Uncertain Supply Chain Management 13 (2025) 751–762

Contents lists available at GrowingScience

Uncertain Supply Chain Management

homepage: www.GrowingScience.com/uscm

Factors affecting cybersecurity awareness: A qualitative study in Saudi Arabia

Tariq Saleh[a*], Raed Kanaan[b], Rania Alzubaidi[c], Ghassan Ghazi Kanaan[d] and Marko Nino[e]

[a]*Business Administration Department, College of Business, Westcliff University, 17877 Von Karman Ave, Suite 400, Irvine, CA 92614, United States*
[b]*Department of Digital Marketing, Faculty of Business, Al-Zaytoonah University of Jordan, Amman 11733, Jordan*
[c]*Department of Computer Science, Faculty of Information Technology, Al-Ahliyya Amman University, Amman 19111, Jordan*
[d]*Department of Artificial Intelligence, Faculty of Science and Information Technology, Al-Zaytoonah University of Jordan, Amman 11733, Jordan*
[e]*College of Business, Westcliff University, 17877 Von Karman Ave, Suite 400, Irvine, CA 92614, United States*

A B S T R A C T

The objective of this research was to gain a deeper comprehension of how individuals perceive and respond to cybersecurity and how various internal and external factors influence these behaviors and attitudes. Conducted at ABC organization in Saudi Arabia, the study employed the qualitative methodology. Two online focus groups were employed featuring open-ended questions. The data were subsequently analyzed thematically using inductive and deductive coding techniques. Several theories were used as theoretical lenses to analyze the data. After the collected data had been analyzed, three main themes emerged: (a) perceived safeguards and threats, (b) personal and professional experience in information security, and (c) necessity of education and raising awareness. Additionally, two sub-themes were revealed: (a) costs and benefits and (b) necessity of safeguard measures and attaining trust. The study's identified themes and sub-themes offer a thorough comprehension of the demographic, social, cultural, and internalized factors influencing cybersecurity-related behavior. The identified themes could potentially be applicable to other settings. Future qualitative research could further explore the transferability of these findings by conducting similar studies in different organizational, cultural, and linguistic contexts. It is also recommended for future quantitative research to delve deeper than surface-level data and consider underlying meaning, factors, connections, or relationships that may skew the results. It is crucial to delve into hidden meanings, not just accept data at face value.

Article history:
Received September 24, 2024
Received in revised format October 22, 2024
Accepted December 26 2024
Available online December 26 2024

Keywords:
Cybersecurity awareness
Information security
Unified theory of acceptance and use of technology
Technology acceptance model
Thematic analysis
Protection motivation theory

1. Introduction

The information technology revolution has significantly increased individuals' access to the internet, which in turn led to significant security risks. Cybercriminals are now primarily targeting sensitive data, financial accounts, and passwords. The infrastructure is also vulnerable to cyberattacks, resulting in data leakage, significant financial losses, and even life-threatening consequences (Alzubaidi, 2021). Organizations' and users' assets include telecommunications systems, services, applications, infrastructure, personnel, connected computing devices, and the entirety of stored or transmitted information in cyberspace. However, the goal of cybersecurity is to achieve and maintain the security aspects of organizations' and users' assets against security threats in cyberspace (Veale & Brown, 2020). While many factors influence cybersecurity practices, the awareness of individuals regarding cybersecurity threats and their ability to assess and act upon those threats are considered significant factors in this context (Quayyum et al., 2021). Cybersecurity awareness and practices, in addition to technical remedies, can assist individuals in avoiding or mitigating cybersecurity risk-related damages (Quayyum et al., 2021). Consequently, it is

* Corresponding author
E-mail address: t.saleh.108@westcliff.edu (T. Saleh)

ISSN 2291-6830 (Online) - ISSN 2291-6822 (Print)

doi: 10.5267/j.uscm.2024.12.005

imperative to raise cybersecurity awareness and safeguard measures, given humans' critical role in these technologies (Yaseen & El Qirem, 2018, Abu-Alhaija, 2020, Alzubaidi, 2021).

2. Literature Review

Various theories, in addition to context-related and behavior-related factors, can be used to explain cybersecurity-related behavior (Mou et al., 2022).

2.1 Theoretical Dimension

Human behavior can be studied using a variety of theories and frameworks. Within the realm of cybersecurity, the investigation of human behavior can be approached by drawing upon theories and perspectives derived from other disciplines. For instance, the protection motivation theory (PMT) from health psychology can be employed to assess and understand behavioral patterns in the cybersecurity domain (Kannelønning & Katsikas, 2023). PMT is one of the notable theories used to investigate cybersecurity behavior (Almansoori et al., 2023; Ng et al., 2021; Sulaiman et al., 2022). In addition, the technology acceptance model (TAM) is widely used among scholars to investigate cybersecurity behavior and practices (Alsmadi et al., 2022; Alzighaibi, 2021; An et al., 2022; Jamil, 2022, Ali, 2023, Al-Soud et al., 2024). The PMT, derived from health psychology, is used to understand behavioral patterns in cybersecurity. It suggests that individuals assess threats based on their severity and vulnerability, and then consider various protective actions as potential responses. The theory has four main aspects: perceived severity of the hazard, likelihood of the hazard occurring, available mitigation measures, and the individual's ability to enact those measures. When encountering a threat, individuals' first instinct is to assess it by determining how severe it is (referred to as perceived severity) and how vulnerable one is to it (referred to as perceived vulnerability). If a threat's perceived vulnerability and perceived severity are high, then threat appraisal is also high. After threat appraisal, various protective actions are considered as potential responses. During this phase of the coping appraisal, individuals consider the believed effectiveness of these protective measures in mitigating the current risk (response efficacy), their perceived capability to execute these actions (self-efficacy), and the perceived personal costs, whether intrinsic or extrinsic, associated with implementing these actions (response cost). As a result, individuals develop protection motivation, expressed as the intention to engage in protective behavior. The TAM is a psychological framework designed to elucidate how new technologies are accepted and used by users. It has been expanded and modified over time to articulate the acceptance of technology in various settings more effectively. The theory is composed of two beliefs, "perceived usefulness" and "perceived ease of use." It is theorized that these beliefs influence behavioral intention. Perceived usefulness gauges an individual's perception that leveraging technology would improve work efficiency. Perceived ease of use is associated with an individual's belief that leveraging technology will require a little effort. Individuals have a greater propensity to embrace technology if it is extremely beneficial and straightforward. On the contrary, individuals tend to resist adopting a technology if they believe it has a low level of usability and is difficult to use. Also, perceived ease of use affects perceived usefulness. Thus, an individual who finds technology easier to use will likely have a higher chance of taking advantage of its capabilities. Building upon this, TAM2 introduced additional cognitive and social factors to provide a more nuanced understanding of technology acceptance. Finally, TAM3 further expanded the model by incorporating predictor factors for ease of use and system-related factors like perceived usability and enjoyment, offering a comprehensive framework for analyzing technology acceptance and usage.

