scientific reports

Check for updates

OPEN

Information security behavior of healthcare professionals in the Sultanate of Oman based on the PMT model

A. Al Toobi & M. Al Suqri

Protecting sensitive information is critical in healthcare. Healthcare professionals (HCPs) must adhere to information security rules to safeguard patient information and maintain the integrity of healthcare systems. This study explores the impact of the Protection Motivation Theory (PMT) on the information security behavior of HCPs in the Sultanate of Oman's MOH hospitals. This study uses a quantitative research design to assess information security behaviors of HCPs using PMT factors, including perceived severity, perceived vulnerability, maladaptive rewards, response efficacy, self-efficacy, and response costs. A standardized questionnaire was used to collect data from a sample of HCPs in MOH hospitals in the Sultanate. The study found that perceived severity and response efficacy significantly influence HCPs' motivation to engage in secure practices. Maladaptive rewards did not affect security behavior, likely due to a robust organizational culture and effective training programs. Response costs positively influenced security behaviors, suggesting that effective communication, balancing response costs, and leveraging organizational culture can foster a more substantial commitment to information security. The study highlights the importance of threat and coping appraisal in HCPs' security protocols, emphasizing the need for tailored interventions and ongoing education to foster a security culture.

Keywords Healthcare professionals, Information security, Protection motivation theory, Sultanate of oman, Security, Behavior

The widespread adoption of electronic health records (EHRs), growing regulatory demands, and the increasing need for data exchange among healthcare stakeholders have made robust security measures essential[1]. Although EHRs streamline the storage and exchange of patient information, they also bring significant security challenges, as stated by Folasole[2]. The healthcare sector has become an increasingly frequent target for cyberattacks, mainly due to the high value of patient data and other sensitive information it manages[3,4]. Khan[4] and Triplett[5] emphasized that threats such as ransomware and phishing attacks can lead to severe financial losses, disruptions to healthcare operations, and significant breaches of patient privacy. Cartwright[6] justified that the widespread use of EHRs and Internet of Medical Things (IoMT) devices has further broadened the attack surface, exposing new vulnerabilities. On average, Rai[3] reported that healthcare organizations worldwide experience approximately 1,463 cyberattacks per week, a situation exacerbated by persistent underinvestment in cybersecurity[6]. Addressing these threats requires a comprehensive strategy that includes frequent system updates, strong data encryption, staff training, and advanced threat detection technologies[4,5]. The COVID-19 pandemic has only intensified the sector's vulnerability, underscoring the urgent need for more effective and resilient cybersecurity defenses[6].

Safeguarding sensitive information is paramount in healthcare. Information security protocols implemented by healthcare professionals (HCPs) are critical in protecting patient information and maintaining the integrity of healthcare systems. Prior studies[7–9] have investigated several factors that impact information security behaviors, including variables related to the Protection Motivation Theory (PMT). The study of these behaviors in the context of the Sultanate of Oman is particularly relevant, given the Sultanate's distinctive cultural and technological environment. The health sector in the Sultanate of Oman, like many countries worldwide, is rapidly moving into digital media. As healthcare facilities use modern information technology, the demand for robust information security policies grows. However, it is essential to emphasize that, despite technological advancements, the human factor remains vital in ensuring information security. Through their behaviors, attitudes, and beliefs,

Department of Information Studies, Sultan Qaboos University, Muscat, Oman. email: asiaaltoobi@gmail.com

they play an essential role in maintaining the integrity and confidentiality of patient information. Understanding and influencing these aspects is crucial for adequate information security in the healthcare sector.

However, PMT offers a comprehensive framework for understanding the cognitive processes that underlie individuals' protective behaviors. PMT, as defined by Rogers[10] and Maddux and Rogers[11] posits that several cognitive appraisals influence individuals' motivation to protect themselves from threats: perceived severity and vulnerability of the threat, maladaptive rewards (the perceived benefits of not adopting the protective behavior), response efficacy (belief in the effectiveness of the protective behavior), self-efficacy (confidence in one's ability to perform the protective behavior), and response cost (perceived barriers to performing the protective behavior). By analyzing these variables, researchers can gain insights into the factors that drive healthcare professionals' information security behaviors.

Statement of the problem

Healthcare organizations are increasingly becoming prime targets for cyberattacks due to the vast amount of sensitive information they handle, including personal and medical records. In the Sultanate of Oman, the rapid digital transformation of the healthcare sector has not been matched with a corresponding increase in robust cybersecurity measures. This gap leaves healthcare institutions vulnerable to breaches, potentially compromising patient confidentiality, data integrity, and service availability. Despite this critical issue, a dearth of research focuses on the security behaviors of HCPs in the Sultanate of Oman. Understanding and improving these behaviors is essential to mitigating risks and protecting sensitive health information. Although cybersecurity research in healthcare has expanded, non-technological elements, such as human-based and organizational aspects, still require further study, underscoring the need for future research on physical security[12]. More research is needed on healthcare information security in the Sultanate of Oman. The need for research into information security is evident, and as a result, a significant gap remains in our understanding. This study aims to fill that gap.

Study aims and objectives

This study uses PMT to evaluate the information security behaviors of HCPs in the Sultanate of Oman. It assesses the impact of perceived vulnerability, severity, rewards, response efficacy, self-efficacy, and response costs on these actions.

Significance of the study

Understanding HCP security behaviors is essential because it addresses significant gaps in protecting sensitive patient data, which is critical for retaining trust and providing high-quality treatment. The findings will help policymakers and healthcare administrators in the MOH in the Sultanate of Oman build focused interventions and training programs to improve information security and secure patient data. This research supports the development of a robust security culture within healthcare facilities, thereby reducing the risk of data breaches and fostering an environment that prioritizes patient safety and operational efficiency.

Theoretical background

Understanding the theoretical basis of information security behavior will provide a more systematic approach to studying people's behaviors that either protect or compromise information security. Theoretical frameworks have facilitated an in-depth understanding of the cognitive, emotional, and social factors that influence decisions related to security, enabling researchers and practitioners to develop more effective interventions. A significant strand of research covers using behavioral models to understand and predict compliance intentions. Researchers have examined conceptual frameworks within various disciplines, including psychology, criminology, and public health[13]. Towbin[14] has argued that the technological acceptance model (TAM), theory of planned behavior TPB, and unified theory of use and acceptance of technology (UTAUT) are some of the frameworks used in assessing implementation programs, specifically information technology. According to Lebek[15], theoretical approaches dominating information security include a theory of planned behavior (TPB), the theory of reasoned action (TRA), the general deterrence theory (GDT), the protection motivation theory (PMT), and the TAM. The present study confirmed that TRA/TPB, GDT, TAM, and PMT are the most applied behavior-based security theories.

