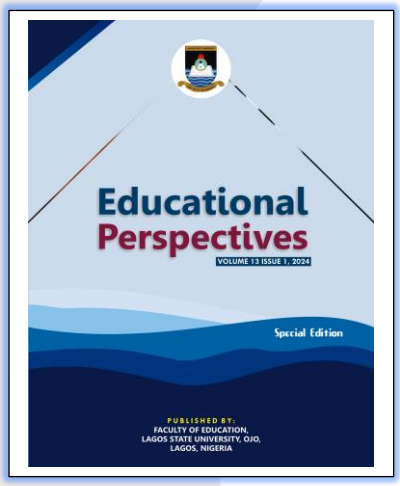

Understanding Online Security Perceptions and Practices: A Qualitative Study

Michael Adelani Adewusi, Adebanjo Adeshina Wasiu & Ola Tokunbo Odekeye

School of Mathematics and Computing, Kampala International University
ACEITSE, Lagos State University, Ojo
Department of Educational Technology, Osun State University, Oshogbo

KEYWORDS:

Online security, Perception, Digital security, online threats.

WORD COUNT:
268

CORRESPONDING EMAIL ADDRESS:
mikeade3000@yahoo.com

ORCID NUMBER:

0000-0002-8003-6761

ABSTRACT

This explore the relationship between individuals' perceptions of online security and their corresponding practices, with the goal of understanding how these perceptions influence protective strategies against digital threats. The study utilizes a qualitative design, specifically employing thematic analysis to delve into the diverse attitudes and actions that individuals adopt concerning online security measures. Data were collected through in-depth interviews and surveys, which provided a view of the factors influencing online security perceptions and behaviors among participants. The study reveals a broad spectrum of user attitudes towards online security, showing that an individual's understanding of online threats significantly shapes their protective actions. Key influences on these perceptions include personal experiences with online threats, societal influences, and the media's portrayal of cyber risks. The study also highlights the crucial role of trust in shaping user behavior, balancing the trade-off between convenience and security. Additionally, it examines how organizational policies and practices impact personal security behaviors, demonstrating the dynamic interaction between individual choices and structured regulations. The findings underscore the intricate nature of online security perceptions and actions, emphasizing the importance of trust and the impact of external influences on user behavior. It provides valuable insights for policymakers, cybersecurity experts, and users, highlighting the need for a deeper understanding of the human elements at the core of online threats. The study recommends the development of customized educational programmes and user-friendly security measures to enhance digital literacy and promote safer online practices. These should aim to empower users with the knowledge and tools necessary to navigate the digital landscape securely, thereby mitigating the risks associated with cyber threats and protecting digital environments.

HOW TO CITE

Adewusi M.A, Adebanjo A.W & Odekeye O.T. (2024). Understanding Online Security Perceptions and Practices: A Qualitative Study. *Educational Perspectives, 13*(1), 206-218.

Introduction

This study provides an examination of how individuals perceive and respond to the risks associated with online activities, particularly focusing on the measures they take to protect their digital presence. The study employs a qualitative methodology to subjective experiences and understandings of users across diverse demographics, offering rich insights into the current landscape of digital security.

As digital interactions become increasingly integral to everyday life, the corresponding rise in cyber threats, such as phishing scams, malware attacks, data breaches, and identity theft, has become a significant concern. These threats highlight the critical need for effective online security practices (Twomey et al., 2023). The study explores the diverse challenges users face in navigating the digital environment, where the severity and likelihood of online security threats are perceived differently by individuals, influenced by various factors including past experiences, awareness levels, and personal attitudes towards risk.

The study utilizes thematic analysis to extract perspectives online security threats from a broad spectrum of participants. These participants include those with high digital literacy and those for whom the digital world remains relatively unfamiliar. This diversity ensures that the study captures a wide range of perspectives and practices related to online security, providing a comprehensive overview of how different groups understand and manage their online safety (Twomey et al., 2023).

A significant finding of the study is the variation in how individuals perceive online security threats. While some participants demonstrate high levels of awareness and concern—often influenced by negative experiences or close encounters with cyber-threats, others display a more complacent attitude. This complacency is frequently due to a lack of personal experience with such threats or a general skepticism about the severity of the risks (Rahi et al., 2023). The study reveals a general trend towards reactive rather than proactive security measures, with many individuals seeking information on online security only after a breach has occurred or when alerted by their social circles (Rangaraju, 2023).

The psychological factors influencing online security behaviors are another critical aspect of this study. It investigates concepts such as risk perception, trust in digital platforms, and the psychological impact of media reports on cyber-threats, all of which significantly shape individuals' approaches to online security (Haugli-Sandvik, 2024). Trust emerges as a serious factor in decision-making processes related to online security, influencing how users engage with security measures, the credibility they assign to security advice, and their overall belief in the effectiveness of these measures (Telo, 2023).

