, C. A. (2019). An initial model of trust in chatbots for customer service—findings from a questionnaire study. Interacting with Computers, 31(3), 317-335. https://doi.org/10.1093/iwc/iwz022

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. ACM Transactions on Management Information Systems (TMIS), 12(2), 1-29. https://doi.org/10.1145/3424282

Prakash, A. V., Joshi, A., Nim, S., & Das, S. (2023). Determinants and consequences of trust in AI-based customer service chatbots: 基于人工智能的客户服务聊天机器人信任的决定因素和后果. The Service Industries Journal, 43(9-10), 642-675. https://doi.org/10.1080/02642069.2023.2166493

Przegalinska, A., Ciechanowski, L., Stroz, A., Gloor, P., & Mazurek, G. (2019). In bot we trust: A new methodology of chatbot performance measures. Business Horizons, 62(6), 785-797. https://doi.org/10.1016/j.bushor.2019.08.005

Qammar, A., Wang, H., Ding, J., Naouri, A., Daneshmand, M., & Ning, H. (2023). Chatbots to chatgpt in a cybersecurity space: Evolution, vulnerabilities, attacks, challenges, and future recommendations. arXiv preprint arXiv:2306.09255. https://doi.org/10.48550/arXiv.2306.09255

Rajivan, P., Moriano, P., Kelley, T., & Camp, L. J. (2017). Factors in an end user security expertise instrument. Information & Computer Security, 25(2), 190-205. https://doi.org/10.1108/ICS-04-2017-0020

Rana, J., Jain, R., & Nehra, V. (2024). Utility and acceptability of AI-enabled chatbots on the online customer journey. International Journal of Computing and Digital Systems, 15(1), 323-335. http://dx.doi.org/10.12785/ijcds/150125

Reddy, D., & Rao, V. (2016). Cybersecurity Skills: The Moderating Role in the Relationship between Cybersecurity Awareness and Compliance. https://aisel.aisnet.org/amcis2016/ISSec/Presentations/23

Sebastian, G. (2023). Do ChatGPT and other AI chatbots pose a cybersecurity risk?: An exploratory study. International Journal of Security and Privacy in Pervasive Computing (IJSPPC), 15(1), 1-11. doi.org/10.4018/IJSPPC.320225

Shafee, S., Bessani, A., & Ferreira, P. M. (2024). Evaluation of LLM Chatbots for OSINT-based Cyberthreat Awareness. arXiv preprint arXiv:2401.15127. https://doi.org/10.48550/arXiv.2401.15127

Shukla, S. S., Tiwari, M., Lokhande, A. C., Tiwari, T., Singh, R., & Beri, A. (2022). A Comparative Study of Cyber Security Awareness, Competence and Behavior. Paper presented at the 2022 5th International Conference on Contemporary Computing and Informatics (IC3I). https://doi.org/10.1109/IC3I56241.2022.10072880

Simas, G., & Ulbricht, V. R. (2024). Human-AI Interaction: An Analysis of Anthropomorphization and User Engagement in Conversational Agents with a Focus on ChatGPT. Intelligent Human Systems Integration (IHSI 2024): Integrating People and Intelligent Systems, 119(119). http://doi.org/10.54941/ahfe1004510

Solomovich, L., & Abraham, V. (2024). Exploring the influence of ChatGPT on tourism behavior using the technology acceptance model. Tourism Review. https://doi.org/10.1108/TR-10-2023-0697

Sudirjo, F., Gugat, R. M. D., Utama, A. N. B., Utami, E. Y., & Martis, A. (2023). The Application of User Experience Questionnaire to Evaluate Customer Experience When Using Digital Platform to Purchase Flight Ticket in Two Travel and Ticketing Digital Companies. Jurnal Sistim Informasi dan Teknologi, 57-62. https://doi.org/10.60083/jsisfotek.v5i4.333

Ting, T. T., Cheah, K. M., Khiew, J. X., Lee, Y. C., Chaw, J. K., & Teoh, C. K. (2024). Validation of cyber security behaviour among adolescents at Malaysia university: Revisiting gender as a role. International Journal of Innovative Research and Scientific Studies, 7(1), 127-137. https://doi.org/10.53894/ijirss.v7i1.2544