Protection motivation theory

Rogers proposed PMT in 1975 and extended the model in 1983. The theory is a psycho-social hypothesis that describes reasons for one's protective behavior against hazards. For some time, the PMT has remained among the most widely used theories in the study of health-related behaviors, such as individual responses to health hazards. The model has been used in formulating and testing intervention programs aimed at safe online security behaviors. It describes how, when faced with risk, a person evaluates it and alternative solutions before deciding whether to respond adaptively or in an ill-adapted manner[16].

According to Ma[17], the PMT was designed as a behavioral science theory to anticipate and clarify the behaviors impacted by a person's threat appraisal (how exciting and frightening a lousy result is) and coping appraisal (how effective the risk-reduction activity is). Threat appraisal factors include maladaptive response rewards, both intrinsic and extrinsic, as well as perceived threat severity and vulnerability. Floyd et al.[18] stated that reward variables enhance the likelihood of engaging in maladaptive behavior, while threat factors lower it. People will examine how severe the effects of the threat are (perceived severity) and the possibility of the danger materializing in a way that directly affects them (perceived vulnerability) in PMT threat appraisal. This threat appraisal may lead to maladaptive actions, such as denial or avoidance[19]. Factors influencing copying appraisal include response efficacy, self-efficacy, and response costs, which determine whether people will examine whether implementing a recommended course of action will reduce the threat (response efficacy) and their

degree of confidence in carrying out that action (self-efficacy) in their coping appraisal[11]. This appraisal may result in adaptive actions if the costs of developing an adapted response (response costs) are low. The schematic presentation of the PMT and its constructions, adapted from Floyd et al.[18], is illustrated in Fig. 1.

Therefore, PMT has recently been employed and verified as the foundational theory in numerous studies[9,20,21] related to information security in organizations. However, according to[22,23], the PMT is the most relevant theoretical framework to analyze the factors leading to medical professionals' non-compliance with organizational security requirements for using personal mobile devices. Haag and colleagues[24] argued that researchers increasingly use PMT to understand information system security behavior. In contrast, Li et al.[25] believed that PMT is a widely recognized theoretical framework for analyzing and evaluating the recommended behaviors or measures essential for reducing the damage caused by threats.

Review of literature

Information security in healthcare has been well recognized due to the sensitivity of patient information and the potential implications of security breaches. Understanding the factors that influence the information security behaviors of healthcare professionals is crucial for developing practical solutions to address these behaviors. PMT provided a sound framework for investigating these behaviors, focusing on the cognitive processes that lead individuals to protect themselves against threats. Indeed, several works have extended the application of PMT to various fields, including health-related behaviors and information security, as seen in studies by[7,8,18,26–29]. However, there is a relative scarcity of research that explicitly studies the information security behaviors of HCPs, especially within the unique cultural and organizational environment of the Sultanate of Oman.

According to Floyd et al.[18], threat appraisal in PMT is a user's criterion for choosing a specific coping strategy. The primary threat appraisal constructs are perceived vulnerability and perceived severity. Likely, Johnston et al.[26] demonstrated that perceived vulnerability significantly influences individuals' intentions to engage in information security behaviors. Their study, grounded in the PMT, found that higher levels of perceived vulnerability led to stronger intentions to adopt protective measures in information security contexts. In information security, the perceived severity of breaches has been shown to influence compliance behaviors[7]. Research indicates that when people view a threat as both severe and likely to affect them personally, they are more inclined to take preventive action[30]. Conversely, Thompson[31] stated that threat depression—when individuals minimize or dismiss the seriousness of a threat—can weaken security responses, underscoring the need for accurate threat appraisal. Therefore, HCPs recognizing the severe consequences of security breaches are expected to exhibit more robust information security behaviors[8]. Maladaptive rewards, such as increased efficiency or reduced workload from circumventing security procedures, may reward non-compliant behavior[32]. Likely, Almansoori et al.[33] demonstrated that perceived rewards for non-compliance and the effort or cost associated with protective actions significantly shape security behavior. When individuals perceive more benefits in ignoring security protocols or find protective measures too burdensome, they are less likely to engage in secure practices. Hence, HCPs who perceive significant benefits related to violating security procedures are expected to exhibit a lower intention to comply with information security practices[8].

Specifically, Bandura[34] describes self-efficacy as the belief an individual has in their ability to perform the required behaviors to realize specified results. The concept of self-efficacy is crucial in motivating individuals to initiate and sustain specific behaviors[35]. Concerning information security, Ifinedo[7] reported that high levels of self-efficacy are exhibited with high compliance with security policies. Additionally, Borgert et al.[36] and Thompson et al.[31] reported that high self-efficacy supports both problem-focused and emotion-focused coping, resulting in better overall security outcomes. It is expected, therefore, that health professionals who are confident of their ability to perform information security behaviors successfully will be more likely to engage in those behaviors. On the other hand, however, empirical investigations have also demonstrated that the perceived

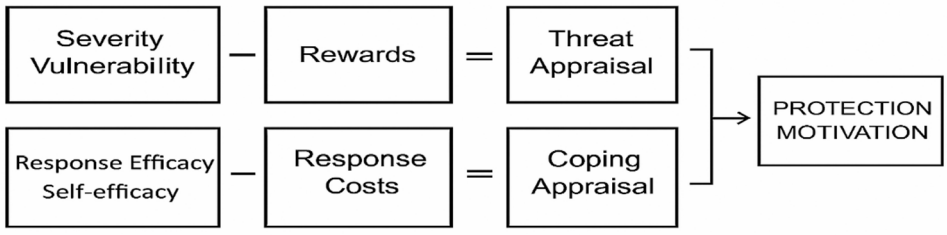

Fig. 1. Schematic presentation of the PMT constructs. Source: Adapted from Floyd et al.[18]

costs of acting can significantly discourage individuals from engaging in recommended protective behaviors[37]. Healthcare professionals who perceive information security protocols as cumbersome or time-intensive might exhibit lower levels of adherence to these procedures[8].