Education and awareness play crucial roles in enhancing online security practices. However, the study finds that current educational efforts may not be sufficiently tailored to meet the diverse needs of different user groups. It advocates for more personalized, context-specific educational approaches that can effectively address these varying needs and improve online security behaviors (Hong et al., 2023). Furthermore, the study identifies a gap between the availability of sophisticated security technologies and the average user's ability to effectively utilize these tools, pointing to the need for user-friendly security solutions that do not compromise on usability (Aslan et al., 2023).

Related Studies

Exploration of the psychological aspects that influence individuals' perceptions of security and their behaviors online. Delving into how cognitive biases and heuristics affect the decision-making process in security-related scenarios. The emphasizes was on the role of cognitive biases in shaping security behaviors, highlighting the need for understanding psychological factors in designing effective security measures (Brinton Anderson et al., 2016).

A comparative study that investigates the different factors that influence online security behaviors in the UK and the USA, including cultural, social, and individual determinants by identifying cultural differences as significant determinants in shaping security behaviors, emphasizing the need for culturally sensitive security education programs (Baltuttis et al., 2024).

Karvonen, (2008), and Adewusi et al., (2021) argue that usability and trust are critical in encouraging users to follow security protocols, proposing that security mechanisms should be user-friendly and trustworthy. He stated that the reasons behind users' non-compliance with security protocols and suggests strategies to improve user adherence by addressing usability and trust issues.

Bowen and Chawla (2012) highlight the crucial role of trust in determining cybersecurity practices, by suggesting that fostering trust can enhance security compliance. Their analysis examines how trust impacts cybersecurity practices across various sectors, highlighting the balance between trust and security in digital interactions.

The security behaviors of smartphone users, exploring the factors that influence their decisions and the effectiveness of different interventions to promote better security practices indicated that direct experiences with security incidents significantly influence smartphone users' security behaviors, advocating for targeted interventions to improve security awareness and practices (Naga et al., 2024).

Aim

This study aim to delve into the relationship between individuals' perceptions of online security and their actual security practices. By investigating how people's understanding of online threats shapes their protective strategies, the study hope to uncover a wide spectrum of attitudes and behaviors. This includes examining the influence of personal experiences, societal pressures, and media portrayals on individuals' security perceptions. Such insights will help elucidate why people act the way they do regarding online security, providing an understanding of the factors that drive these behaviors.

Additionally, the study seeks to highlight the delicate balance users must navigate between convenience and security in digital spaces. In many cases, individuals may prioritize ease of use over stringent security measures, which can leave them vulnerable to cyber threats. By exploring this the study aim to shed light on how trust and usability impact security behavior. Furthermore, by evaluating how current policies and practices influence personal security actions, the study can better understand the dynamic interplay between individual choices and structured regulations. This aspect of the study is crucial for identifying where current approaches may fall short and how they can be improved.

The study aspires to provide actionable insights for various stakeholders, including policymakers, cybersecurity experts, and everyday users. By identifying research gaps and highlighting the need for more effective response and recovery mechanisms, the study hope to pave the way for future investigations that bolster online security. This study aims to enhance the comprehension of the human elements central to online security, thereby fostering more sophisticated and effective strategies to combat cyber threats and protect digital environments.

Statement of the Problem

The digital age has ushered in unparalleled convenience, transforming how we communicate, work, and manage our daily lives (Gao, 2023). However, this digital integration comes with a significant caveat: the escalation of online security threats (Blackmon & Major, 2023). Cyberattacks have become increasingly sophisticated, targeting not just large corporations and government entities but also individuals who may lack the resources or knowledge to protect themselves adequately (Kayode-Ajala, O. (2023). This situation underlines a critical problem: a widespread gap in the general population's understanding of online security risks and the practices necessary to mitigate these threats (Alqudhaibi et al., 2024; Adewusi et al., 2024). The disparity between the rapid advancement of cyber threats and the slower pace of user knowledge on security practices poses a significant challenge, leaving individuals vulnerable to data breaches, identity theft, and other forms of cyber exploitation.

Compounding this issue is the diversity of the online user base, encompassing a broad spectrum of backgrounds, and technical proficiencies (Ajani, O. A. (2023). This diversity results in varied perceptions of online security, with some users underestimating the risks and others overwhelmed by the complexity of securing their digital footprint (Fosch-Villaronga & Drukarch, 2023). The problem is not just a lack of awareness but also a

disconnect between understanding the severity of online threats and implementing effective protective measures (Nwankpa & Datta, 2023). Many individuals rely on outdated or simplistic security strategies, if any at all, rendering them exposed to evolving cyberattacks that can have devastating personal and financial repercussions (Aslan et al., 2023).

Moreover, the problem extends beyond individual action or inaction. There is a critical need for systemic changes in how online security education is approached and delivered (McCarthy et al., 2023; Adewusi et al., 2021). Traditional cybersecurity awareness campaigns often fail to resonate with or reach the wider public effectively (Starks & Reich, 2023). This inadequacy is partly due to their one-size-fits-all approach, which does not account for the varying levels of digital literacy or the specific needs and concerns of different user groups (Starks & Reich, 2023). As a result, even when users are aware of online security risks, they may not have the knowledge or tools to take appropriate action. This gap highlights an urgent need for innovative, engaging, and accessible knowledge methods that empower users to protect themselves online.

