Library Progress International *Print version ISSN 0970 1052*
Vol.44, No.3, Jul-Dec 2024: P. 11558-11566 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Security And Privacy Of Mobile Banking In Qatar: A Case Highlighting Current Challenges And Future Recommendations

Amira Omar M M Ali[1*], Dr. Avtar Singh[2]

[1*]Research Scholar, Mittal School of Business, Lovely Professional UniversityEmail: ameera82@icloud.com
[2]Associate Professor, Mittal School of Business, Lovely Professional University Email: avtar257@gmail.com

How to cite this article: Amira Omar M M Ali, Avtar Singh (2024). Security And Privacy Of Mobile Banking In Qatar: A Case Highlighting Current Challenges And Future Recommendations Library Progress International, 44(3), 11558-11566.

Abstract
This study explores the multidimensional security and privacy issues in mobile banking within Qatar through semi-structured interviews with seven key industry participants, including representatives from the Qatari Central Bank, cybersecurity specialists, bankers, a mobile banking technology provider, and an academic expert in digital security. Using thematic analysis based on Braun and Clarke's framework, the study identifies key themes: regulatory challenges, technological vulnerabilities, user behavior and education, and future trends in mobile banking security. The findings reveal the necessity for continuous enhancement of regulatory frameworks, adoption of advanced technological solutions, comprehensive user education programs, and a balanced approach to security and user experience. The study provides valuable insights into the current landscape and future directions for mobile banking security in Qatar, highlighting the importance of a proactive, collaborative approach to safeguarding against cyber threats.

Keywords: Mobile Banking, Security, Privacy, Regulatory Frameworks, Cybersecurity, User Behavior, Technological Vulnerabilities, Qatar

Introduction

Mobile banking is rapidly increasing in usage in Qatar, and through the use of this opinion of mobile banking, consumers have benefited through enhanced convenience and accessibility when using banking facilities (Khan et al., 2015). But, the rapidly emerging mobile banking also poses greater risks to users' identity and institutions' security and privacy. These challenges must be faced and solved as people utilise mobile banking services; it is essential to implement and create strong security features that can address these threats in the banking sector and for individuals (Alsalem & Abu-Shanab, 2022).

The current context of mobile banking security and privacy in Qatar could be described by a number of factors, including the ongoing development of new and more sophisticated threats from hackers (Al-Mhiqani et al., 2018). The existing loopholes that surround mobile banking applications and networks have increased the need for the education of users and the assurance of safe practices in mobile banking (Au & Kauffman, 2008). The main actors in this threat landscape are innovative and often change their strategies, focusing on the uses of malware, phishing attacks, and man-in-the-middle tricks in order to gain unauthorised access to financial information and damage mobile banking systems (Alsayed & Bilgrami, 2017). However, common threats targeting mobile applications and the overall architectures of the managed mobile banking applications, like insecure data storage, weak authentication methods and ineffective application updating, offer enough openings for these threats to work (Weichbroth & Łysik, 2020). This is made worse again by the fact that users are not equally knowledgeable, and some are bound to engage in risky behaviours, as seen through the use of weak passwords and failure to update mobile banking apps, among others (Sharma et al., 2021).

Security features show that mobile banking apps have a significant number of risks and deficiencies, meaning that protection requirements in Qatar are insufficient (Tsobdjou et al., 2024). The issues are the use of mobile external storage, so, hardcoded urls, insecure functions, broadcast receiver permission, log files in the app, ECB cipher, empty certificate method, data backup in manifest, and no check permission functions (Al-Delayel, 2022). The activities displayed in both apps present risks of security that can cause acts of breach of privacy and invasions. Therefore, the research community can be expanded to future research to reveal insights in to security vulnerabilities in Android and iOS banking applications in Qatar to minimise risks for users (Bassolé et al., 2020). Some of the recommendations for improvement are to adopt APK Signature Scheme V2 or V3; utilise SHA-256 or SHA-512 for enhanced security; avoid log prints, web views and

insecure function; Secure code through tools like "SAST by KIUWAN"; minimise extraneous data retention; Train the payment blocking models through artificial intelligence and machine learning (Omeleze & Venter, 2013).
The purpose of this study is to gain essential information regarding the security and privacy of mobile banking in the context of Qatar by assessing the current practices of mobile banking, comparing them with global standards, examining the security policies and regulatory mechanisms currently in use, learning more about the consumers' behavior, as well as identifying the most significant cyber risks and establishing the trends that may be expected in the near future.