PMT has been extensively applied in healthcare settings to explore and predict a wide range of health-related behaviors. For example, it has been instrumental in examining COVID-19 preventive behaviors among healthcare providers in Saudi Arabia, where self-efficacy emerged as the most influential factor driving intentions to follow preventive guidelines[38]. In the context of information security, Sreenath et al.[39] emphasized that PMT has demonstrated strong predictive capabilities, outperforming Technology Threat Avoidance Theory in a study on healthcare professionals' security behaviors, which explained 60% of the variance in security intentions.

Additionally, Sari et al.[40] demonstrated that self-efficacy, perceived severity, and attitudes are the most common individual elements influencing security behavior. Management support and company culture are other important aspects to consider. In contrast, Yeng et al.[41,42] reported that work-related variables, such as busyness and emergencies, may compromise security practices. Additionally, personality factors such as conscientiousness and agreeableness have been linked to security behavior hazards[40]. The study by Yeng et al.[42] revealed discrepancies between staff information security awareness and self-reported conscious care behavior, with approximately half of the respondents residing in a high-risk zone.

Recent research further supports these findings by extending PMT across various contexts, devices, and populations, including its integration with data-driven approaches to improve out-of-sample predictive accuracy. For example, SEM–AI hybrid models have demonstrated that self-efficacy and response efficacy are the most powerful drivers of secure behaviors, while response costs negatively impact protective intentions[29,43]. PMT-based interventions have also been evaluated in security training and awareness programs, where frameworks such as the Kirkpatrick model have shown significant improvements in behavioral intentions by enhancing self-efficacy[44]. More recent experimental studies (2025) reveal that response efficacy messages are more effective than self-efficacy messages in influencing specific behavioral outcomes. However, the gap between reported and actual behavior remains a challenge[45,46].

Furthermore, research highlights the crucial role of contextual factors, including the digital divide and socioeconomic status, in shaping individuals' ability to assess threats and adopt effective coping strategies. This underscores the need for interventions that address structural constraints[47,48]. Current PMT applications have expanded to address emerging issues, including how security perceptions influence technology adoption among older adults, integrating PMT-based interventions into organizational culture, and utilizing PMT for real-time behavioral nudges[49–51].

This review underscores the scarcity of research applying Protection Motivation Theory (PMT) within healthcare settings in the Gulf region, particularly in the Sultanate of Oman. Although e-health studies have expanded across Gulf Cooperation Council (GCC) countries, a notable lack of controlled interventional research and limited exploration of gender and religious considerations remain[52]. In the Sultanate of Oman, existing studies have primarily focused on public awareness and attitudes toward genetic disorders and premarital screening, highlighting significant gaps in health education and promotion efforts[53,54]. Despite the availability of free premarital screening services, participation rates remain low, highlighting the need for targeted community-based awareness campaigns[54]. Research on autism in the Gulf, including in Qatar and Oman, has also highlighted ongoing healthcare challenges and the importance of public engagement in informing policy and resource allocation[55]. Nonetheless, the direct application of PMT in these areas has yet to be thoroughly investigated. Therefore, exploring the limited application of PMT in Gulf healthcare settings—especially in Oman—is essential for gaining deeper insight into the behavioral factors that shape security practices among HCPs. Such research can help design more effective strategies and interventions to enhance the protection of sensitive health information.

This study helps bridge the existing gap by applying PMT to explore how HCPs in Oman respond to security threats related to EHRs. By uncovering the psychological and contextual factors that influence their behavior, the research provides practical insights for developing more effective security policies, training programs, and protective measures tailored to the local healthcare environment.

A summary of key PMT-based studies, including their context, methodologies, main findings, and relevance to the current study, is presented in Table 1 below.

Methodology

This study investigates information security practices by HCPs in the Sultanate of Oman, focusing on factors derived from the Protection Motivation Theory. This study shall investigate perceived vulnerability, perceived severity, maladaptive rewards, response efficacy, self-efficacy, and response cost regarding their impact on the security behaviors of HCPs. These components are crucial in understanding the motivations and deterrents of driving secure or insecure practices across healthcare settings. In so doing, the study aims to contribute to the understanding of how best to improve the information security behavior of the HCPs.

Method

To gather data from the healthcare professionals working in the MOH hospitals of Oman, a structured questionnaire was used. The questionnaire was designed based on renowned literature in the field, such as[7,8,26] and was first tested for clarity and validity on a small group of healthcare professionals. The final questionnaire was distributed via both electronic media, such as email, and in hard copy form to increase the response rate. The measurement instrument included 37 items divided into three parts: (a) demographic information, (b) PMT variables of perceived severity, vulnerability, maladaptive rewards, response efficacy, self-efficacy, and response cost, and (c) security behavior.

Author (s) & year	Study context	Theory/model	Key constructs	Methodology	Main findings	Relevance to current study
Ifinedo (2012)	IS Security Policy Compliance	PMT + TPB	Threat & Coping Appraisal, Self-efficacy, Response Efficacy	Survey (Quantitative)	Perceived severity & self-efficacy predict compliance	Supports PMT in organizational security behavior
Hearth & Rao (2009)	Security Policy Compliance	PMT + Deterrence Theory	Threat Appraisal, Sanctions	Theoretical + Conceptual	Combines PMT with deterrence for security compliance	Provides a hybrid framework for compliance
Floyd, Prentice-Dunn & Rogers (2000)	Meta-analysis of PMT Research	PMT	Threat appraisal, Coping appraisal	Meta-analysis	PMT widely effective for predicting protective behaviors	Establishes PMT validity
Johnston, Warkentin& Siponenal (2015)	Fear Appeals in IS Security	PMT + Rhetorical Framework	Fear appeal, Severity, Vulnerability	Conceptual + Empirical Validation	Strong fear appeals increase compliance	Relevant for designing security messages
Khan, Murtaza, Malik, Mahmood & Asadi (2025)	Smartphone Security	PMT + SEM-AI	Self-efficacy, Response Efficacy, Response Cost	SEM + AI predictive modeling	Coping appraisal strongly predicts security behavior	Highlights the predictive power of PMT constructs
Kiran, Khan, Murtaza, Farooq & Pirkkalainen (2025)	Cybersecurity Behaviors	PMT	Threat Appraisal, Coping Appraisal	Quantitative (Modeling)	PMT predicts behavior effectively across contexts	Validates PMT for cybersecurity
Khan, Ikram, Murtaza & Javed (2023)	Cybersecurity Awareness Training	PMT + Kirkpatrick	Self-efficacy, Response Efficacy	Experimental + Evaluation	Training improves coping appraisal, and behavior	Shows intervention effectiveness
Simon et al. (2025)	Password Creation Behavior	PMT	Self-efficacy vs. Response Efficacy	Longitudinal Experiment	Response-efficacy messages are more effective than self-efficacy	Messaging framing in interventions
van't Hoff-de Goede et al. (2025)	Online Self-protective Behavior	PMT	Threat & Coping Appraisal	Survey Experiment	PMT predicts reported and actual online behavior	Confirms PMT applicability in real behavior
Khan, Ikram & Saleem (2023a)	Developing country – general cybersecurity behaviors	PMT + Socioeconomic Factors	Threat appraisal, Coping appraisal, Socioeconomic & digital inequalities	Survey	Socioeconomic and digital inequalities significantly affect cybersecurity behaviors and PMT pathways	Highlights the importance of contextual factors in PMT application for developing countries
Khan, Ikram & Saleem (2023b)	University students – smartphone security	PMT	Digital divide, Socioeconomic status, Threat & Coping appraisal	Survey/ Empirical	Socioeconomic differences significantly influence smartphone security behavior; PMT constructs mediate behavior	Supports the role of PMT and socioeconomic context in shaping protective behaviors among young adults
Kanimozhi et al. (2025)	Aging Population & Digital Threats	PMT	Perceived Threat, Vulnerability	Survey	Higher threat perception influences safe usage	Highlights demographic-specific factors
Khadka & Ullah (2025)	Human Factors in Cybersecurity	Interdisciplinary Framework	Cognitive, Social, Behavioral	Literature Review	Human behavior is central to security risks	Provides a comprehensive behavioral perspective
Zou et al. (2024)	Password Change Behavior	PMT	Fear, Threat, Coping Appraisal	Experimental Study	PMT-based interventions encourage password updates	Practical application of PMT in user behavior

