International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (5)

IJCI

المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (5)

May 2024

Assessing the Level of Cybersecurity Awareness and Practices of Application Users and Their Impact on Privacy Policy Consents: A Case Study in Application Downloading

Sabah Abdellatif Hassan Ahmed
Assistant Professor, College of Computers and Information Technology, University of Bisha, Kingdom of Saudi Arabia
sahmad@ub.edu.sa

Abstract

The aim of this study is to understand the level of cybersecurity awareness and practices of application users and determine the impact on their consent to privacy policies through a case study in application downloading. To achieve this aim, this study employs quantitative research methodology. The primary data collection instrument is a structured questionnaire designed to gather insights and perspectives from 65 participants of application users in the Kingdom of Saudi Arabia, including several types of applications. The collected data was collected and analyzed using SPSS software. The findings revealed that most of the study participants disagree that they understand the importance of cybersecurity measures when using mobile applications with a frequency of 27 and a percentage of 41.5%. Also, most of the study participants disagree that they are aware about negative cybersecurity practices with a frequency of 26 and a percentage of 40%. Furthermore, only 23 participants are paying attention to Download applications from only official app stores or trusted sources with a percentage of 35.4% The findings of the study also revealed that a p-value related to Pearson Chi-Square is (0.019) which is less than a significance level

of (0.05), this proves a significant statistical relationship between cybersecurity awareness and practices of application users on privacy policy consents.

Keywords: Cybersecurity Awareness, Application Users, Privacy Policy Consents, Applications Downloading.

Introduction

In today's digital age, mobile applications have become an integral part of our daily lives, offering a plethora of services and conveniences at our fingertips (Goel et al., 2023). However, as we embrace these technological advancements, concerns regarding cybersecurity and privacy have come to the forefront (Chang et al., 2023). With the ever-increasing number of cyber threats and data breaches, it is crucial to understand the level of awareness and practices among application users regarding cybersecurity and privacy (Mungo et al., 2024).

Mobile applications often request access to various permissions, including personal data, location, and other sensitive information (Ambore et al., 2017). While these permissions may be necessary for the application to function properly, users frequently grant them without fully comprehending the implications or reading the privacy policies (Brown et al., 2023). This lack of awareness and understanding can potentially compromise users' privacy and expose them to cyber risks (Zhang and He, 2019).

Furthermore, the widespread use of mobile applications has led to the accumulation of vast amounts of personal data, which can be a lucrative target for cybercriminals (Mumford and Shires, 2023). Inadequate cybersecurity measures or a lack of awareness among users can make them vulnerable to various cyber threats, such as malware, phishing attacks, and data breaches (Mary and Tiwari, 2017).

Recognizing the significance of this issue, it is essential to assess the level of cybersecurity awareness and practices among application users and investigate their impact on privacy policy consents (Wang, 2019). By understanding the current state of awareness and the factors influencing users' decisions to grant or deny permissions, we can develop strategies to enhance cybersecurity education and promote more informed decision-making (Cristiano et al., 2024).

In Saudi Arabia, the adoption of mobile applications has been rapidly increasing, driven by the growing demand for digital services and the country's efforts to foster a thriving digital economy. However, as the usage of mobile applications continues to rise, so do the potential risks associated with cybersecurity and privacy concerns (Alammary et al., 2022).

The Saudi Arabian government has recognized the importance of cybersecurity and has taken steps to enhance the country's cybersecurity capabilities. However, the effectiveness of these efforts may be limited if users lack awareness and proper practices when it comes to granting permissions and consenting to privacy policies of using mobile applications (Zadeh et al., 2021).

It is important to evaluate the level of cybersecurity awareness among application users, including their understanding of potential risks, threats, and the importance of cybersecurity measures (AlBenJasim et al., 2023). Furthermore, it is essential to investigate users' comprehension of privacy policies and their ability to interpret the implications of granting or denying permissions to applications (Aggarwal and Reddie, 2018).

This study aims to explore the factors that influence users' decisions to grant or deny permissions to applications, such as perceived benefits, convenience, trust in the application developer, and awareness of potential risks (Kanwal et al., 2022). And it aims to determine the impact of users' cybersecurity practices, such as updating

software, using antivirus software, and implementing security measures, on their decision to grant or deny permissions to applications.