In addition, the unified theory of acceptance and use of technology (UTAUT) is commonly used as an overarching theory. It integrates several models and theories. UTAUT analyzes users' attitudes and motivations in adopting and using technology. UTAUT states that four independent variables affect information system user behavior: "performance expectancy," "expected effort," "social impact," and "facilitating conditions". Performance expectancy is characterized as the extent to which technology will improve users' ability to carry out specific activities. High-performance expectation refers to the user's expectation that utilizing information systems will increase productivity. The expected effort is the degree of convenience consumers associate with utilizing technology. It refers to the usability of the information system. It reflects the perceived ease of use and the system's complexity. Social impact is the perception of individuals about the extent to which their friends and family advocate the use of a certain technology. Facilitating conditions refer to users' perceptions of organizational and technological infrastructure availability to engage in a behavior. The way in which the four independent variables affect behavior intentions is influenced by experience, age, gender, and whether the behavior is voluntary. Building upon the Unified Theory of Acceptance and Use of Technology (UTAUT), UTAUT2 introduced additional variables such as habit, hedonic motivation, and price value, while removing the willingness of usage as a moderating variable. These additions provide a more comprehensive understanding of technology acceptance and usage.

2.2 Behavior-Related Dimension

The role of organizational and societal norms in shaping an individual's cybersecurity awareness and behavior is crucial. The approach an organization takes towards cybersecurity plays a crucial role in shaping an information security culture. It influences the values of employees and guides their computer security behavior. However, home users often lack the mandatory security protocols present in workplace environments, leading to heightened risk perception due to the personal

relevance of their data. Some employees, accustomed to safety protocols at work, may not prioritize similar precautions at home. Additionally, home users without security training might remain unaware of threats and the protective resources available to them. Consequently, many individuals who use the internet at home lack essential tools for safeguarding themselves from security risks. Over half of employees working from home during the COVID-19 pandemic fail to adhere to the same security policies they follow when using company-provided devices at their workplace. Common contributing factors include the absence of organizational IT monitoring, the need to find productivity workarounds, and the lack of an office-like setup. Daily distractions, such as childcare responsibilities, also play a role in this behavior. The social context of a home computer user has informal determinants of an individual's cybersecurity awareness. Social learning about cybersecurity can be enhanced by hearing personal stories from family members and friends.

2.3 Research Gap

Numerous studies have delved into the intricate web of factors that shape cybersecurity awareness. For example, Alzubaidi (2021) employed the unified theory of acceptance and use of technology (UTAUT) and the technology acceptance model (TAM) to gauge cybersecurity awareness. While TAM focuses on usability and efficacy, UTAUT delves into individual demographics. However, Alzubaidi's study did not consider later variants of these theories, such as the extended unified theory of acceptance and use of technology (UTAUT2), the extended technology acceptance model (TAM2), and the technology acceptance model 3 (TAM3). These extended models incorporate additional factors like job relevance and social influence. By integrating these elements, researchers could uncover fresh insights, especially since social factors significantly impact security awareness levels (Dwivedi et al., 2017; Li & Siponen, 2011). Contradicting Alzubaidi's findings, Juozapavičius et al. (2022) discovered that password hygiene, a critical cybersecurity practice, is influenced by age and gender. Meanwhile, Addae et al. (2019) merged the protection motivation theory (PMT) with TAM to explore user behavior related to adaptive cybersecurity. Factors like attitude toward personal data and the value of personalization played a crucial role in their investigation. Interestingly, individuals often become more aware of cybersecurity after encountering threats, which challenges PMT's initial premise (Y. Li & Siponen, 2011). This underscores the need for further research to unravel the intricate interplay of internal and external factors in shaping cybersecurity awareness.

2.4 Research Methods

This study aimed to explore individuals' thoughts and actions related to cybersecurity, considering both external and internal factors. Leveraging focus groups, a qualitative research method, allowed for a comprehensive understanding of human behaviors, including norms, reasoning, thought processes, and interactions. Researchers' interactions with participants significantly shaped the study (Ahmad et al., 2019; Eyisi, 2016; Fidler et al., 2011). Conducted at ABC organization in Saudi Arabia, this qualitative study gathered primary data through online focus groups featuring open-ended questions. The diverse demographic backgrounds of participants enriched insights into the subject matter. Focus groups, as highlighted by Morgan and Hoffman (2018), excel in revealing varied opinions and experiences, fostering dynamic discussions beyond what individual interviews can achieve.