Table 1. Summary of literature on PMT and information security behavior.

Role \ hospital	Royal	Nizwa	Ibri	Sohar	SQH	Al Buraimi	Khasab	Hima	Sur	Al Rustaq	Ibra	Total
Doctors	31	12	8	15	16	5	3	1	7	9	7	**114**
Nurses	96	34	20	43	50	14	4	2	18	29	21	**331**

Table 2. Study sample distributed in the MOH Governorate hospitals.

Study sample

The study sample consists of HCPs, including doctors and nurses, working in central government hospitals of the Ministry of Health in the Sultanate of Oman across all 11 governorates. According to MOH's annual report[56], the overall number of doctors, including medical administrators, consultants, specialists, and general practitioners, was 9,960, while there were 14,460 nurses throughout the Sultanate. There were approximately 2,271 doctors and 6,615 nurses in the sample hospitals of the governorate. Given accessibility to all participants and their size, it would be difficult, if not impossible, to sample the entire population; as a result, a sampling technique is necessary. Therefore, cluster random sampling probability was used in this study, where the diverse population shares one or more similar traits[57]. The representative sample is 5%, which corresponds to a 95% confidence level and a margin of error of approximately 2% for the total population of 114 doctors and 331 nurses. These are clustered by the hospital and are shown in Table 2.

Study hypothesis

According to the PMT, we hypothesize that:

H1: Higher levels of perceived vulnerability will positively influence HCPs' information security behaviors in the Sultanate of Oman.

H2: Higher levels of perceived severity will positively influence HCPs' information security behaviors in the Sultanate of Oman.

H3: Negative reward perceptions from insecure behaviors will negatively impact HCPs' information security behavior in the Sultanate of Oman.

H4: Higher levels of response efficacy will positively influence HCPs' information security behaviors in the Sultanate of Oman.

H5: Higher self-efficacy will positively influence HCPs' information security behaviors in the Sultanate of Oman.

H6: Higher perceived response costs will negatively influence HCPs' information security behaviors in the Sultanate of Oman.

The conceptual model in Fig. 2 visually represents the proposed interactions between PMT's threat appraisal and coping appraisal components and their impact on HCPs' information security behaviors. This framework guides the development of the study's hypotheses and the subsequent empirical investigation.

Data collection

The finalized questionnaire was distributed using electronic email distribution and paper-based copies. The electronic questionnaire was emailed to the eligible HCPs, and reminder emails were constantly sent to the participants. Moreover, paper-based questionnaires were posted within the hospitals to achieve a high response rate. Two approaches were deemed appropriate, as this would serve participants' preferences and increase the likelihood of a diverse representative sample. Participants were guaranteed confidentiality and anonymity, and engagement in the questionnaire was voluntary. The data collection phase spanned several weeks, with periodic follow-ups conducted to enhance participation rates.

Instrument

Data were collected using an electronic and paper-based, distributed, structured questionnaire. The questionnaire measured perceived vulnerability, severity, rewards, response efficacy, self-efficacy, response cost, and information security behaviors. It comprised 37 items divided into three sections: demographic information, PMT constructs [perceived severity, perceived vulnerability, maladaptive rewards, response efficacy, self-efficacy, and response cost], and security behaviors.

Data analysis

The data analysis was conducted in two stages to gain comprehensive insights into the security behaviors of HCPs. In the first stage, descriptive analysis was conducted to summarize the essential characteristics of the data, encompassing data cleaning, demographic analysis, and calculation of descriptive statistics. The second stage involved inferential analysis to examine relationships and test hypotheses. This included factor analysis to identify underlying constructs, reliability analysis to assess internal consistency, and correlation and regression analyses to determine predictors of key security behaviors.

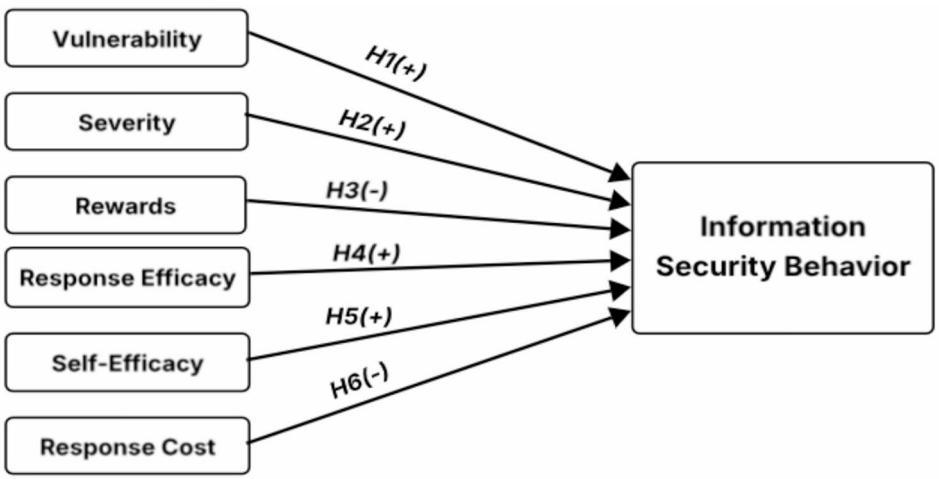

Fig. 2. Research conceptual model.