The situation is further complicated by the evolving nature of technology itself. With the introduction of new digital services and the Internet of Things (IoT), the landscape of potential security vulnerabilities continues to expand (Ahmed & Khan, 2023). Users are often unaware of the risks associated with these new technologies, or they might underestimate the importance of securing devices and services that seem benign (Stephenson et al., 2023). The proliferation of digital technologies has outpaced the development of user-friendly security solutions, leading to a paradox where the most effective security measures are those least understood and used by the average person (Lottu et al., 2023). Addressing this complex web of challenges requires a multifaceted approach that not only enhances the individual's capacity to engage in secure online behaviours but also fosters an environment where security is accessible, intuitive, and embedded within the fabric of digital technology use (Ahmad, 2024; Allioui & Mourdi, 2023; Adewusi et al., 2022).

Research questions

1. How do you perceive the security of your online accounts, and what influences your feelings of safety or vulnerability?
2. How confident are you in recognizing and stopping phishing attempts, and what experiences or knowledge have shaped this confidence?
3. How frequently do you update your online account passwords, and why?
4. How do you manage sharing personal information online, and what precautions do you use, and why are they significant to you?
5. How well do you understand common online security threats, and what has contributed to your knowledge in this area?

Methodology

Research Design

This study employs a qualitative research design, focusing on understanding individuals' perceptions and practices regarding online security. The research utilizes a thematic approach, guided by questions that are designed to elicit detailed responses about participants' experiences, knowledge, and behaviors related to online security (Aslam, 2023). This approach is well-suited for capturing the views and practices among diverse user groups, facilitating a rich, in-depth exploration of the subject matter.

Population

The study targeted a broad population of online users, including individuals with varying levels of digital literacy, backgrounds, and experiences with online security. The population was intended to reflect a wide range of ages, professions, and digital usage patterns, thereby mirroring the diverse spectrum of online users in general (Petrovčič et al., 2023).

Sample Size and Sampling Technique

Participants were selected through purposive sampling, a technique chosen to ensure that the sample included individuals representing different levels of digital literacy and varied experiences with online security. This method allowed for the inclusion of a representative mix of 60 participants, ensuring that the study captured a comprehensive

picture of current trends and issues in online security (Petrovčič et al., 2023).

Instrument

Data collection was conducted using an online Google Form that facilitated semi-structured interviews. The instrument was developed based on a set of thematic questions designed to explore key areas of online security, such as participants' confidence in handling phishing attempts, their approaches to sharing personal information online, their password management practices, and their overall perception of their knowledge concerning common online security threats.

Development, Content, and Validation

The interview questions were developed through a rigorous process involving a review of relevant literature and consultations with cybersecurity experts to ensure the instrument's relevance and comprehensiveness. The content covered critical areas of online security and was designed to encourage open-ended responses that would provide deep insights into participants' practices and perceptions. The instrument was validated through peer review by other researchers in the field, ensuring that the questions were clear, relevant, and capable of eliciting the desired information. The reliability coefficient was established at 0.85 using Cronbach's alpha, indicating a high level of internal consistency.

Method of Data Collection

Data collection involved the use of semi-structured interviews conducted online via Google Forms. This method allowed for a flexible yet focused dialogue, enabling participants to express their thoughts, experiences, and behaviors in their own words. The open-ended nature of the questions facilitated rich, qualitative data that was critical for the study's thematic analysis.

Method of Data Analysis

Following the data collection, the qualitative data was analyzed using thematic analysis. The analysis began with a thorough review of the interview transcripts, during which initial codes were generated based on recurring concepts related to the thematic questions (Naeem et al., 2023). These codes were then grouped into broader themes that encapsulate the key findings of the study, such as the influence of personal experiences on security behaviors, the role of knowledge in shaping security perceptions, and the variety of practices adopted to mitigate online security risks.

Reliability and Validity

To ensure the reliability and validity of the findings, the study incorporated several methodological checks, including peer debriefing, where discussions with other researchers were used to scrutinize the analysis process and conclusions drawn. This rigorous approach ensures that the study's findings are both reliable and valid, providing a solid foundation for understanding online security perceptions and practices (Naeem et al., 2023; Adewusi et al., 2024).

Findings

How do you perceive the security of your online accounts, and what influences your feelings of safety or vulnerability?

This thematic question probes participants' perceptions of their online account security, focusing on the factors that contribute to their sense of safety or vulnerability. The collected responses reveal a spectrum of attitudes towards online security, highlighting a complex interplay between knowledge, behaviour, and emotional responses to the digital environment. This analysis categorises the findings into key themes that emerge from participants' perceptions and experiences, providing a nuanced understanding of online security awareness and practices.