2.5 Data Collection

The study utilized Zoom as a means to conduct online focus groups. Additionally, Zoom's recording feature captured the sessions for subsequent transcription. Each session was 60 minutes long. After conducting the first focus group, coding was performed. Then, the second online focus group was initiated, followed by the coding cycle. Identifying themes started, and thematic analysis was performed in preparation for reporting the findings, limitations, recommendations, and future research. These steps are asserted by Guest et al. (2016), Nowell et al. (2017), and Saldana (2013).

2.6 Data Analysis

The study utilized NVivo 14 to transcript the recorded sessions. The accuracy of NVivo Transcription is up to 90% (QSR International, 2022). In addition, according to Krueger and Casey (2015), NVivo software allows for analytical possibilities that would not be reasonable with conventional methodologies. For example, this software enables the nesting of codes, in which a discourse between multiple participants can be coded in several ways. Nevertheless, the automated transcription was reviewed and adjusted as necessary. After transcribing the recorded sessions, coding began. The study used a hybrid technique combining inductive and deductive coding. According to Williams and Moser (2019), "using inductive and deductive approaches to data analysis can maximize analytic acuity and enable precise thematic categorization" (p. 51). Consequently, a priori codes were developed in deductive coding grounded on the literature review and the constructs inherent in the theories, namely, PMT, TAM, and UTAUT. Alternatively, the direction of the discourse surrounding open-ended questions was unknown, and it was critical for the data to give rise to the codes. As a result, this study also employed inductive coding techniques. According to Nguyen et al. (2021), in qualitative data analysis, a general inductive method (rather than a hypothetical-deductive one) is commonly used, in which particular theories are not imposed on the data to verify a specific hypothesis. Instead, forming conceptual categories and descriptive themes allows the data to "speak for themselves."

3. Results

This part is organized into several sections to ensure a coherent and comprehensive presentation of the findings. It begins with a detailed overview of the sample used in the study. It is followed by the result section that presents the raw data collected during the study. These data were then dissected and categorized into themes, representing the study's key findings.

3.1 Characteristics of the Sample

Two online focus groups were conducted, each of which consisted of five participants. The participants were 5 females and 5 males with varying professional backgrounds, and their age range was from 22 to 44 years old, as shown in Table 1.

Table 1
Participants Demographic Characteristics

Participants	Focus Group	Gender	Age (Year)	Profession
Participant 1	1st Focus Group	Male	38	Head of project management
Participant 2	1st Focus Group	Female	37	Administrative assistant
Participant 3	1st Focus Group	Male	41	Accountant
Participant 4	1st Focus Group	Female	22	HR operations specialist
Participant 5	1st Focus Group	Male	25	Marketing specialist
Participant 6	2nd Focus Group	Male	44	Deputy executive manager
Participant 7	2nd Focus Group	Female	26	Graphic designer
Participant 8	2nd Focus Group	Female	24	Public relations specialist
Participant 9	2nd Focus Group	Female	24	HR specialist
Participant 10	2nd Focus Group	Male	25	Business development specialist

Zoom was used to conduct the online focus groups. According to Archibald et al. (2019), Zoom can be used as a qualitative data collection tool due to its user-friendly interface, affordability, data handling capabilities, and security measures. Each online focus group session lasted for 60 minutes. Table 2 shows the initial probing questions asked during the sessions.

Table 2
Initial Probing Questions

#	Probing Questions
1.	What first comes to mind when you think about cybersecurity? And why?
2.	In your opinion, what aspects of your life shape your cybersecurity practices? And why?
3.	What safety measures do you use to protect yourself in cyberspace? And why?
4.	How do you ensure the security of your mobile devices?
5.	What are your thoughts on public Wi-Fi networks? Do you use them often?
6.	Are you familiar with the concept of social engineering? Can you explain?
7.	What are the biggest challenges in maintaining cybersecurity at home or in the workplace?

The Zoom sessions were audio recorded and then transcribed using NVivo Transcription's automated service. It was essential to transcribe the focus groups to start a thematic analysis. A total of 40 pages of double-spaced, 12-point, Times New Roman font transcriptions were generated, as shown in Table 3.

Table 3
Online Focus Groups Breakdown: Date, Duration, and Number of Transcribed Pages

Focus group	Zoom session date	Duration (minutes)	Number of Pages Transcribed
1st focus group	December 4, 2023	60	19
2nd focus group	December 5, 2023	60	21

The thematic analysis involves several steps: (a) become familiar with the data, (b) generate initial codes, (c) search for themes, (d) review themes, (e) define themes, and (f) write-up (Nowell et al., 2017). The automated transcripts were reviewed as part of data familiarization. Automated transcription can save time and effort. However, the automated transcription of non-native English speakers was challenging due to the speaker's accent, pronunciation, and grammar. In addition, the accuracy of the automated transcription depended on the audio quality and the internet stability. Therefore, the transcripts were reviewed while listening to the audio recording and corrected as necessary. In addition, any identifiable information was obscured. The corrected transcripts were then converted to Microsoft Word files and then sent to participants for their feedback and comments to verify the transcription accuracy. After ascertaining the transcription accuracy, the converted transcripts were imported into NVivo software. In the second step of the thematic analysis process, codes were assigned to the qualitative data by systematically categorizing and organizing the data to identify patterns, themes, and insights. There were two main approaches to coding: deductive and inductive. Deductive coding involves using the constructs of the relevant theories to guide the analysis, while inductive coding allows the codes to emerge from the data. To assign codes, the data were read through several times. Notes were taken, and important sections were highlighted to help identify relevant segments of data. Once a segment of data relevant to the research question was identified, a code was assigned to it.

The following example provides deductive and inductive coding rationales. One of the participants said:

Well, can I say something about the password manager? It is a good idea to use it, but at the same time, it is not. You know, the problem is, if you lose [*sic*] the access to the password manager itself, you lose [*sic*] everything. Losing [*sic*] the passwords of everything. This [*sic*] actually happened with [*sic*] me.