Results

Demographic characteristics of respondents

A total of 455 HCPs completed the questionnaire voluntarily. After excluding 10 incomplete questionnaires, data from 445 participants were analyzed. The questionnaire had 103 male respondents (23.1%) and 342 female respondents (76.9%), with 44% falling within the age range of 36 to 46. Over half of the respondents had more than 11 years of experience. The respondents consisted of 114 physicians (25.6%) and 331 nurses (74.4%).

Hypothesis testing

Multiple linear regression analysis was used to test the hypotheses, after verifying the validity of statistical assumptions, including linearity and normality.

Hypothesis 1 (perception of vulnerability)
The results showed that perception of vulnerability positively and statistically significantly affects healthcare providers' information security behaviors ($B = 0.34$, $\beta = 0.32$, $t = 7.86$, $p < 0.001$), supporting the hypothesis. This model explains 11% of the variance in security behaviors ($R^2 = 0.11$).

Hypothesis 2 (perception of severity)
The analyses revealed a strong positive relationship between perceived threat severity and security behaviors ($B = 0.64$, $\beta = 0.61$, $t = 17.66$, $p < 0.001$), with this model accounting for 37% of the variance ($R^2 = 0.37$).

Hypothesis 3 (reward perceptions)
The data did not support the hypothesis that perceived rewards for unsafe behaviors negatively impact security behaviors, as the results showed no significant effect ($B = 0.03$, $\beta = 0.03$, $t = 0.68$, $p = 0.496$).

Hypothesis 4 (response efficacy)
The results showed that response efficacy had a positive and significant effect on security behaviors ($B = 0.58$, $\beta = 0.57$, $t = 15.99$, $p < 0.001$), explaining 33% of the variance ($R^2 = 0.33$).

Hypothesis 5 (self-efficacy)
Self-efficacy demonstrated a positive and significant effect on security behaviors ($B = 0.53$, $\beta = 0.45$, $t = 11.47$, $p < 0.001$), and explained approximately 20% of the variance ($R^2 = 0.20$).

Hypothesis 6 (response costs)
Results demonstrated a positive effect of response costs on security behaviors ($B = 0.19$, $\beta = 0.18$, $t = 4.28$, $p < 0.001$), contrary to expectations, thus rejecting the hypothesis. This model explained only 3% of the variance ($R^2 = 0.03$).

Table 3 below summarizes the regression results of all hypotheses.

Structural model results (path analysis)

After evaluating the structural model, path coefficients were analyzed to examine the strength and significance of the relationships between the variables. Figure 3 illustrates the paths and their significance levels. The results showed that perceived severity, perceived vulnerability, response efficacy, and self-efficacy had positive and statistically significant effects on information security behaviors ($p < 0.01$). Response costs also appeared to have a positive effect on the significance level ($\alpha = 0.05$). In contrast, maladaptive rewards had no significant effect, leading to the rejection of Hypotheses H3 and H6.

Furthermore, the analyses revealed that perceived severity accounted for approximately 37% of the variance in security behaviors ($R^2 = 0.37$). In comparison, response efficacy explained approximately 33% of this variance, highlighting the importance of these two variables in promoting security behaviors compared to other factors. These results indicate that perceived severity and response efficacy, along with self-efficacy in implementing security measures, are the most influential factors in promoting security behaviors among HCPs. In contrast, response costs and rewards play a less significant role. Table 4 provides a summary of the results of the hypothesis testing.

Predictor	Dependent variable	B	SE	Beta	t	Sig.	r	R^2	Constant
Perceived vulnerability	Vulnerability	0.34	0.04	0.32	7.86	< 0.001	0.33	0.11	2.89
Perceived severity	Severity	0.64	0.04	0.61	17.66	< 0.001	0.61	0.37	1.57
Rewards from Insecure Behavior	Rewards	0.03	0.04	0.03	0.68	0.496	0.03	0	3.87
Response efficacy	Efficacy	0.58	0.04	0.57	15.99	< 0.001	0.57	0.33	1.75
Self-efficacy	Self-efficacy	0.53	0.05	0.45	11.47	< 0.001	0.45	0.20	2.10
Response costs	Costs	0.19	0.04	0.18	4.28	< 0.001	0.18	0.03	3.40

Table 3. Multiple regression analysis predicting hcps' information security behaviors.

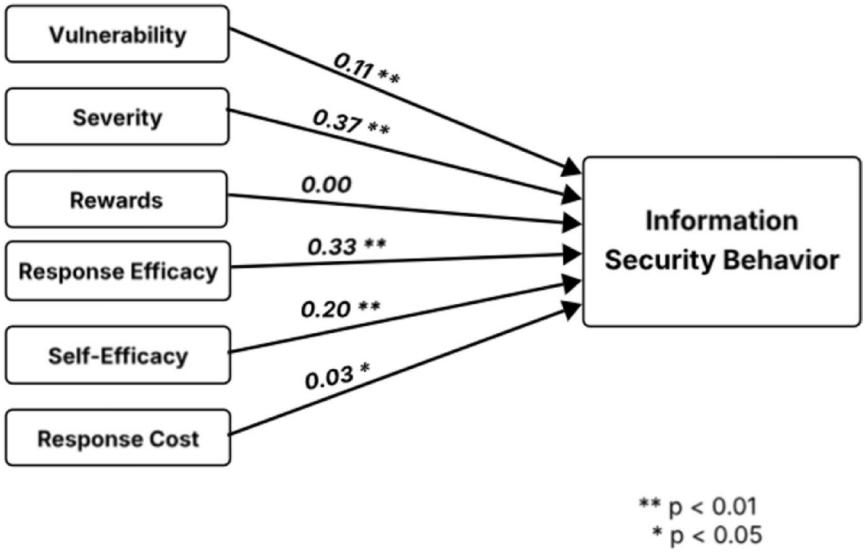

Fig. 3. Path diagram for research model.