Toader, D.-C., Boca, G., Toader, R., Măcelaru, M., Toader, C., Ighian, D., & Rădulescu, A. T. (2019). The effect of social presence and chatbot errors on trust. Sustainability, 12(1), 256. https://doi.org/10.3390/su12010256

Trim, P., & Upton, D. (2016). Cyber security culture: Counteracting cyber threats through organizational learning and training: Routledge. https://doi.org/10.4324/9781315575681

Wang, W., & Siau, K. (2018). Trust in Health Chatbots. https://aisel.aisnet.org/icis2018/treos/treos/29

Wen, L., Lingdi, P., Kuijun, L., & Xiaoping, C. (2009). Trust model of users' behavior in trustworthy internet. Paper presented at the 2009 WASE International Conference on Information Engineering. https://doi.org/10.1109/ICIE.2009.33

Wijayanti, D. M., Al-Banna, H., & Nurdany, A. (2024). Improving Digital Banking Through Risk Assurance: Tam Modification Analysis. Journal of Central Banking Law and Institutions, 3(1), 153-176. https://doi.org/10.21098/jcli.v3i1.172

Williams, I., & Yuan, X. (2015). Evaluating the effectiveness of microsoft threat modeling tool. Paper presented at the Proceedings of the 2015 information security curriculum development conference. https://doi.org/10.1145/2885990.2885999

Yang, J., Chen, Y.-L., Por, L. Y., & Ku, C. S. (2023). A systematic literature review of information security in chatbots. Applied Sciences, 13(11), 6355. https://doi.org/10.3390/app13116355

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study.

Journal of Computer Information Systems, 62(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

Appendix 1: Questionnaire

Access to chatbot	
1. The chatbot was easy to access. 2. The chatbot function was easily detectable. 3. It was easy to find the chatbot.	(Borsci et al., 2022)
Ease of use	
1. It was easy for me to learn how to use this Chatbot 2. The chatbot is easy to use 3. I feel it is easy to get the chatbot to do what I want it to do 4. My dialogue with the chatbot was clear and understandable	(Nordheim, 2018)
Organizational Cyber security Culture	
1. Employees would regularly compare notes on Third Party Risk Management and discuss other cyber topics. 2. The core team working with cybersecurity leaders included members from across the enterprise, not just the tech departments 3. Employees indicated that they knew what to do when they received a suspicious email, and knew who to contact should they notice any other potential cyber incident brewing. 4. Employees were regularly told about cyber threats and were encouraged to take steps to both protect the company asset and their own personal assets. 5. The entire organization was continually updated on cybersecurity news and issues through campaigns designed to facilitate long-term retention of cybersecurity practices and behaviours. 6. Employees who got involved in cyber-related activities were praised and given 'status' in the organization.	(Huang & Pearlson, 2019)
Threat Model Evaluation	
1. I think I would like to use the proposed threat model 2. I find the proposed threat model unnecessarily complex 3. I think the proposed threat model is easy to use 4. I think I would need the support of security experts to be able to understand and use the proposed threat model 5. I found the identified threats and suggested mitigations in the model well integrated 6. I think there is too much inconsistency in this threat model 7. I think most people will learn to use this threat model very quickly	(Bokolo, 2023)

8. I find the threat model very cumbersome to use	
9. I feel very confident in using the threat model	
10. I need to learn a lot of things before I use the proposed threat model	
Cybersecurity Awareness and Behaviour	
Experiential Attitude	(Blythe, Coventry, & Little, 2015)
1. Security measures disrupt our existing workflows or business processes	
Self-efficacy	
2. We are implementing security measures in our organization	
Response cost	
3. The initial and ongoing costs of implementing and maintaining the security measures	
User Trust in Chatbots	
1. The interaction with the chatbot felt secure in terms of privacy.	(Borsci et al., 2022)
2. I believe the chatbot informs me of any possible privacy issues.	
3. I believe that this chatbot maintains my privacy.	
User Expertise Level	
1. I experienced to get my question answered	(Nordheim, 2018)
2. The content of the chatbot reflects expertise	
3. The chatbot appears knowledgeable	
4. I feel very sure about the chatbots	
5. competence	
6. The chatbot is well equipped for the task it is set to do	