1. Perceived Vulnerability and Trust Issues

Many participants express a generalised sense of insecurity regarding their online accounts, often citing hacking incidents and the potential for unauthorised access as primary concerns. This fear is exacerbated by high-profile breaches in organisations, leading to a distrust in the security measures of online platforms. The mention of "*fearing data hackers*" and considering email communication as fundamentally "*unsafe*" underscores a prevailing scepticism towards the digital infrastructure's ability to protect user data. This perception of vulnerability is not just linked to their own practices but extends to a broader

mistrust in the entities responsible for safeguarding their online presence.

2. Proactive Measures and Security Practices

Contrasting with the expressed fears, some participants detail specific proactive measures they employ to enhance their online security. The use of two-factor authentication and a cautious approach to interacting with suspicious online requests indicate a higher level of security awareness and personal responsibility. This proactive stance suggests that while there is a general concern about online security, individuals are not entirely resigned but instead take steps within their control to mitigate risks. This behaviour reflects an awareness of security practices and a commitment to personal online safety.

3. Reliance on External Protections

A subset of responses highlights a reliance on perceived external protections, such as the security features of frequently visited sites or institutional safeguards. This trust in external protections indicates a segment of users who feel secure not because of their actions but due to their confidence in the security measures implemented by the platforms they use. However, this trust could potentially overlook the limitations of external protections and underestimate the importance of personal security measures.

4. Personal Responsibility and Caution

The sentiment of personal responsibility permeates the responses, with participants emphasising the importance of being careful and not sharing passwords. This awareness of the need for caution in digital interactions suggests a foundational understanding of good security practices among participants. However, the varying degrees of confidence in these measures, from believing in the adequacy of personal practices to acknowledging a persistent risk of breach, reflect the complexity of achieving a sense of security in the online realm.

5. Emotional and Psychological Impact

Finally, the responses touch on the emotional and psychological impact of online security threats. Fears of losing control, property, social connections, and even personal safety underline the profound effect of perceived online vulnerabilities on well-being. The mention of an adaptation process under severe conditions suggests resilience among users, indicating that while threats can induce significant stress, individuals find ways to cope and adjust their behaviours in response to these challenges.

The analysis uncovers a layered landscape of online security perceptions among users. It reveals a delicate balance between fear and proactive behaviour, mistrust in online platforms, and reliance on their protective measures. The findings underscore the importance of enhancing digital literacy and promoting more robust, user-friendly security solutions to address the multifaceted concerns and behaviours identified. Recognizing the emotional and psychological dimensions of online security will be crucial in developing more effective educational programs and interventions that resonate with users' experiences and concerns, ultimately fostering a safer online environment for all.

How confident are you in recognizing and stopping phishing attempts, and what experiences or knowledge have shaped this confidence?

The thematic question regarding confidence in recognizing and stopping phishing attempts, we categorise the responses into three main groups: those who demonstrate a proactive approach against phishing, those who show uncertainty or lack of confidence, and those who rely on non-strategic, instinctive measures. Each group represents a different level of alignment with the proactive and knowledgeable stance that the thematic question probes.

1. Proactive and Knowledgeable Responses

Responses such as "*Once, any phishing attempt, I block immediately*" indicate a high degree of alignment with the thematic question's focus on confidence in recognizing and stopping phishing attempts. These participants show not only awareness but also an active engagement in protective practices against phishing. They represent a group that has either received adequate education on the matter or has developed sufficient personal strategies through experience, standing in strong support of the thematic question by demonstrating both recognition and action.

2. Uncertainty or Lack of Confidence

A significant portion of responses, like "*I don't know how to prevent*" and "*I don't have much confidence*," highlights a direct contrast to the thematic question's inquiry into confidence and action. These participants openly express their insecurity and lack of knowledge regarding phishing detection and prevention, indicating a gap in cybersecurity education and awareness. Their responses are in opposition to the desired outcome suggested by the thematic question, as they reflect a passive stance towards or an acknowledgment of the challenge in dealing with phishing threats effectively.

3. Instinctive and Non-Strategic Measures

Responses that mention reliance on instinct or general caution, such as "*No, I just trust my instinct*" and "*I am always sceptical about online fraudsters*," present a middle ground. While these individuals acknowledge the threat of phishing and attempt to guard against it, their methods may not be grounded in a strategic understanding of phishing tactics or effective prevention measures. Their approach aligns with the thematic question in recognizing the importance of being vigilant against phishing attempts but diverges in the lack of specific, knowledge-based strategies to counteract these threats effectively.