Problem Definition

Mobile applications have become an integral part of our daily lives, providing users with a wide range of services and functionalities. However, the widespread use of mobile apps has also raised significant concerns regarding user privacy and data security. Many apps collect and share sensitive user data, often without providing clear and transparent information to users about how their data is being used. While app developers are required to provide privacy policies outlining their data collection and usage practices, these policies are often long, complex, and difficult for the average user to understand. As a result, users frequently agree to these policies without fully comprehending the implications, potentially exposing their personal data to misuse or unauthorized access. Furthermore, users' level of cybersecurity awareness and practices can significantly impact their ability to make informed decisions regarding privacy policy consents. Users with limited cybersecurity knowledge may be more likely to overlook or disregard potential risks, while those with more awareness may be better equipped to evaluate the privacy implications of app installations.

Research Objectives

The main objectives of these studies are to:

1. Understand the level of cybersecurity awareness and practices of application users and determine the impact on their consent to privacy policies.
2. Assess the level of awareness of application users regarding cybersecurity risks and potential threats.
3. Analyze application users' practices regarding cybersecurity such as choosing passwords, updating applications, and using secure networks.

4. Evaluate the extent to which application users understand privacy policies and their implications for sharing their personal data.
5. Analyze the impact that users' level of cybersecurity awareness can have on their decisions to agree to privacy policies.
6. Develop practical recommendations to enhance application users' awareness of cybersecurity risks and improve their behavior regarding keeping personal data safe.

Research Questions

1. What is the level of awareness of application users about cybersecurity risks and potential threats?
2. What are the practices of application users regarding cybersecurity such as choosing passwords, updating applications, and using secure networks?
3. How do app users understand privacy policies and their implications for sharing their personal data?
4. What impact can users' level of cybersecurity awareness have on their decisions to agree to privacy policies?
5. How can practical recommendations be developed to enhance application users' awareness of cybersecurity risks and improve their behavior regarding keeping personal data secure?

Research Hypotheses

H1: The level of cybersecurity awareness among application users in Saudi Arabia is low, and many users are unaware of the potential risks and threats associated with mobile applications.

H2: Application users in Saudi Arabia often exhibit poor cybersecurity practices, such as using weak passwords, failing to update applications regularly, and

connecting to unsecured networks, which can increase their vulnerability to cyber threats.

H3: Many application users in Saudi Arabia have a limited understanding of privacy policies and their implications for sharing personal data, leading them to grant permissions without fully comprehending the consequences.

Importance of the Research

The importance of this research is multifaceted and has significant implications for various stakeholders, including users, app developers, and the user Education and Awareness Campaigns.

1. This study sheds light on the critical issue of user privacy and data protection in the context of mobile app usage. By assessing users' cybersecurity awareness and practices, it provides valuable insights into the factors that influence their understanding and acceptance of privacy policies. This knowledge can empower users to make more informed decisions about their data sharing and help them better protect their personal information.
2. The findings of this research can contribute to increased transparency and accountability in the data practices of app developers and service providers. Through identifying gaps in user understanding and areas of concern, it can inform the development of more clear and accessible privacy policies, fostering trust and ethical data management practices within the industry.
3. The research outcomes can provide valuable insights for developing effective user education and awareness campaigns. by understanding the factors that influence users' cybersecurity awareness and practices, stakeholders can design targeted campaigns and educational resources to enhance users' understanding of data privacy risks and empower them to make more informed choices.

International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (5)
IJCI
May 2024
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (5)

Research Domain and Limitations

This research falls within the domain of human-computer interaction (HCI), with a specific focus on user behavior, privacy, and security in the context of mobile applications. It draws upon principles and methodologies from various disciplines, including computer science, psychology, and behavioral economics, to holistically examine the interplay between users' cybersecurity awareness, practices, and their decision-making processes regarding privacy policy consents.

The scope of the study is centered on the application downloading process, as this represents a critical juncture where users are presented with privacy policies and required to make decisions about data sharing. However, it is important to note that the findings and implications of this research may extend beyond the specific context of app downloads and hold relevance for broader digital services and platforms that involve user data collection and privacy considerations.

While the research aims to provide valuable insights and recommendations, it is subject to certain limitations inherent in its methodological approach and the dynamic nature of the digital landscape. These limitations include:

1. Sample Representation: The study relies on a specific sample of application users (sample comprises 65 participants), which may not be fully representative of the diverse user population across different geographic regions, demographic groups, and technological proficiency levels.
2. Rapidly Evolving Technology Landscape: The digital world, including mobile applications and privacy practices, is constantly evolving. As new technologies, platforms, and regulations emerge, the findings of this study may require periodic reevaluation and updating to maintain their relevance and applicability.
3. Subjectivity in User Perceptions and Behaviors: User perceptions, attitudes, and behaviors related to cybersecurity and privacy are inherently subjective and

influenced by various factors, such as personal experiences, cultural norms, and individual risk tolerance.