Hypothesis	Path	Path coefficient	t-value	Supported
H1	Perceived vulnerability → Information Security Behaviors	0.11	7.86**	Yes
H2	Perceived severity → Information Security Behaviors	0.37	17.66**	Yes
H3	Maladaptive rewards → Information Security Behaviors	0.00	0.68*	No
H4	Response efficacy → Information Security Behaviors	0.33	15.99**	Yes
H5	Self-efficacy → Information Security Behaviors	0.20	11.47**	Yes
H6	Response cost → Information Security Behaviors	0.03	4.28*	No

Table 4. Summary of hypothesis testing results. ** Statistically Significant ($P < 0.01$). *Statistically Significant ($P < 0.05$).

Discussion and implication

This study evaluated the elements that drive HCPs' security behaviors. It developed a PMT-based research model, considering all the variables and information security behaviors. The research model yielded insightful results, which are reported here. First, the study found that PMT is an effective model for predicting HCPs' information security behaviors. Perceived severity and response efficacy have the most significant impact on healthcare professionals' motivation to practice information security. HCPs are more likely to utilize information security when it is viewed as successful and practical, leading to increased confidence. This finding is consistent with Herath and Rao[8], who emphasize the importance of perceived severity and response efficacy in influencing motivation to practice information security. Likewise, Ifinedo[7] demonstrated that the perceived severity of breaches has been shown to influence compliance behaviors. Additionally, recent experiments (2025) have shown that response efficacy messages are more effective than self-efficacy messages in influencing specific behavioral outcomes[45,46]. However, Van Bavel et al.[19] argue that once secure behaviors become habitual, they are more likely to be sustained, regardless of the perceived severity of threats or the efficacy of response findings. In addition, the study found that vulnerability also influences the security behaviors of HCPs. This finding is consistent with the study by Johnston et al.[26], which found that perceived vulnerability significantly influenced individuals' intentions to engage in information security actions.

Second, maladaptive rewards do not affect HCPs' security behaviors. In our study, this result can be attributed to several key factors. For instance, the MOH hospitals in the Sultanate of Oman have a solid organizational culture, and severe security procedures will likely outweigh any immediate non-compliance benefits. Furthermore, broad security awareness and training programs effectively managed to enlighten the HCPs about the severe consequences of insecure behavior, reducing the attractiveness of short-term rewards. The high perceived severity and vulnerability to security threats, in combination with intrinsic motivators like personal responsibility and professional pride, ensure that the HCP will prefer secure practices to possibly harmful incentives. The integration of such attributes creates an environment in which the benefits derived from noncompliance are recognized as inconsequential in comparison to the broader commitment to ensuring information security. These findings also contrast with Moody et al.'s[13] study, which found that destructive incentives, such as convenience and the quick benefits from noncompliance, play a significant role in shaping information security behaviors. The investigators speculate that the short-term benefits associated with insecure behavior, such as saving time or effort, outweigh the perceived benefits of secure behavior.

Third, response costs have a positive influence on HCPs' security behavior. The awareness and conscientiousness that such expenses bring about can substantiate the fact that such expenses are instilled in an individual. When the HCP perceives that setting security measures in terms of time, effort, and resources is vital, they will be more willing to take them seriously and follow them closely. Greater investment in security procedures, therefore, means greater accountability and a more profound commitment to upholding established norms, as the significance and need to maintain security are better emphasized by the considerable effort required. Higher response costs, therefore, encourage more robust and standardized security, as health professionals are more aware of their key role in protecting corporate assets. This finding is inconsistent with those from other studies[8,19,26]. These studies find that increased response costs tend to have a demotivating effect on compliance with security policies due to the perceived difficulty they entail. Response costs positively influence information security behavior, necessitating the integration of stringency in security protocols with usability and user-friendliness. In contrast, organizations see compliance as a strategic decision that balances costs and sanctions, promoting cautious behavior and cooperation[58]. In information security, strict policies with high response costs often enhance compliance but can lead to resistance if perceived as overly harsh[59]. For example, Bozeman[60] found employees comply more when sanctions are significant. This perspective clarifies the results in the Omani healthcare context.

The findings also have important implications for reinforcing perceived severity and response efficacy as critical motivators for secure behavior. This emphasizes the importance of organizational activities aimed at mitigating the consequences of security breaches and communicating the effectiveness of various protective strategies. This is supported by the limited influence of maladaptive rewards, suggesting that a strong corporate culture and relevant training weaken the appeal of immediate improbable gains, thus underlining the importance of security awareness programs. Finally, the beneficial effect of response costs defies expectations, showing that once employees feel that security measures are demanding in terms of effort, they are more likely to treat these seriously. This demonstrates that carefully designed, effortful security protocols can improve compliance if they are manageable. Our findings offer valuable insights into developing more effective information security policies and training programs, utilizing key characteristics of PMT to cultivate a robust security culture.

Furthermore, this study offers valuable insights for enhancing information security practices in Oman's healthcare sector. For policymakers, the results suggest that applying PMT can help design more effective awareness programs that boost HCPs' motivation to follow secure behaviors. The government can utilize these findings to eliminate barriers such as time and complexity, thereby making it easier for staff to adhere to security protocols. For healthcare managers, the study emphasizes the importance of creating a supportive culture by providing training, simplifying procedures, and promoting secure practices through positive feedback. On a broader level, the research underscores the importance of human-centered approaches to cybersecurity, rather than relying solely on technical solutions. Theoretically, it expands the use of PMT in the healthcare context, particularly in the Gulf region, and demonstrates that factors such as response cost may play unexpected roles, highlighting the need for more context-sensitive research in the future.

Conclusion

This study uses the PMT to provide necessary insights into the information security behaviors of HCPs within the Sultanate of Oman. The findings emphasize the critical importance of threat appraisal and coping appraisal in the performance of security protocols by healthcare professionals, highlighting the need for tailored interventions that enhance their perception of threats and confidence in the effectiveness of protective measures. The study also highlights the crucial role of ongoing education and organizational support in fostering a security culture within healthcare organizations. The study offers some practical recommendations to the MOH and healthcare administrators on how to enhance information security behaviors in the Sultanate of Oman's health sector for better protection of sensitive patient data and healthcare system integrity.

Data availability

The datasets used and/or analyzed during the current study would be available from the corresponding author upon request.