The degree of alignment with the thematic question varies significantly among the responses. While a small segment demonstrates a proactive and knowledgeable stance towards phishing prevention, a larger portion reveals gaps in confidence and awareness, highlighting the need for improved cybersecurity education and resources. The reliance on instinctive measures, although indicative of an awareness of threats, underscores the importance of supplementing such instincts with concrete knowledge and strategies for effective online security practices. While some individuals exhibit a degree of caution and adopt specific protective measures, a significant portion of the responses reflect uncertainty, reliance on instinct, and a lack of comprehensive strategies to combat phishing. These findings underscore the importance of targeted cybersecurity education efforts that address the identified knowledge gaps and misconceptions, empowering individuals with the skills and confidence to navigate the digital world more securely.

How frequently do you update your online account passwords, and why?

The thematic question on password update frequency provides insight into the varied practices and underlying motivations concerning online account security among individuals. The responses span infrequent updates based on perceived security to more systematic approaches triggered by necessity or precaution. These insights illustrate the respondents' alignment with recommended cybersecurity practices, as well as highlight areas of potential vulnerability.

Perceived Security and Infrequent Updates: Many responses, such as "*Rarely*" and "*Hardly update because it is secure*," suggest a strong sense of confidence in their existing password security. This perception of security leads to infrequent updates, with some individuals only changing passwords when prompted by the system. This group's practices align partially with the thematic question by acknowledging the concept of password updates but diverge in the lax approach to frequency, potentially against best practices advocating regular updates for enhanced security.

Compelled by Circumstances: A subset of respondents indicates changing passwords reactively, such as when they forget their password or when specific needs arise. This reactive approach, highlighted in responses like "*I often forget my password and that compels me to change*," represents a departure from proactive security measures, aligning with the thematic question in the acknowledgment of password changes but diverging in the lack of a systematic, security-driven update routine.

Systematic and Precautionary Updates: Contrasting the more passive approaches, some responses suggest a more disciplined strategy, with updates occurring "*So often*" or on a set schedule like "*Once a year*." These individuals appear to recognize the importance of regular password updates as a proactive security measure. Their practices closely align with the thematic question's focus on frequency and rationale, adhering to a more robust stance on cybersecurity.

Misconceptions about Password Sharing and Security: Responses indicating a lack of updates due to non-sharing of passwords, such as "*I don't update as I don't share my password with anyone*," reveal a common misconception that password security is solely compromised through sharing. This perspective overlooks the myriad of ways passwords can be compromised beyond direct sharing, indicating a divergence from the cybersecurity best practices implied in the thematic question.

A significant number of responses exhibit a sense of complacency or misunderstanding of best practices, suggesting a misalignment with the proactive security measures implicit in the thematic question. However, a smaller segment of the respondents demonstrates a precautionary approach to password management, closely aligning with the inquiry's intent and reflecting an adherence to recommended cybersecurity behaviours.

While there is an acknowledgment across most responses of the concept of password updating, the motivations, frequency, and understanding of its importance vary widely. The findings suggest a need for increased awareness and education on the critical role of regular password updates in maintaining online security, addressing misconceptions, and promoting more systematic and proactive practices among users.

How do you manage sharing personal information online, and what precautions do you use, and why are they significant to you?

The responses to the thematic question about managing the sharing of personal information online reveal a general trend towards caution and restraint among participants. These responses are dissected into several key themes that reflect the participants' attitudes and practices towards online privacy, underscoring a predominant concern for safeguarding personal information in the digital realm.

Caution and Restraint: A significant portion of responses, such as "*I share scantily*," "*Hardly share personal info*," and "*I restrain as much as possible*," highlight a deliberate approach to minimise the sharing of personal information online. This cautious stance signifies a high level of awareness regarding the risks associated with oversharing in digital spaces and aligns closely with the thematic question's focus on managing and safeguarding personal information.

Selective Sharing and Trust: Some respondents indicate that they share personal information only in environments they perceive as secure or with individuals who have a legitimate need to know. Phrases like "*I share personal information where I feel secured*" and "*Share it with those that should get it*" suggest an approach that balances the need for online interaction with privacy concerns. This selective sharing based on trust and security perception is in line with the thematic question, reflecting a strategic and mindful approach to online privacy.

Proactive Security Measures: While the thematic question specifically probes sharing practices and precautions, responses such as "*Changing passwords often*" hint at broader security measures participants associate with protecting their personal information. Although not directly about sharing practices, this proactive measure demonstrates an underlying commitment to privacy and security that supports the question's intent.

Explicit Non-sharing Policy: A stance of outright refusal to share personal information online is evident in responses like "*As much as possible, I don't share personal information online*" and "*They are my personal information which I shouldn't share anyhow online*." These responses directly align with the thematic question by underscoring a proactive and explicit policy against the sharing of personal data, reflecting a strong inclination towards privacy preservation.

The emphasis on minimal sharing, selective trust, proactive security measures, and an outright non-sharing policy illustrates a deep-seated concern for personal privacy and a keen awareness of the potential risks posed by digital environments. However, the mention of changing passwords as a precaution, while indicative of a general privacy-conscious mindset, suggests some participants may conflate general security measures with specific practices for managing the sharing of personal information. This conflation notwithstanding, it

still contributes to the overarching theme of caution and protective behaviour online.