Despite these limitations, the research aims to provide a robust and rigorous examination of the current landscape, offering valuable insights and recommendations to enhance user awareness, protect privacy, and promote responsible data practices within the digital ecosystem.

Research Methodology

To achieve the study aim, this study employs quantitative research methodology where questionnaires were the primary data collection tool (Snyder, 2019).

Study Sample

The study sample comprises 65 participants carefully selected to represent various application users which have different interests, experiences, and education.

Data Collection

A questionnaire was developed in consultation with experts ensuring the clarity and validity of the questions. It consists of closed-ended questions, utilizing Likert 5-point scales and multiple-choice format.

The questionnaire was distributed through various channels, including email and online platforms to be suitable to the preferences and accessibility of the study participants. Appropriate precautions were taken to maintain the anonymity and confidentiality of the respondents.

The collected data underwent accurate statistical analysis, including descriptive statistics and inferential statistics, to identify patterns and relationships among the variables using "SPSS" statistical software.

International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (5)
IJCI
May 2024
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (5)

Data Analysis

Through using a 5-point Likert scale, these closed-ended questions allow respondents to indicate their level of agreement or disagreement with each statement or question, providing quantifiable data for analysis.

1- Age groups:

Table 1: age groups of the participants

What is your age group?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	16	24.6	24.6	24.6
	25-34	23	35.4	35.4	60.0
	35-44	15	23.0	23.0	83.0
	55 years or above	11	16.9	16.9	100.0
	Total	65	100.0	100.0	

Table 1 indicates the age groups of the participants, most of the participants are within the young generation (25-34) years old with a percentage of 35.4%.

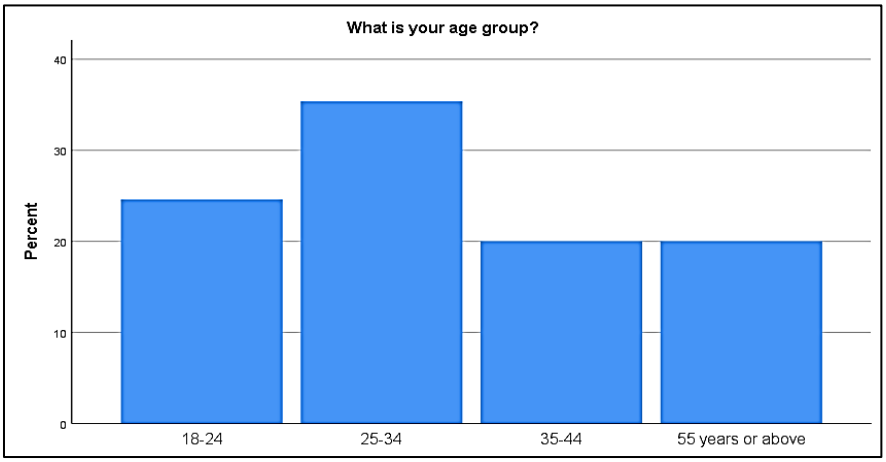

Figure 1: age groups of the participants

International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (5)
IJCI
May 2024
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (5)

2- Gender of the participants:

Table 2: gender of the participants

What is your gender?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	27	41.5	41.5	41.5
	Male	38	58.5	58.5	100.0
	Total	65	100.0	100.0	

Table 2 indicates the gender of the participants, most of the participants are males (38 participants) with a percentage of 58.5%, and females are (27 participants) with a percentage of 41.5%.