The a priori code "perceived usefulness" was used to deductively code "It is a good idea to use it," while the rest was coded as "fear of losing access to saved passwords and payment methods" inductively.

The inductive code "fear of losing access to saved passwords and payment methods" was also used to code another participant's experience with the password manager when the participant said, "If I lost my account, I'm going to lose everything. Even the payment method."

In addition, the discourse context was used during the codes' development. For example, two participants were asked the same question and had the same answer, but the context differed. The two participants were asked about their opinions regarding mobile text awareness messages, and the answers were similar in that they did not pay attention to those messages. However, one participant did not pay attention to those messages because the participant had a false sense of security, and the participant said, "I think because no one can access your bank account without the password [one-time code] that will be sent to your mobile phone." The other participant ignored those messages because the participant could not verify the sender's identity, and the participant said, "I ignore it because I know it is not a formal message or email." The first response was coded as "ignoring awareness messages because of two-factor authentication," while the second was coded as "trust issues of third entities."

3.2 Themes

Once codes were assigned to the data, patterns and connections between codes were determined. Similar codes were grouped together to form themes and sub-themes, as shown in Fig. 1 and Fig. 2.

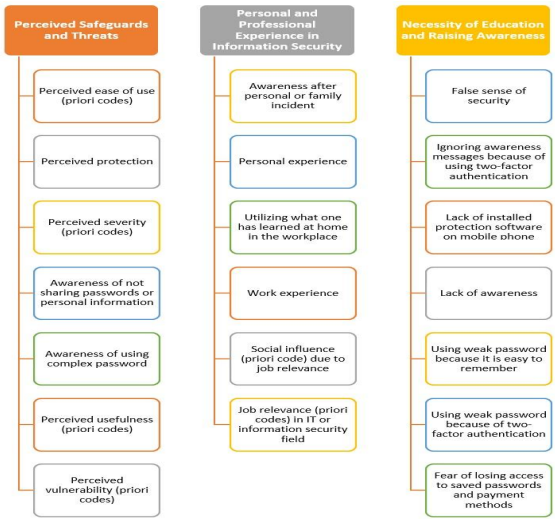

Fig. 1. Main Themes

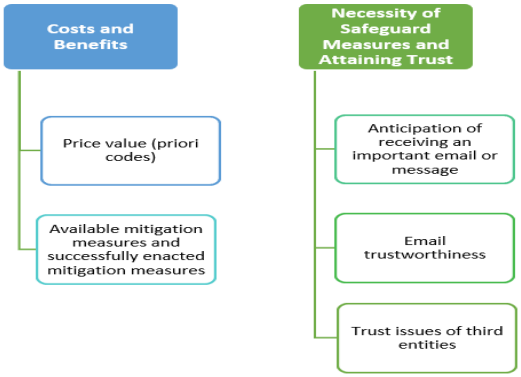

Fig. 2. Sub-Themes

3.2 Theme 1: Perceived Safeguards and Threats

Perceived Safeguards and Threats is a theme that revolves around how individuals perceive the measures in place to protect against cyber threats, as well as their awareness and understanding of the potential threats that exist in the digital world. The following codes are associated with this theme:

Perceived ease of use: This a priori code, adopted from TAM theory, refers to the ease with which users can access and use security measures (Castillo-Vergara et al., 2022; Singh et al., 2020). If security measures were too complicated or difficult to use, participants were less likely to use them.

Perceived protection: This code refers to the extent to which users believe that security measures will protect their personal information. If participants did not believe that security measures were effective, they were less likely to use them.

Perceived severity: This a priori code, adopted from PMT theory, refers to the perceived severity of the consequences of a security breach (Mou et al., 2022). If participants did not believe that the consequences of a security breach were severe, they were less likely to use security measures.

Awareness of not sharing passwords or personal information: This code refers to participants' awareness of the importance of not sharing passwords or personal information with others.

Awareness of using complex passwords: This code refers to participants' awareness about the importance of using complex passwords.

Perceived usefulness: This a priori code, adopted from TAM theory, refers to the extent to which users believe that security measures are useful (Castillo-Vergara et al., 2022; Singh et al., 2020). If participants did not believe that security measures were useful, they were less likely to use them.

Perceived vulnerability: This a priori code, adopted from PMT theory, refers to the extent to which users believe that they are vulnerable to security breaches (Mou et al., 2022). If participants did not believe that they were vulnerable to security breaches, they were less likely to use security measures.

3.3 Sub-Theme: Costs and Benefits

The Costs and Benefits sub-theme are around the trade-off between the perceived benefits of the security measures and their associated costs. The following codes are associated with this theme:
Price value: This a priori code, adopted from the UTAUT2 theory, refers to the cognitive choices that users make between the apparent benefits of utilizing a specific technology and the costs involved in using these technologies (Chaveesuk et al., 2022). Participants were more likely to use technology if they perceived that the benefits outweighed the costs.
Available mitigation measures and successfully enacted mitigation measures: this code is derived from the coping appraisal aspect of the PMT theory (Westcott et al., 2017). Participants were more likely to use technology if they perceived that effective mitigation measures were available and that they could successfully enact these measures.

3.4 Theme 2: Personal and Professional Experience in Information Security

The Personal and Professional Experience in Information Security theme is about the participants' cybersecurity experience. The following codes are associated with this theme:

Awareness after personal or family cybersecurity incidents: participants became more aware of cybersecurity after experiencing a personal or family cybersecurity incident. After such incidents, the participants realized the importance of using strong passwords, enabling two-factor authentication, and avoiding suspicious links and attachments.

Personal experience: participants expressed their experience with phishing emails and links while surfing the internet and phishing text messages.

Utilizing what one has learned at home in the workplace: Participants reported that they were able to apply what they had learned about cybersecurity at home to their work environment.

Work experience: participants reported that their work experience had helped them become more aware of cybersecurity risks and better equipped to protect themselves and their families.