The analysis reveals a predominant cautionary approach towards the sharing of personal information online among participants, closely aligning with the concerns and precautions the thematic question aimed to explore. The findings highlight a strong collective awareness of online privacy risks and a commitment to implementing measures that safeguard personal information, reflecting a widespread acknowledgment of the importance of privacy management in the digital age.

How well do you understand common online security threats, and what has contributed to your knowledge in this area?

The responses to the question regarding understanding common online security threats and the sources of that knowledge reveal a range of awareness and learning methods among the respondents. These insights were distilled into themes reflecting varying degrees of familiarity with online security risks and the diverse avenues through which individuals acquire their knowledge.

Varied Levels of Understanding: Participants express a range of understanding regarding online security threats, from "*I know a bit*" and "*Average*" to "*Insignificant, so needs more knowledge*." This variation highlights the disparity in cybersecurity awareness among internet users, underscoring the need for accessible and comprehensive education on these issues.

Educational Sources and Self-Learning: Some respondents attribute their knowledge to specific educational experiences, such as "*The education I had on phishing documents*," while others rely on self-directed learning methods like "*tips and online checks*." This diversity in learning sources suggests that while formal education contributes to awareness, there is also a significant reliance on informal learning and self-education in the digital age.

Acknowledgment of Risks and Caution: A common theme among responses is the acknowledgment of security threats and the consequent cautious behaviour, as seen in "*I am aware of them that is why I am always careful*." This awareness, even if not accompanied by in-depth knowledge, indicates a baseline understanding that online security threats are a genuine concern requiring vigilance.

Fear and Limited Understanding: Fear of specific threats, such as suspicious links, is mentioned as a significant concern, despite a self-professed lack of comprehensive knowledge: "*I'm not very knowledgeable about common online security threats but I fear https links coming from people that I don't know*." This suggests that fear, possibly fueled by media coverage or anecdotal experiences, can be a motivator for cautious online behaviour, even in the absence of detailed knowledge.

Recognition of Cybercrime Tactics: A few responses indicate a more detailed understanding of cybercrime tactics, mentioning phishing, spam, spyware, and malware as tools used by hackers for economic gain. This recognition of specific strategies employed by cybercriminals points to a higher level of cybersecurity literacy among some participants. While the depth of understanding and the confidence in this knowledge vary significantly, the majority acknowledge the existence of these threats and express a desire to learn more or rely on specific strategies to mitigate risks.

However, the responses also reveal a notable gap between awareness and in-depth knowledge. Many participants express a need for further education or a reliance on basic cautionary practices without a robust understanding of the threats they face. This gap suggests an alignment with the thematic question's implication that understanding common online security threats is crucial, but also highlights a divergence in terms of the adequacy of current knowledge levels and learning sources.

The analysis underscores the importance of enhancing cybersecurity education and awareness initiatives to address the varied understanding and educational needs identified. By fostering a more comprehensive and accessible approach to cybersecurity learning, individuals can be better equipped to navigate and protect themselves

against the evolving landscape of online security threats.

Discussion

The exploration of participants' perceptions of their online account security has unearthed a complex landscape of attitudes, behaviours, and emotional responses to digital safety (Ashraf et al., 2023). This examination reveals that while some individuals take proactive measures to safeguard their online presence, a prevailing sense of vulnerability persists among many (Heino & Huotari, 2023). This vulnerability is not only a reflection of personal security practices but also signifies a deeper mistrust in the digital infrastructure and the entities tasked with ensuring online safety (Nguyen & Tran, 2023). High-profile hacking incidents and data breaches have eroded trust in online platforms, prompting a cautious approach to digital interactions (Nguyen & Tran, 2023).

Participants' reliance on both internal and external security measures underscores a layered approach to online safety, balancing personal responsibility with trust in institutional protections (Nguyen & Tran, 2023). This was in consonant with the study of An, et al (2024), where they categorize different types of cyberattacks based on what they target and how they operate, giving a clearer picture of the vulnerabilities in SG systems. Their categorization covers all five functions of the National Institute of Standards and Technology (NIST) cybersecurity framework: Identify, Protect, Detect, Respond, and Recover. This comprehensive approach helps organizations implement well-rounded and strong security measures.

The study's findings underscore the critical importance of enhancing digital literacy and cybersecurity awareness among internet users. The varied degrees of understanding and confidence in handling phishing attempts, coupled with the sporadic updating of passwords, indicate a substantial gap in cybersecurity knowledge (Spencer & Pizio, 2023). These gaps highlight the need for targeted education efforts that address both the technical aspects of online threats and the psychological factors that influence security behaviours (Alsharida et al., 2023). Such initiatives should aim to empower individuals with the knowledge and tools necessary to navigate the digital landscape confidently and securely (Abulibdeh et al., 2024).