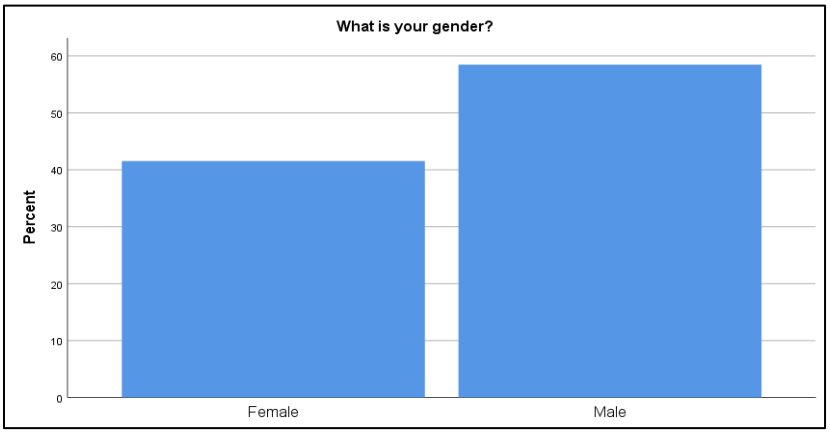

Figure 2: gender groups of the participants

International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (5)
IJCI
May 2024
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (5)

3- level of education of the participants:

Table 3: highest level of education of the participants

What is the highest level of education you have completed?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bachelor's degree	30	46.2	46.2	46.2
	Doctoral degree	8	12.3	12.3	58.5
	High school	13	20.0	20.0	78.5
	Master's degree	14	21.5	21.5	100.0
	Total	65	100.0	100.0	

Table 3 indicates the highest level of education of the participants, most of the participants have bachelor's degrees (30 participants) with a percentage of 46.2%, and master's degrees are (14 participants) with a percentage of 21.5%.

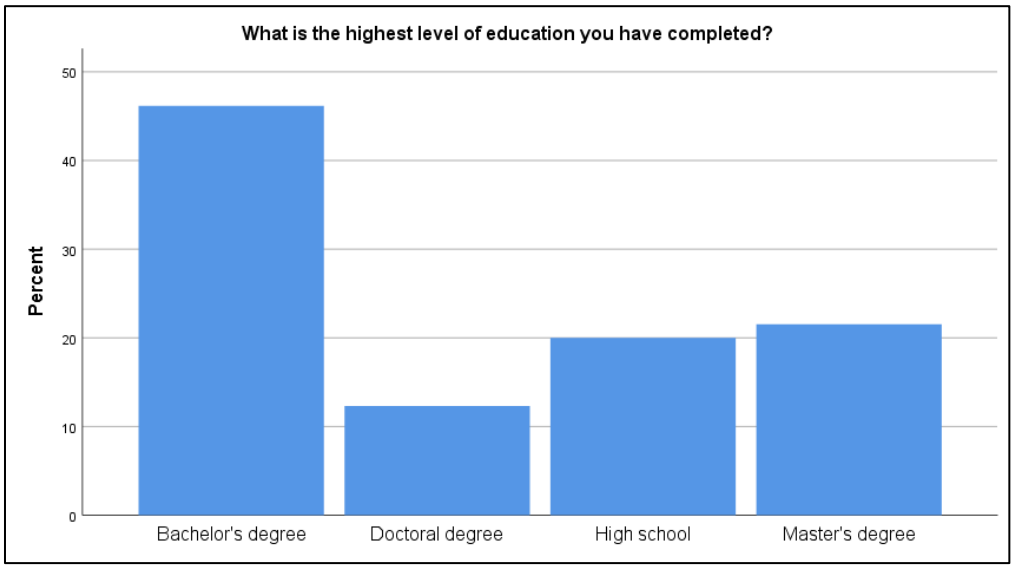

Figure 3: highest level of education of the participants

4- I understand the importance of cybersecurity measures when using mobile applications.

Table 4: the level of cybersecurity awareness when using mobile applications.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	14	21.5	21.5	21.5
	Disagree	27	41.5	41.5	63.1
	Neutral	4	6.2	6.2	69.2
	Strongly Agree	4	6.2	6.2	75.4
	Strongly Disagree	16	24.6	24.6	100.0
	Total	65	100.0	100.0	

Table 4 indicates that most of the study participants disagree that they understand the importance of cybersecurity measures when using mobile applications with a frequency of 27 and a percentage of 41.5%. Which confirms the first hypotheses "the level of cybersecurity awareness among application users in Saudi Arabia is low, and many users are unaware of the potential risks and threats associated with mobile applications.

5- I'm aware about negative cybersecurity practices, such as using weak passwords, failing to update applications regularly, and connecting to unsecured networks.