Social influence (a priori code) due to job relevance: participants reported that they became more aware of cybersecurity when a family member or friend had an IT or information security background.
Job relevance (a priori codes) in the IT or information security field: participants reported that they became more aware of cybersecurity when they started working in the IT or information security field.

3.5 Sub-Theme: Necessity of Safeguard Measures and Attaining Trust

The Necessity of Safeguard Measures and Attaining Trust theme is about the necessity of employing safeguard measures to attain individuals' trust. The following codes are associated with this theme:

Anticipation of receiving an important email or message: the analysis revealed that anticipating an important email or message can make participants more vulnerable to phishing emails.
Email trustworthiness: participants also expressed the challenge of receiving phishing emails that appeared to be from a trusted entity.

Trust issues of third-party entities: participants expressed difficulties in knowing the legitimacy of received text messages from third-party entities.

3.6 Theme 3: Necessity of Education and Raising Awareness

The Necessity of Education and Raising Awareness theme is centered around the need for more education and awareness about cybersecurity. The following codes are associated with this theme:

False sense of security. Some participants showed a false sense of security and believed that their devices were secure and no safeguard measures were needed.

Ignoring awareness messages because of using two-factor authentication. Some participants ignored awareness messages because they thought they were not at risk.

Lack of installed protection software on mobile phones. Many participants did not have installed protection software on their mobile phones and were unaware of the need for that.

Lack of awareness. Some participants showed moderate knowledge about cybersecurity threats.

Use weak passwords because they are easy to remember. Some participants also reported using weak passwords because they were easy to remember.

Using weak passwords because of two-factor authentication. Some participants even used weak passwords because of two-factor authentication, which made them feel secure.

Fear of losing access to saved passwords and payment methods. Some participants did not use a password manager because they feared losing access to the saved passwords and payment methods if they forgot their master password.

In addition, future longitudinal studies could provide insights into how cybersecurity awareness changes over time and how it is influenced by various factors such as training, technological changes, or experiences with cyber threats.

Based on the findings of this study, programs could be developed and tested to enhance cybersecurity awareness. This could include training programs, awareness campaigns, or changes in organizational policies. Moreover, considering the language barrier limitation, conducting future research in native languages can provide valuable insights by allowing the participants to express their thoughts, experiences, and perceptions more accurately and completely. Last, future quantitative research should delve deeper than surface-level data and consider underlying meaning, factors, connections, or relationships that may skew the results. It is crucial not just to accept data at face value but also to delve into the hidden patterns and meanings. For example, in future quantitative research that will examine the demographic effects on cybersecurity awareness and practices, the researchers should consider that the users will likely employ weak passwords if the application does not store sensitive or payment-related information. Furthermore, the reliance on two-factor authentication may lead some users to believe that password strength is less important.

4. Interpretations and Implications

Theme 1: Perceived Safeguards and Threats

Interpretation

This theme suggests that the way individuals perceive cyber threats and the protective measures in place significantly shapes their cybersecurity behaviors. The perceived ease of use, the protection offered by these measures, and the severity of potential threats play pivotal roles in whether individuals adopt these measures. This indicates that perception plays a crucial role in shaping cybersecurity behaviors. For example, Juozapavičius et al. (2022) discussed the age and gender impact on password hygiene by examining a leaked customer database of a ride-sharing company. The authors overlooked the sensitivity of the data stored in the mobile application, a factor that could potentially skew the results. For example, several participants in this study said they would likely use a weaker password if the application did not store sensitive or payment-related information. This theme addresses the factors affecting cybersecurity awareness (Research Question 1).

Implication

This theme implies that understanding these perceptions can help in designing more effective cybersecurity measures and training programs. If security measures are perceived as user-friendly and practical, individuals are more likely to adopt them.

Conversely, if the consequences of a security breach are perceived as severe, individuals are more likely to take preventive measures. This highlights the need for user-friendly and effective cybersecurity measures.

Connection to Literature

This theme aligns with the PMT and TAM discussed in the literature review. PMT suggests that individuals' threat and coping appraisals influence their motivation to adopt protective behaviors. TAM posits that perceived ease of use and perceived usefulness are key determinants of technology acceptance.
However, the study's findings suggest that not all constructs of TAM2, TAM3, UTAUT, and UTAUT2 theories were significant, such as computer playfulness, voluntariness of use, age, and gender. This could be for a variety of reasons. For instance, certain constructs might be more relevant to specific types of technology or user groups. The context in which the technology is used could also play a role. It is also possible that the insignificant constructs are overshadowed by other more influential factors. These findings highlight the importance of not taking these models at face value, but rather, critically examining their applicability in different scenarios.

Sub-Theme: Costs and Benefits

Interpretation. This sub-theme suggests that individuals weigh the costs and benefits of using security measures. If the perceived benefits outweigh the costs, individuals are more likely to adopt the measures. One participant said about the free and premium antivirus software: "I don't trust the free [antivirus] because they have had some incidents before . . . I decided to go with the paid one." Another participant did not renew his antivirus subscription because of its cost and said, "for me. I had one last year, but the subscription ended [sic] and didn't renew."
This sub-theme provides insights into the factors influencing cybersecurity awareness (Research Question 1).

Implication. The implication is that cybersecurity measures need to be cost-effective and provide clear benefits to encourage adoption. For cybersecurity measures to be widely adopted, they need to strike a balance between cost and benefit. They should be affordable and manageable while providing a significant increase in security. Additionally, the benefits of these measures should be clearly communicated to encourage their adoption.

Connection to Literature. This sub-theme is related to the concept of response cost, response efficacy, and self-efficacy in PMT and price value in UTAUT2, suggesting that the perceived costs of protective actions can influence individuals' protection motivation.
The study's findings emphasize the significance of the aforementioned constructs.