Moreover, the discussions on managing personal information online reveal a cautious stance among participants, driven by a legitimate concern for privacy and the potential consequences of data exposure (Cooper et al., 2023). The strategic, minimal sharing of personal information, often dictated by the perceived security of the platform or the necessity of the exchange, illustrates a conscious effort to mitigate risks (Gastaldi et al., 2023). This careful management of personal data, alongside proactive security measures like regular password updates, reflects a foundational understanding of good cybersecurity knowledge among participants (F Naga et al., 2024).

However, the analysis also highlights a significant reliance on instinct and non-strategic measures for some participants, suggesting a need for a more grounded understanding of online threats and their mitigation (Colabianchi, 2023). The fear of suspicious links and the acknowledgment of cybercrime tactics without a comprehensive strategy to counteract these threats point to an awareness influenced more by caution than by an informed understanding of cybersecurity (Alqahtani, 2023).

The emotional and psychological impact of perceived online vulnerabilities cannot be overstated. The fear of losing control, property, social connections, and even personal safety elucidates the profound effect that security threats can have on individuals' well-being (Mock et al., 2023). This dimension of online security underscores the necessity of addressing not only the practical aspects of cybersecurity but also the emotional resilience and coping mechanisms required to navigate online threats effectively (Al-Hashem & Saidi, 2023).

In conclusion, this highlights a delicate balance between fear and proactive behaviour, a balance that is influenced by a variety of factors including knowledge, trust, personal responsibility, and emotional impact. The findings from this study advocate for a multifaceted approach to cybersecurity education and awareness, one that not only enhances digital literacy but also acknowledges and addresses the emotional

dimensions of online security. By fostering a more informed and resilient online community, we can work towards a safer digital environment for all users.

References

Twomey, J., Ching, D., Aylett, M. P., Quayle, M., Linehan, C., & Murphy, G. (2023). Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine. *Plos one*, *18*(10), e0291668.

Rahi, S., Alghizzawi, M., & Ngah, A. H. (2023). Understanding consumer behavior toward adoption of e-wallet with the moderating role of pandemic risk: an integrative perspective. *Kybernetes*.

Jones, E., Samra, R., & Lucassen, M. (2023). Key challenges and opportunities around wellbeing for distance learning students: the online law school experience. *Open Learning: The Journal of Open, Distance and e-Learning*, *38*(2), 117-135.

Rangaraju, S. (2023). Secure by Intelligence: Enhancing Products with AI-Driven Security Measures. *EPH-International Journal of Science and Engineering*, *9*(3), 36-41.

Haugli-Sandvik, M. (2024). Cyber Risk Perception in Offshore Operations: An Exploratory Study of Deck Officers' Perceptions of Cyber Risks in Norwegian Shipping Companies.

Telo, J. (2023). Understanding Security Awareness Among Bank Customers: A Study Using Multiple Regression Analysis. *Sage Science Review of Educational Technology*, *6*(1), 26-38.

Gao, L. (2023). The Art of Communication in the Digital Age: Trends, Challenges, and Innovations. *International Journal of Education and Humanities*, *11*(3), 287-290.

Blackmon, S. J., & Major, C. H. (2023). Inclusion or infringement? A systematic research review of students' perspectives on student privacy in technology-enhanced, hybrid and online courses. *British Journal of Educational Technology*, *54*(6), 1542-1565.

Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21.

Alqudhaibi, A., Krishna, A., Jagtap, S., Williams, N., Afy-Shararah, M., & Salonitis, K. (2024). Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. *Discover Food*, *4*(1), 1-18.

Adewusi, M. A., Adebanjo, A. W., Odekeye, T., & Kazibwe, S. (2024). Rise of the Machines: Exploring the Emergence of Machine Consciousness. European Journal of Theoretical and Applied Sciences, 2 (4), 563-573. DOI: 10.59324/ejtas.2024.2 (4). 48

Ajani, O. A. (2023). Challenges mitigating against effective adoption and usage of e-learning in curriculum delivery in South African universities. *International Journal of Innovative Technologies in Social Science*, (2 (38)).

Fosch-Villaronga, E., & Drukarch, H. (2023). Accounting for diversity in robot design, testbeds, and safety standardization. *International Journal of Social Robotics*, *15*(11), 1871-1889.

Starks, A. C., & Reich, S. M. (2023). "What about special ed?": Barriers and enablers for teaching with technology in special education. *Computers & Education*, *193*, 104665.

Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security*, *130*, 103266.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. European Journal of Information Systems, 25(4), 364-390.

Baltuttis, D., Teubner, T., & Adam, M. T. (2024). A typology of cybersecurity behavior among knowledge workers. Computers & Security, 140, 103741.

Karvonen, K. (2008). Bridging the gap between human and machine trust: applying methods of user-centred design and usability to computer security. Teknillinen korkeakoulu.

Adewusi, M. A., Egbowon, S. E., & Akindoju, G. (2021). COVID-19 pandemic: An indigenously designed platform to the rescue. Journal of Computer Science and Its Application, 28(2), 33-44.