Received: 23 April 2025; Accepted: 31 October 2025
Published online: 02 December 2025

References

1. Kittur, L. J., Mehra, R. & Chandavarkar, B. R. The dependency of healthcare on security: Issues and challenges. In *ICCCE 2020: Proceedings of the 3rd International Conference on Communications and Cyber Physical Engineering*. 119–129. (Springer Nature Singapore, 2020). https://doi.org/10.1007/978-981-15-7961-5_12
2. Folasole, A., Adegboye, O. S., Ekuewa, O. I. & Eshua, P. E. Security, privacy challenges and available countermeasures in electronic health record systems: A review. *Eur. J. Electr. Eng. Comput. Sci.* **7** (6), 27–33. https://doi.org/10.24018/ejece.2023.7.6.561 (2023).
3. Rai, A. Case studies on disproportionate impact of cyberattacks in the healthcare sector. *J. High. School Res.* https://doi.org/10.70671/gad6q058 (2024).
4. Khan, M. Healthcare cybersecurity: A mini review on recent incidents and preventive strategies. *SSN J. Manage. Technol. Res. Commun.* https://doi.org/10.21786/mntrc/1.1.3 (2024).
5. Triplett, W. Ransomware attacks on the healthcare industry. *J. Bus. Technol. Leadersh.* **4** (1), 1–13. https://doi.org/10.54845/btljournal.v4i1.31 (2022).
6. Cartwright, A. J. The elephant in the room: cybersecurity in healthcare. *J. Clin. Monit. Comput.* **37** (5), 1123–1132. https://doi.org/10.1007/s10877-023-01013-5 (2023).
7. Ifinedo, P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* **31** (1), 83–95. https://doi.org/10.1016/j.cose.2011.06.002 (2012).

8. Hearth, T. & Rao, H. R. Protection motivation and deterrence: A framework for security policy compliance in organizations. *Eur. J. Inform. Syst.* **18** (2), 106–125. https://doi.org/10.1057/ejis.2009.6 (2009).
9. Workman, M., Bommer, W. H. & Straub, D. Security lapses and the omission of information security measures: A threat control model and empirical test. *Comput. Hum. Behav.* **24** (6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005 (2008).
10. Rogers, R. W. A protection motivation theory of fear appeals and attitude change1. *J. Psychol.* **91** (1), 93–114 (1975).
11. Maddux, J. E. & Rogers, R. W. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *J. Exp. Soc. Psychol.* **19** (5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9 (1983).
12. Jalali, M. S. & Kaiser, J. P. Cybersecurity in hospitals: a systematic, organizational perspective. *J. Med. Internet. Res.* **20** (5), e10059. (2018).
13. Moody, G. D., Siponen, M. & Pahnila, S. Toward a unified model of information security policy compliance. *MIS Q.* **42** (1), 285–A22. https://doi.org/10.25300/MISQ/2018/13853 (2018).
14. Towbin, R. S. *A Protection Motivation Theory Approach To Healthcare Cybersecurity: A Multiple Case Study* (Northcentral University, 2019).
15. Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, H. & M Information security awareness and behavior: a theory-based literature review. *Manage. Res. Rev.* **37** (12), 1049–1092 (2014).
16. Menard, P., Warkentin, M. & Lowry, P. B. The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers Secur.* **75**, 147–166. https://doi.org/10.1016/j.cose.2018.01.020 (2018).
17. Ma, X. IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Inf. Process. Manag.* **59** (1), 102744. https://doi.org/10.1016/j.ipm.2021.102744 (2022).
18. Floyd, D. L., Prentice-Dunn, S. & Rogers, R. W. A meta-analysis of research on protection motivation theory. *J. Appl. Soc. Psychol.* **30** (2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x (2000).
19. Van Bavel, R., Rodríguez-Priego, N., Vila, J. & Briggs, P. Using protection motivation theory in the design of nudges to improve online security behavior. *Int. J. Hum. Comput. Stud.* **123**, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003 (2019).
20. Liang, H. & Xue, Y. Avoidance of information technology threats: A theoretical perspective. *MIS Q.* 71–90. https://doi.org/10.2307/20650279 (2009).
21. Lee, Y. & Larsen, K. R. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *Eur. J. Inform. Syst.* **18** (2), 177–187. https://doi.org/10.1057/ejis.2009.12 (2009).
22. Hwang, I., Kim, D., Kim, T. & Kim, S. Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Inf. Rev.* **41** (1), 2–18. https://doi.org/10.1108/OIR-11-2015-0358 (2017).
23. Nelson, R. *Factors that Influence Medical Professionals' Noncompliance with Organizational Mobile Device Security Policies* (Doctoral Dissertation, Capella University, 2019).
24. Haag, S., Siponen, M. & Liu, F. Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: DATABASE Adv. Inform. Syst.* **52** (2), 25–67. https://doi.org/10.1145/3462766.3462770 (2021).
25. Li, W., Liu, R., Sun, L., Guo, Z. & Gao, J. An investigation of employees' intention to comply with information security system—A mixed approach based on regression analysis and FsQCA. *Int. J. Environ. Res. Public Health.* **19** (23). https://doi.org/10.3390/ijerph192316038 (2022).
26. Johnston, A. C., Warkentin, M. & Siponen, M. An enhanced fear appeal rhetorical framework. *MIS Q.* **39** (1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06 (2015).
27. Schneider, M. *Protection Motivation Theory Factors that Influence Undergraduates to Adopt Smartphone Security Measures* (Doctoral Dissertation, Capella University, 2020).
28. Tsai, H. Y. S. et al. Understanding online safety behaviors: A protection motivation theory perspective. *Computers Secur.* **59**, 138–150. https://doi.org/10.1016/j.cose.2016.02.009 (2016).
29. Khan, N. F., Murtaza, H., Malik, K., Mahmood, M. & Asadi, M. A. Explanatory and predictive analysis of smartphone security using protection motivation theory: a hybrid SEM-AI approach. *Inform. Technol. People.* **38** (4), 2041–2068 (2025).
30. Warkentin, M., Johnston, A. C., Shropshire, J. & Barnett, W. D. Continuance of protective security behavior: A longitudinal study. *Decis. Support Syst.* **92**, 25–35. https://doi.org/10.1016/J.DSS.2016.09.013 (2016).
31. Thompson, N., McGill, T. & Narula, N. No point worrying'–The role of threat devaluation in information security behavior. *Comput. Secur.* **143**. https://doi.org/10.1016/j.cose.2024.103897 (2024).
32. Burns, A. J., Posey, C., Roberts, T. L. & Lowry, P. B. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Comput. Hum. Behav.* **68**, 190–209 (2017).
33. Almansoori, A., Al-Emran, M. & Shaalan, K. Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Appl. Sci.* **13** (9), 5700. https://doi.org/10.3390/app13095700 (2023).
34. Bandura, A. *Self-Efficacy: The Exercise of Control* (Macmillan, 1997).
35. Bandura, A. *Social Foundations of Thought and Action* (Englewood Cliffs, 1986).
36. Borgert, N. et al. Self-efficacy and security behavior: Results from a systematic review of research methods. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–32. (2024). https://doi.org/10.1145/3613904.3642432
37. Vance, A., Siponen, M. & Pahnila, S. Motivating IS security compliance: insights from habit and protection motivation theory. *Inf. Manag.* **49** (3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002 (2012).
38. Mortada, E., Abdel-Azeem, A., Al Showair, A. & Zalat, M. M. Preventive behaviors towards Covid-19 pandemic among healthcare providers in Saudi Arabia using the protection motivation theory. *Risk Manag. Healthc. Policy* 685–694. https://doi.org/10.2147/RMHP.S289837 (2021).
39. Sreenath, S. S., Hewitt, B. & Sreenath, S. Understanding security behaviour among healthcare professionals by comparing results from technology threat avoidance theory and protection motivation theory. *Behav. Inform. Technol.* **44** (2), 181–196. https://doi.org/10.1080/0144929X.2024.2314255 (2024).
40. Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S. & Aji, R. F. Information security behavior in health information systems: A review of research trends and antecedent factors. In *Healthcare*. Vol. 10(12) 2531. (MDPI, 2022). https://doi.org/10.3390/healthcare10122531
41. Yeng, P. K., Fauzi, M. A. & Yang, B. A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals. *Information* **13** (7), 335. https://doi.org/10.3390/info13070335 (2022).
42. Yeng, P. K., Fauzi, M. A. & Yang, B. Assessing the effect of human factors in healthcare cyber security practice: An empirical study. In *Proceedings of the 25th Pan-Hellenic Conference on Informatics*. 472–476. (2021). https://doi.org/10.1145/3503823.3503909
43. Kiran, U., Khan, N. F., Murtaza, H., Farooq, A. & Pirkkalainen, H. Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers Secur.* **149**, 104204 (2025).
44. Khan, N. F., Ikram, N., Murtaza, H. & Javed, M. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's model. *Computers Secur.* **125**, 103049 (2023).
45. Simon, J., Watson, S. J., & van Sintemaartensdijk, I. Response-efficacy messages produce stronger passwords than self-efficacy messages… for now: A longitudinal experimental study of the efficacy of coping message types on password creation behaviour. *Comput. Hum. Behav. Rep.* **17**, 100615 (2025).