Table 5: Awareness about negative cybersecurity practices

		Frequency	Percent	Cumulative Percent
Valid	Agree	20	30.8	30.8
	Disagree	26	40.0	70.8
	Neutral	8	12.3	83.1
	Strongly Agree	3	4.6	87.7
	Strongly Disagree	8	12.3	100.0
	Total	65	100.0	

Table 5 indicates that most of the study participants disagree that they are aware about negative cybersecurity practices with a frequency of 26 and a percentage of 40%. Which confirms the second hypotheses "Application users in Saudi Arabia often exhibit poor cybersecurity practices, such as using weak passwords, failing to update applications regularly, and connecting to unsecured networks, which can increase their vulnerability to cyber threats".

6- My understanding of privacy policies affects my willingness to share personal data with mobile applications.

Table 6: understanding of privacy policies

		Frequency	Percent	Cumulative Percent
Valid	Agree	30	46.2	46.2
	Disagree	23	35.4	81.5
	Neutral	2	3.1	84.6
	Strongly Agree	4	6.2	90.8
	Strongly Disagree	6	9.2	100.0
	Total	65	100.0	

Table 6 indicates that most of the study participants agree that they have a significant understanding of privacy policies related to mobile applications, with a frequency of 30 and a percentage of 46.2%.

Which not confirms the third hypotheses "Many application users in Saudi Arabia have a limited understanding of privacy policies and their implications for sharing personal data, leading them to grant permissions without fully comprehending the consequences".

International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (5)
IJCI
May 2024
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (5)

7- **Review the permissions requested by an application before downloading and installing it.**

Table 7: Review the permissions before downloading application.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	33	50.8	50.8	50.8
	Disagree	18	27.7	27.7	78.5
	Neutral	3	4.6	4.6	83.1
	Strongly Agree	3	4.6	4.6	87.7
	Strongly Disagree	8	12.3	12.3	100.0
	Total	65	100.0	100.0	

Table 7 indicates that 33 participants agree that they review the permissions requested by an application before downloading and installing it with a percentage of 50.8%.

There are 18 participants who disagree that they review the permissions requested by an application before downloading and installing it with a percentage of 27.7%. which is a good indicator of the high cybersecurity awareness.

8- **Download applications from official app stores or trusted sources.**

Table 8: Download applications from trusted sources.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	23	35.4	35.4	35.4
	Disagree	29	44.6	44.6	80.0
	Neutral	3	4.6	4.6	84.6
	Strongly Agree	1	1.5	1.5	86.2
	Strongly Disagree	9	13.8	13.8	100.0
	Total	65	100.0	100.0	

Table 8 indicates that only 23 participants are paying attention to Download applications from only official app stores or trusted sources with a percentage of 35.4%,

There are 29 participants who disagree that they are paying attention to download applications from only official app stores or trusted sources with a percentage of 44.6%. which is a very risky indicator as downloading applications from untrusted sources may cause several cybersecurity risks.

9- The effect of cybersecurity awareness and practices of application users on privacy policy consents

Table 8: Chi-Square Test to measure the effect of cybersecurity awareness and practices of application users on privacy policy consents.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	13.724[a]	16	.019
Likelihood Ratio	16.727	16	.003
N of Valid Cases	65		
a. 21 cells (84.0%) have expected count less than 5. The minimum expected count is .18.			

Table 9 indicates that a p-value related to Pearson Chi-Square is (0.019) which is less than a significance level of (0.05), this proves a significant statistical relationship between cybersecurity awareness and practices of application users on privacy policy consents. This positive relationship indicates that as cybersecurity awareness increases, the practices of application users on privacy policy consents enhanced accordingly.

Results and Discussion

The finding of this study revealed that there is a significant statistical relationship between cybersecurity awareness and practices of application users on privacy policy consents. Which was proven by a p-value related to Pearson Chi-Square is (0.019) which is less than a significance level of (0.05).

The findings of this study provide valuable insights into the current state of cybersecurity awareness, practices, and understanding of privacy policies among mobile application users in Saudi Arabia. The results have implications for various stakeholders, including policymakers, application developers, educational institutions, and end-users themselves.

One of the key findings of the study is the generally low level of cybersecurity awareness among application users in Saudi Arabia. This lack of awareness may contribute to users' vulnerability to cyber threats and their tendency to grant permissions without fully comprehending the implications. These findings align with previous studies conducted in other regions, which have highlighted the need for increased cybersecurity education and awareness campaigns.

Furthermore, the study revealed that many users exhibit poor cybersecurity practices, such as using weak passwords, failing to update applications regularly, and connecting to unsecured networks. These practices can expose users to various cyber threats, including malware, phishing attacks, and data breaches. This finding underscores the importance of promoting best practices and fostering a culture of cybersecurity among application users.