Bowen and Chawla (2012) highlight the crucial role of trust in determining cybersecurity practices, suggesting that fostering trust can enhance security compliance.

F Naga, J., Tinam-isan, A. C., Maluya, M. O., Panal, A. D., & Tupac, T. A. (2024). Investigating the Relationship between Personality Traits and Information Security Awareness. International Journal of Computing and Digital Systems, 16(1), 1-15.

McCarthy, A. M., Maor, D., McConney, A., & Cavanaugh, C. (2023). Digital transformation in education: Critical components for leaders of system change. *Social sciences & humanities open*, *8*(1), 100479.

Adewusi, M. A., Egbowon, S. E., Abodunrin, I., & Rahman, K. (2021). Accra Bespoke

Multidisciplinary Innovations Conference (ABMIC).

Ahmed, S., & Khan, M. (2023). Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem. *AI, IoT and the Fourth Industrial Revolution Review*, *13*(9), 1-17.

Lottu, O. A., Abdul, A. A., Daraojimba, D. O., Alabi, A. M., John-Ladega, A. A., & Daraojimba, C. (2023). Digital transformation in banking: a review of Nigeria's journey to economic prosperity. *International Journal of Advanced Economics*, *5*(8), 215-238.

Ahmad, E. A. (2024). Revolutionizing learning: leveraging social media platforms for empowering open educational resources. *International Journal of e-Learning and Higher Education (IJELHE)*, *19*(1), 83-106.

Adewusi, M. A., Odekeye, T., Egbowon, E. S., Alade, R., & Akindoju, O. G. (2022). Requirement Engineering in Learning Analytics (Machine Learning) in an Indigenously Designed Learning Platform: A Case Study. Advances in Multidisciplinary and Scientific Research Journal, 1, 119-126.

Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors*, *23*(19), 8015.

Aslam, U. (2023). Understanding the usability of retail fashion brand chatbots: Evidence from customer expectations and experiences. *Journal of Retailing and Consumer Services*, *74*, 103377.

Petrovčič, A., Reisdorf, B. C., Grošelj, D., & Prevodnik, K. (2023). A typology of aging internet users: exploring digital gradations in internet skills and uses. *Social Science Computer Review*, *41*(5), 1921-1940.

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *International Journal of Qualitative Methods*, *22*, 16094069231205789.

Adewusi, M. A., Asiimwe, S., & Odekeye, O. T. (2024). PHILOSOPHY OF KNOWLEDGE-THE EPISTEMIC EXPLORATIONS INTO THE DEPTHS OF KNOWLEDGE AND. . . ResearchGate. https://www.researchgate.net/publication/379732176_PHILOSOPHY_OF_KNOWLEDGE-THE_EPISTEMIC_EXPLORATIONS_INTO_THE_DEPTHS_OF_KNOWLEDGE_AND_WISDOM-ISBN-978-620-7-48534-5

Heino, O., & Huotari, V. (2023). How considering memory as an analogy to preparedness reveals its weaknesses. *Risk, Hazards & Crisis in Public Policy*, *14*(3), 209-225.

Ashraf, A., König, C. J., Javed, M., & Mustafa, M. (2023). " Stalking is immoral but not illegal": Understanding Security, Cyber Crimes and Threats in Pakistan. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)* (pp. 37-56).

Nguyen, M. T., & Tran, M. Q. (2023). Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *International Journal of Intelligent Automation and Computing*, *6*(5), 1-12.

Nguyen, M. T., & Tran, M. Q. (2023). Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *International Journal of Intelligent Automation and Computing*, *6*(5), 1-12.

An, C., Huang, M., Lu, X. et al. Polar code-based secure transmission with higher message rate combining channel entropy and computational entropy. Cybersecurity 7, 36 (2024). https://doi.org/10.1186/s42400-024-00229-5

Spencer, M., & Pizio, D. (2023). The de-perimeterisation of information security: The Jericho Forum, zero trust, and narrativity. *Social Studies of Science*, 03063127231221107.

Abulibdeh, A., Zaidan, E., & Abulibdeh, R. (2024). Navigating the confluence of artificial intelligence and education for sustainable development in the era of industry 4.0: Challenges, opportunities, and ethical dimensions. *Journal of Cleaner Production*, 140527.

Gastaldi, L., Appio, F. P., Trabucchi, D., Buganza, T., & Corso, M. (2023). From mutualism to commensalism: Assessing the evolving relationship between complementors and digital platforms. *Information Systems Journal*.

Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: A stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

Colabianchi, S. (2023). Humans in cyber resilience: managerial and operational opportunities.

Alqahtani, H. S. D. (2023). *Analysis and evaluation of cybersecurity awareness using a game-based approach* (Doctoral dissertation, Macquarie University).

Mock, K. O., Moyer, A., & Lobel, M. (2023). Explaining sex discrepancies in sterilization rates in the United States: An evidence-informed commentary. *Perspectives on Sexual and Reproductive Health*, *55*(3), 116-121.