46. van't Hoff-de Goede, M. S., Leukfeldt, E. R., van de Weijer, S. G. A. & van der Kleij, R. Does protection motivation predict self-protective online behaviour? Comparing self-reported and actual online behaviour using a population-based survey experiment. *Computers Hum. Behav. Rep.* **18**, 100649 (2025).
47. Khan, N. F., Ikram, N. & Saleem, S. Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Secur. J.* **1** (2023).
48. Khan, N. F., Ikram, N. & Saleem, S. Digital divide and socio-economic differences in smartphone information security behaviour among university students: empirical evidence from Pakistan. *Int. J. Mobile Commun.* **22** (1), 1–24 (2023b).
49. Kanimozhi, R., Padmavathi, V. & Ramesh, P. S. Perceived digital threats influencing smartphone use among the aging population. *Sci. Rep.* **15** (1), 27813 (2025).
50. Khadka, K. & Ullah, A. B. Human factors in cybersecurity: an interdisciplinary review and framework proposal. *Int. J. Inf. Secur.* **24**, 119. https://doi.org/10.1007/s10207-025-01032-0 (2025).
51. Zou, Y. et al. Encouraging users to change breached passwords using the protection motivation theory. *ACM Trans. Computer-Human Interact.* **31** (5), 1–45 (2024).
52. Weber, A. S. et al. Systematic thematic review of e-health research in the Gulf Cooperation Council (Arabian Gulf): Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and United Arab Emirates. *J. Telemed. Telecare*. **23**, 452–459. https://doi.org/10.1177/1357633X16647894 (2017).
53. Al-Azri, M. H., Al-Belushi, R., Al-Mamari, M., Davidson, R. & Mathew, A. C. Knowledge and health beliefs regarding sickle cell disease among Omanis in a primary healthcare setting: cross-sectional study. *Sultan Qaboos Univ. Med. J.* **16** (4), e437. https://doi.org/10.18295/squmj.2016.16.04.006 (2016).
54. Al-Farsi, O. A. et al. A study on knowledge, attitude, and practice towards premarital carrier screening among adults attending primary healthcare centers in a region in Oman. *BMC Public. Health*. **14**, 1–7. https://doi.org/10.1186/1471-2458-14-380 (2014).
55. Qoronflesh, M. W., Essa, M. M., Alharahsheh, S. T., Al-Farsi, Y. M. & Al-Adawi, S. Autism in the Gulf states: A regional overview. *Front. Bioscience-Landmark*. **24** (2), 334–346. https://doi.org/10.2741/4721 (2019).
56. MOH. *MOH Annual Report*. (2020).
57. Walliman, N. *Research Methods: The Basics* (Routledge, 2011).
58. Oniwinde, B. The essence of compliance is making choices. *Social Sci. Res. Netw.* https://doi.org/10.2139/ssrn.4708345 (2024).
59. Lowry, P. B. & Moody, G. D. Proposing the control-reactance compliance model CRCM to explain opposing motivations to comply with organisational information security policies. *Inform. Syst. J.* **25** (5), 433–463. https://doi.org/10.1111/ISJ.12043 (2015).
60. Bozeman, B. Rules compliance behavior: A heuristic model. *Perspect. Public. Manage. Gov.* **5** (1), 36–49. https://doi.org/10.1093/ppmgov/gvab028 (2022).

Author contributions
Al Toobi, A.: writing the original draft preparation and the main manuscript text .Al Suqri, M.: writing, review & editing.

Declarations

Competing interests
The authors declare no competing interests.

Human ethics and consent to participate declarations
This study received ethical approval from the Research Ethics Committee at Sultan Qaboos University. All participants provided informed consent, and the research adhered to the ethical standards of the Declaration of Helsinki.

Consent to participate
Informed consent was obtained from all participants prior to their participation in the study. Participation was voluntary, and participants were assured of anonymity and confidentiality.

Additional information
Correspondence and requests for materials should be addressed to A.A.T.

Reprints and permissions information is available at www.nature.com/reprints.

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

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

© The Author(s) 2025