Interestingly, the results also indicated that even when users are aware of potential risks and threats, their understanding of privacy policies remains limited. The complexity and legal jargon used in these policies can create barriers to comprehension, leading users to grant permissions without fully understanding the implications for their personal data.

This highlights the need for application developers to adopt more user-friendly and transparent privacy policies, as well as the importance of educational initiatives to improve users' ability to interpret and understand these policies. The study also revealed that a higher level of cybersecurity awareness was positively associated

with more cautious behavior regarding granting permissions and sharing personal data. Users who were more aware of the risks and potential threats were more likely to exercise caution when consenting to privacy policies and granting permissions to applications.

This finding reinforces the significance of raising cybersecurity awareness to empower users to make informed decisions and protect their personal data. It is worth noting that the study found some variations in cybersecurity awareness and practices across different demographic groups, such as age, education level, and technology proficiency. These differences suggest that targeted awareness campaigns and educational initiatives may be necessary to address the specific needs and challenges faced by diverse segments of the population.

While the findings of this study contribute to our understanding of cybersecurity awareness and practices among application users in Saudi Arabia, there are certain limitations that should be acknowledged. First, the study relied on self-reported data, which may be subject to response biases or inaccuracies. Additionally, the sample size and geographic coverage of the study may limit the generalizability of the findings to the entire population of Saudi Arabia.

Despite these limitations, the insights gained from this study have important implications for policymakers, application developers, educational institutions, and end-users themselves. By addressing the identified gaps in cybersecurity awareness and promoting best practices, stakeholders can work towards creating a safer and more secure digital environment for mobile application users in Saudi Arabia.

Recommendations

Based on the findings of this study, the following recommendations are proposed to enhance cybersecurity awareness and promote responsible decision-making among application users in Saudi Arabia:

1. Develop and implement comprehensive cybersecurity education programs targeting different age groups and sectors of society. These programs should focus on raising awareness about potential cyber threats, best practices for cybersecurity, and the importance of understanding privacy policies.
2. Encourage application developers to adopt user-friendly privacy policies that are clear, concise, and easily understandable. These policies should be written in simple language and highlight the key points regarding data collection, usage, and sharing practices.
3. Implement transparent and user-friendly consent mechanisms that clearly explain the permissions requested by applications and their implications. Users should be able to easily understand the consequences of granting or denying permissions.
4. Collaborate with educational institutions to incorporate cybersecurity and privacy awareness into their curricula. This will ensure that future generations are equipped with the necessary knowledge and skills to navigate the digital world safely.
5. Utilize social media platforms and engage with influencers to disseminate cybersecurity and privacy awareness messages. This approach can effectively reach a wide audience, particularly younger generations, who are active social media users.
6. Develop initiatives to promote parental involvement in educating children about cybersecurity and privacy. Parents play a crucial role in shaping their children's understanding and practices regarding digital safety.
7. Review and strengthen existing regulatory frameworks related to cybersecurity, data protection, and privacy in Saudi Arabia. Ensure that these frameworks are up-to-date, enforceable, and aligned with international best practices.

Conclusion

The proliferation of mobile applications and the digitalization of various aspects of life have brought about unprecedented convenience but also heightened concerns regarding cybersecurity and privacy. This study aimed to assess the level of cybersecurity awareness and practices among application users in Saudi Arabia and their impact on privacy policy consents. The findings of this study have shed light on the current state of cybersecurity awareness and practices among application users in Saudi Arabia, highlighting areas that require improvement. By identifying the factors influencing users' decisions to grant or deny permissions and their comprehension of privacy policies, this study provides valuable insights for developing effective strategies to enhance cybersecurity education and promote responsible decision-making.

Addressing the challenges of cybersecurity and privacy in the digital realm requires a multi-faceted approach involving government agencies, educational institutions, application developers, and users themselves. By implementing the recommendations outlined in this study and fostering collaboration among stakeholders, Saudi Arabia can take significant strides towards creating a safer and more secure digital environment for its citizens. It is crucial to recognize that cybersecurity and privacy are not static concerns but rather evolving challenges that require continuous vigilance, adaptation, and proactive measures. As technology advances and new threats emerge, it is imperative to remain committed to raising awareness, promoting best practices, and empowering individuals to navigate the digital landscape with confidence and security.