Theme 2: Personal and Professional Experience in Information Security

Interpretation

This theme suggests that personal, family, and friends' experiences with cybersecurity incidents can lead to increased awareness and changes in behavior. One participant said: "there is incident was [*sic*] happened to me a long time ago. And from that incident, I started to be very conscious and aware of securing everything." Another participant said: "some of my friends, they're sharing their stories that they've been hacked before or something like that. So, now, I am more educated about it." Also, the theme suggests that the knowledge of cybersecurity obtained at home is applied in the workplace, and the knowledge obtained at work is similarly used at home. One participant said: "our IT department, they are always giving [*sic*] us warnings to avoid receiving this [*sic*] messages [spam emails] and block the sender and report them." The participant also said: "and the knowledge I took [*sic*] from my home, I use it in my work too. But I have to check and always ask a professional if the information is correct or not." Moreover, the theme suggests that age and gender do not play a significant role in one's understanding and awareness of cybersecurity. Instead, having a family member or friend working in the IT or information security field can enhance one's cybersecurity awareness. These individuals often share their knowledge and insights about the latest threats and protection measures, thereby indirectly educating their circle about cybersecurity. One participant with an IT background said: "usually, I'm the one who will give the awareness to my family, speak to my mother or my brother, my wife." Another participant said: "I have some friends and family members who [*sic*] work in IT or cybersecurity . . . and they always advise us."

In addition, professionals working in IT or information security-related fields have a higher level of cybersecurity awareness due to their job requirements. They are exposed to various cybersecurity issues and solutions as part of their daily work, which keeps them updated and informed about the latest trends and threats in the cybersecurity landscape. One participant said: "so I started [to be aware of cybersecurity] since I started working in the IT field."

This theme addresses the factors affecting cybersecurity awareness (Research Question 1). It also addresses the cultural and social factors that affect cybersecurity awareness (Research Question 2) and the demographic factors that affect cybersecurity awareness (Research Question 3).

Implication

Experiencing a cyber threat firsthand, such as a phishing attack or a malware infection, can be a wake-up call. It highlights the importance of cybersecurity measures and encourages individuals to educate themselves about safe online practices. Also, cybersecurity awareness is not confined to a particular age group or gender. It is influenced more by personal experiences, professional exposure, and the social circle one is part of if this circle has a background in IT or information security.

Connection to Literature

This theme is aligned with the "job relevance" construct of TAM2 and TAM3. It is also aligned with the "social influence" construct of UTAUT and UTAUT2. Although TAM2, TAM3, UTAUT, and UTAUT2 include an "experience" construct, this study's "experience" context differs. The theories define the "experience" construct as "the passage of time from the initial use of a technology by an individual" (C. C. Lee et al., 2021, p. 104). In this study, "experience" is more about personal encounters. Nonetheless, this theme is aligned with Hanna (2020), which suggests cybersecurity awareness and workplace training programs can improve cybersecurity measures at home. This theme is also aligned with the Y. Li and Siponen (2011) study, where the authors state that security awareness among individuals is frequently accompanied by panic after encountering threats such as viruses or losing data. However, the study's findings suggest that "social influence" and "job relevance" are interconnected rather than separate constructs. Moreover, the findings can explain the contradictions among several studies about the effects of demographic factors on cybersecurity awareness and practices. Cybersecurity awareness is not confined to a particular age group or gender, but rather, it is more influenced by individual experiences, professional interactions, and the influence of one's social network, especially if that network includes individuals with expertise in IT or information security. Therefore, it is crucial for quantitative researchers not to take the result at face value, but rather, critically examine the underlying causes or beliefs.

Sub-Theme: Necessity of Safeguard Measures and Attaining Trust

Interpretation. This theme suggests that trust in safeguard measures and their provider is crucial for their adoption and use. Individuals are more likely to embrace cybersecurity measures that they perceive as trustworthy. Participants often encountered emails that seemed to be from official parties. These emails, skillfully mimicking the style and tone of official communications, can be misleading. Distinguishing these deceptive emails from genuine ones remains a challenge for many participants. Similarly, participants also expressed difficulty in determining the legitimacy of text messages they received. Malicious actors increasingly use text messages to trick individuals into revealing sensitive information or downloading malware. For example, several participants complained about the emails and text messages that they received that appeared to be from the Saudi Post.

Implication. Trust is a crucial factor in the adoption of cybersecurity measures. By focusing on reliability, reputation, and transparency, providers can enhance the trustworthiness of their cybersecurity measures and encourage wider adoption.

Connection to Literature. While several studies, including those by Cai et al. (2023), Eneizan et al. (2019), and Hooda et al. (2022), had integrated the "trust" construct into the UTAUT framework to explain the behavioral intention and usage behavior, the context of "trust" in this study differs. In the aforementioned studies, "trust" is viewed in the context of a compromise that emerges from an assessment of advantages and disadvantages. However, in this study, "trust" is contextualized as fostering confidence amid situations characterized by uncertainty and vulnerability.

In addition, this will allow other researchers to assess the potential for applying such findings to their own research contexts.

Theme 3: Necessity of Education and Raising Awareness

Interpretation

This theme suggests that there is a need for more education and awareness about cybersecurity. A lack of awareness or a false sense of security can lead to risky behaviors.

Some participants had a false sense of security, believing that using an iPhone ensured their safety and that there was no need for additional protective measures. For instance, a probing question arose regarding the type of security software installed on mobile phones. Several participants indicated they had none, attributing this to their use of an iPhone. One participant even expressed concern about whether malicious actors could access their credit card information while they were using public wireless access points on their iPhones. For example, according to Kotliar and Carmi (2023), Pegasus is a type of spyware that has been installed on devices running the iOS and Android operating systems from Apple and Google. It was used to infiltrate the phones of activists and journalists.