Future Work

While this study provides valuable insights into the cybersecurity awareness and practices of application users in Saudi Arabia, there are several areas that warrant further investigation:

1. Conduct longitudinal studies to track changes in cybersecurity awareness and practices over time. This will help evaluate the effectiveness of implemented strategies and identify emerging trends or challenges.
2. Perform comparative studies across different regions or countries to identify cultural, social, or regulatory factors that may influence cybersecurity awareness and practices.
3. Investigate cybersecurity awareness and practices in specific sectors, such as healthcare, finance, or government, where the impact of cyber threats and data breaches can be particularly severe.
4. Explore the implications of emerging technologies, such as the Internet of Things (IoT), artificial intelligence (AI), and quantum computing, on cybersecurity awareness and practices. Address new and evolving cyber threats that may arise.
5. Investigate strategies to develop and strengthen the cybersecurity workforce in Saudi Arabia, ensuring that organizations have access to skilled professionals capable of implementing and maintaining robust cybersecurity measures.
6. Foster international collaboration and knowledge sharing among researchers, policymakers, and industry experts to address global cybersecurity challenges and promote best practices.

References

- Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2021). Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. Journal of Computer Information Systems, 61(3), 195–206. https://doi.org/10.1080/08874417.2019.1579076.

- Goel, L., Zhang, J. Z., & Williamson, S. (2023). IT assimilation: construct, measurement, and implications in cybersecurity. Enterprise Information Systems, 17(7). https://doi.org/10.1080/17517575.2022.2052187.
- Ambore, S., Richardson, C., Dogan, H., Apeh, E., & Osselton, D. (2017). A resilient cybersecurity framework for Mobile Financial Services (MFS). Journal of Cyber Security Technology, 1(3–4), 202–224. https://doi.org/10.1080/23742917.2017.1386483.
- Chang, V., Golightly, L., Xu, Q. A., Boonmee, T., & Liu, B. S. (2023). Cybersecurity for children: an investigation into the application of social media. Enterprise Information Systems, 17(11). https://doi.org/10.1080/17517575.2023.2188122.
- Mungo, J. (2024). Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks. Journal of Cyber Security Technology, 8(2), 71–119. https://doi.org/10.1080/23742917.2023.2244210
- He, W., & Zhang, Z. (Justin). (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce, 29(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528
- Alammary, A., Alshaikh, M., & Alhogail, A. (2022). The impact of the COVID-19 pandemic on the adoption of e-learning among academics in Saudi Arabia. Behaviour & Information Technology, 41(14), 3138–3160. https://doi.org/10.1080/0144929X.2021.1973106
- Jeyaraj, A., Zadeh, A., & Sethi, V. (2021). Cybersecurity Threats and Organisational Response: Textual Analysis and Panel Regression. Journal of Business Analytics, 4(1), 26–39. https://doi.org/10.1080/2573234X.2020.1863750
- Mumford, D., & Shires, J. (2023). Toward a Decolonial Cybersecurity: Interrogating the Racial-Epistemic Hierarchies That Constitute Cybersecurity Expertise. Security Studies, 32(4–5), 622–652. https://doi.org/10.1080/09636412.2023.2230879

- Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C. H. (2022). Maritime cybersecurity: are onboard systems ready? Maritime Policy & Management, 1–19. https://doi.org/10.1080/03088839.2022.2124464.
- Aggarwal, V. K., & Reddie, A. W. (2018). Comparative industrial policy and cybersecurity: the US case. Journal of Cyber Policy, 3(3), 445–466. https://doi.org/10.1080/23738871.2018.1551910
- Wang, S., & Wang, H. (2019). Knowledge Management for Cybersecurity in Business Organizations: A Case Study. Journal of Computer Information Systems, 1–8. https://doi.org/10.1080/08874417.2019.1571458.
- Ani, U. P. D., He, H. (Mary), & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology, 1(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211.
- Cristiano, F., Kurowska, X., Stevens, T., Hurel, L. M., Fouad, N. S., Cavelty, M. D., … Shires, J. (2024). Cybersecurity and the politics of knowledge production: towards a reflexive practice. Journal of Cyber Policy, 1–34. https://doi.org/10.1080/23738871.2023.2287687.
- AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2023). FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study. Journal of Computer Information Systems, 1–17. https://doi.org/10.1080/08874417.2023.2251455
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines, Journal of Business Research, 104, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039