Additionally, one participant was using a weak password under the assumption that it would be sufficient due to their use of two-factor authentication. Moreover, some participants avoided using a password manager due to concerns about forgetting

the master password and subsequently losing access. This indicates that education and awareness are crucial in shaping cybersecurity behaviors. This theme addresses the factors affecting cybersecurity awareness (Research Question 1).

Implication

There is a need for more comprehensive and effective cybersecurity education and awareness programs. These programs can help individuals understand the risks associated with cyber threats and the importance of taking preventive measures. This highlights the need for effective cybersecurity education and awareness programs.

Connection to Literature

Cybersecurity awareness and training programs play a vital role in the defense against cyber threats. This aligns with other studies, such as Alzubaidi (2021), Hanna (2020), and Quayyum et al. (2021). However, the study's findings suggest tailoring training programs and awareness campaigns to address the root causes of risky behaviors, misconceptions about cybersecurity, and the false sense of security that can lead to risky behaviors.

5. Limitations

One significant limitation of the study was the language proficiency of the participants. The study was conducted in English with participants who were not native English speakers and were not fluent in the language. This could have potentially influenced the results.

Participants might have found it challenging to fully express their thoughts, experiences, and perceptions in English, which could have led to nuances being lost in translation. This language barrier might have also affected their comprehension of the questions or discussions. In addition, the study's findings are context-specific. Their unique experiences, backgrounds, and current circumstances influenced the participants' responses, which might not apply to other individuals or settings. Therefore, caution should be exercised when extrapolating these findings to different contexts or populations. Also, since the study was conducted in Saudi Arabia, the findings might be influenced by specific cultural factors unique to this region. This could limit the applicability of the results to other cultural contexts.

6. Recommendations for Future Research

This study provides valuable insights into the factors influencing cybersecurity-related behavior. The themes and sub-themes identified in this study could be a useful starting point for future research in different contexts or populations. Future research could further explore the transferability of these findings by conducting similar studies in different organizational, cultural, and linguistic contexts. This would not only validate the findings of this study but also contribute to a more nuanced understanding of the factors influencing cybersecurity-related behavior. Moreover, future research could include employees from different organizations, industries, or countries to enhance the transferability of the findings. In addition, future longitudinal studies could provide insights into how cybersecurity awareness changes over time and how it is influenced by various factors such as training, technological changes, or experiences with cyber threats. Based on the findings of this study, programs could be developed and tested to enhance cybersecurity awareness. This could include training programs, awareness campaigns, or changes in organizational policies. Moreover, considering the language barrier limitation, conducting future research in native languages can provide valuable insights by allowing the participants to express their thoughts, experiences, and perceptions more accurately and completely. Last, future quantitative research should delve deeper than surface-level data and consider underlying meaning, factors, connections, or relationships that may skew the results. It is crucial not just to accept data at face value but also to delve into the hidden patterns and meanings. For example, in future quantitative research that will examine the demographic effects on cybersecurity awareness and practices, the researchers should consider that the users will likely employ weak passwords if the application does not store sensitive or payment-related information. Furthermore, the reliance on two-factor authentication may lead some users to believe that password strength is less important.

References

Abu-Alhaija, M. (2020). Cyber security: Between challenges and prospects. ICIC Express Letters Part B: Applications 11(11), cha 1019–1028. https://doi.org/10.24507/icicelb.11.11.1019

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction, 29*(3), 701–750. https://doi.org/10.1007/s11257-019-09236-5

Ahmad, S., Wasim, S., Irfan, S., Gogoi, S., Srivastava, A., & Farheen, Z. (2019). Qualitative v/s. quantitative research—a summarized review. *Journal of Evidence-Based Medicine and Healthcare*, *6*(43), 2828–2832. https://doi.org/10.18410/jebmh/2019/587

Ali, N. (2023). Influence of Data-Driven Digital Marketing Strategies on Organizational Marketing Performance: Mediating Role of IT Infrastructure. In: Yaseen, S.G. (eds) Cutting-Edge Business Technologies in the Big Data Era. SICB 2023. *Studies in Big Data, vol 135. Springer, Cham*. https://doi.org/10.1007/978-3-031-42463-2_31

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, *13*(9), 5700. https://doi.org/10.3390/app13095700

Alsmadi, D., Maqousi, A., & Abuhussein, T. (2022). Engaging in cybersecurity proactive behavior: Awareness in COVID-19 age. *Kybernetes*. https://doi.org/10.1108/k-08-2022-1104

Al-Soud, A., Al Dweri, K., & Al Dweri, K. (2024). Exploring the landscape of cyber crimes targeting women: A literature review on cyber security laws. Al-Balqa Journal for Research and Studies, 27(2), 272–290 . https://doi.org/10.35875/04x1hz93

Alzighaibi, A. R. (2021). Cybersecurity attacks on academic data and personal information and the mediating role of education and employment. *Journal of Computer and Communications*, *9*(11), 77–90. https://doi.org/10.4236/jcc.2021.911006

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon, 7*(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

An, Q., Hong, W. C. H., Xu, X., Zhang, Y., & Kolletar-Zhu, K. (2022). How education level influences internet security knowledge, behaviour, and attitude: A comparison among undergraduates, postgraduates and working graduates. *Research Square*. https://doi.org/10.21203/rs.3.rs-1977578/v1

Archibald, M. M., Ambagtsheer, R. C., Casey, M., & Lawless, M. (2019). Using Zoom videoconferencing for qualitative data collection: Perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods*, *18*, 160940691987459. https://doi.org/10.1177/1609406919874596

Cai, L., Yuen, K. F., & Wang, X. (2023). Explore public acceptance of autonomous buses: An integrated model of UTAUT, TTF and trust. *Travel Behaviour and Society*, *31*, 120–130. https://doi.org/10.1016/j.tbs.2022.11.010

Castillo-Vergara, M., Alvarez-Marin, A., Pinto, E. C., & Valdez-Juárez, L. E. (2022). Technological acceptance of Industry 4.0 by students from rural areas. *Electronics*, *11*(14). https://doi.org/10.3390/electronics11142109

Chaveesuk, S., Khalid, B., Bsoul-Kopowska, M., Rostańska, E., & Chaiyasoonthorn, W. (2022). Comparative analysis of variables that influence behavioral intention to use MOOCs. *PLOS ONE*, *17*(4), e0262037. https://doi.org/10.1371/journal.pone.0262037

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2017). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers, 21*(3), 719–734. https://doi.org/10.1007/s10796-017-9774-y

Eneizan, B., Mohammed, A. G., Alnoor, A., Alabboodi, A. S., & Enaizan, O. (2019). Customer acceptance of mobile marketing in Jordan: An extended UTAUT2 model with trust and risk factors. *International Journal of Engineering Business Management*, *11*. https://doi.org/10.1177/1847979019889484

Eyisi, D. (2016). The usefulness of qualitative and quantitative approaches and methods in researching problem-solving ability in science education curriculum. *Journal of Education and Practice*, *7*(15), 91–100. (EJ1103224). ERIC. http://files.eric.ed.gov/fulltext/EJ1103224.pdf

Fidler, C. S., Kanaan, R. K., & Rogerson, S. (2011). Barriers to e-Government Implementation in Jordan: The Role of Wasta. *International Journal of Technology and Human Interaction (IJTHI), 7*(2), 9-20. http://doi.org/10.4018/jthi.2011040102

Guest, G., Namey, E., & McKenna, K. (2016). How many focus groups are enough? Building an evidence base for nonprobability sample sizes. *Field Methods*, *29*(1), 3–22. https://doi.org/10.1177/1525822x16639015

Hanna, M. (2020). *Exploring cybersecurity awareness and training strategies to protect information systems and data* [Doctoral dissertation, Walden University]. Walden Dissertations and Doctoral Studies Collection. https://scholarworks.waldenu.edu/dissertations/8902

Hooda, A., Gupta, P., Jeyaraj, A., Giannakis, M., & Dwivedi, Y. K. (2022). The effects of trust on behavioral intention and use behavior within e-government contexts. *International Journal of Information Management*, *67*, 102553. https://doi.org/10.1016/j.ijinfomgt.2022.102553

Jamil, H. (2022). *Factors affecting users cybersecurity practices: A study of Australian microbusinesses* [Doctoral dissertation, Charles Sturt University]. Charles Sturt University Research Output. https://researchoutput.csu.edu.au/ws/portalfiles/portal/290130889/Factors_Affecting_Users_Cybersecurity_Practices_A_Study_of_Australian_Microbusinesses.pdf

Juozapavičius, A., Brilingaitė, A., Bukauskas, L., & Lugo, R. G. (2022). Age and gender impact on password hygiene. *Applied Sciences, 12*(2), 894. https://doi.org/10.3390/app12020894

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security*. https://doi.org/10.1108/ics-08-2022-0139

Kotliar, D. M., & Carmi, E. (2023). Keeping Pegasus on the wing: Legitimizing cyber espionage. *Information, Communication & Society*. https://doi.org/10.1080/1369118x.2023.2245873

Krueger, R., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research* (5th ed.). SAGE.

Lee, C. C., Ruane, S., Lim, H. S., Zhang, R., & Shin, H. (2021). Exploring the behavioral intention to use collaborative commerce: A case of Uber. *Journal of International Technology and Information Management*, 30(5), 97–119. https://doi.org/10.58729/1941-6679.1545

Li, Y., & Siponen, M. T. (2011). A call for research on home users' information security behaviour. *Pacific Asia Conference on Information Systems*, 112. https://aisel.aisnet.org/pacis2011/112/

Morgan, D. L., & Hoffman, K. (2018). Focus groups. In U. Flick (Ed.), *The SAGE handbook of qualitative data collection* (pp. 250–263). SAGE.

Mou, J., Cohen, J. B., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach in search advertising. *Journal of the Association for Information Systems*, *23*(1), 196–236. https://doi.org/10.17705/1jais.00723

Ng, K. C., Zhang, X., Thong, J. Y., & Tam, K. Y. (2021). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems*, *38*(3), 732–764. https://doi.org/10.1080/07421222.2021.1962601

Nguyen, T. N. M., Whitehead, L., Dermody, G., & Saunders, R. (2021). The use of theory in qualitative research: Challenges, development of a framework and exemplar. *Journal of Advanced Nursing*, *78*(1).

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1–13. https://doi.org/10.1177/1609406917733847

QSR International. (2022). *Best transcription software for audio & video for research | NVivo*. https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/about/nvivo/modules/transcription

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Saldana, J. (2013). *The coding manual for qualitative researchers* (2nd ed.). SAGE.

Singh, S., Sahni, M. M., & Kovid, R. K. (2020). What drives FinTech adoption? A multi-method evaluation using an adapted technology acceptance model. *Management Decision*, *58*(8), 1675–1697. https://doi.org/10.1108/md-09-2019-1318

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–Information security compliance and violation behaviour in organisations: A systematic review. *Social Sciences*, *11*(9), 386. https://doi.org/10.3390/socsci11090386

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1533

Westcott, R., Ronan, K., Bambrick, H., & Taylor, M. (2017). Expanding protection motivation theory: Investigating an application to animal owners and emergency responders in bushfire emergencies. *BMC Psychology, 5*(13), 1–14. https://doi.org/10.1186/s40359-017-0182-3

Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International Management Review, 15*(1), 45–55.

Yaseen, S.G. & El Qirem, I.A. (2018). Intention to use e-banking services in the Jordanian commercial banks. *International Journal of Bank Marketing, 36*(3), 557-571. https://doi.org/10.1108/IJBM-05-2017-0082.