Literature Review

Technological Infrastructure and Security Protocols:

The technological transformation of mobile banking in Qatar in the current state of mobile banking in Qatar, the technological infrastructure has been experiencing a significant development and adopting innovations to satisfy the growing demand for digital financial services (Abdul-Wahab & Haron, 2017). The mobile networks in the country have been through substantial developments regarding the overall connectivity and access to such networks with the use of 4G and 5G technologies being implemented (Akpakwu et al., 2017). On the level of security protocols, Qatari banks have put in place various structures or policies to boost the security and privacy of mobile banking (Javed et al., 2021). HTTPS and E2EE are the popular encryption which is employed to secure the data in transmission (Sangwan et al., 2021). Also, two-step verification, which takes the form of a user entering a password or a pin and then a temporary code sent to the user's registered mobile phone to further authenticate that person's login, is a common security mechanism in mobile banking in Qatar (Al-Delayel, 2022). The study evaluates two Android m-banking applications in Qatar, revealing security weaknesses and recommending a more robust approach to enhance user confidence and prompt service delivery (Al-Delayel, 2022).
Biometric verification has also been an emerging feature in the Qatari mobile banking space today where many banking applications have incorporated biometric methods of verification which involve facial or fingerprint recognition of the users (Khan et al., 2023). These biometric mechanisms have been shown to be very useful in preventing the access of unauthorised personnel and in providing overall user convenience (Millett & Pato, 2010). Nevertheless, the adoption of mobile banking systems in Qatar and the issues associated with technological changes and their application have certain impediments attached. Financial institutions face a number of challenges when it comes to implementing change and new technologies often need to work in an environment of old systems (Kruse et al., 2019).

Regulatory Framework and Compliance:

Most of the legal and regulatory frameworks that provide governance to the mobile banking sector in Qatar are administered by the Qatar Central Bank (QCB), which is the central banking institution in the state of Qatar (Albinali, 2023). The QCB has oversight over mobile banking and it has in place strong regulatory policies to enhance security and privacy (Sun, 2020). The 2016 Data Protection and Privacy Law mandates banks to obtain explicit customer consent before collecting, processing, and storing their data (Rojas, 2021). It includes regulations for data management, encryption, and breach response. QCB has specific regulations for mobile banking, including customer verification, transaction recording, and incident reporting (Rojas, 2021). The QCB continuously reviews the mobile banking segment, ensuring security and compliance with the law, through routine audits and inspections by government and financial institutions (Wheeb, 2023). The central bank also works with other regulators including separate ministries of transportation, communication to identify security risks and plan the response (Badran, 2023). Financial institutions are required to ensure security in mobile banking systems through regular audits, vulnerability testing, and industry-standard practices (Council, 2005). They must also have an effective incident response plan to respond to threats and mitigate incidents.

User Awareness and Behavior:

The study has shown that Qatari mobile banking users are moderately aware of potential security threats but are more likely to engage in risky behaviors, making them easy targets for cybercriminals (Apaua & Lallie, 2022). Some identified common behaviors are the use of weak passwords, failing to update applications, using insecure public wireless networks, and doing what phishing scams compel them to do. These behaviors make users vulnerable to attacks such as eavesdropping and man-in-the-middle attacks where their sensitive information is easily retrieved (Al-Hababi & Tokgoz, 2020). Users should be vigilant about app and operating system updates to enhance security, as the issue cannot be resolved easily (Pearce et al., 2013). The study explores factors influencing customers' intention to adopt Mobile Payment Device (MPD) technology in Qatar, using the Unified Theory of Acceptance and Use of Technology Model. Results show performance expectancy, social influence, and perceived information security significantly impact consumer behavior, while demographic factors moderate the relationship (Musa et al., 2015). The factors influencing mobile banking adoption in Qatar using the technology acceptance model and information system success model. Data from 288 participants revealed service quality, perceived usefulness, and ease of use as significant influences. Trust, system quality, and information quality are not significantly influenced by Qatari perceptions and adoption intentions (Al-Naimi & Abu-Shanab, 2024). A cross-national study reveals that age and gender significantly influence consumer intentions and use of mobile banking services. The study, which involved 897 Lebanese and British mobile banking users, found that age moderated consumer behavioral intention, while gender had a significant moderating effect on performance expectancy, effort expectancy, facilitating conditions, price value, and perceived security. This research provides insights into mobile banking adoption variation between different countries (Merhi et al., 2021).

Cyber Threats and Vulnerabilities:

Cyber risks for mobile banking in quantum include Malware, phishing, Man-in-the-Middle (MitM), poor data storage, low authentication techniques, unpatched software's, and outdated network communication protocols (Das & Ganguly, 2024). Malware can also capture user ids, passwords, hijack the transactions, and go around peeking into the financial data that has been restricted for unauthorised access (Team, 2014). Phishing tries to get the user to interpret something as trusted when it is not by using misleading websites or emails to pose as someone trustworthy to get the victim to think that clicking on a link or handing over login credentials is the proper way to do something (Downs et al., 2006). Potential risks of the threats against the mobile banking networks include exposure of extra data in the communication channel, modification of communication and other attacks which can enable the attackers to gains full control of the victim's mobile banking account (Sharma et al., 2022). The survey reveals that cybercrime in Qatar primarily involves website hacking, email cyberattacks, and online banking cyberattacks, driven by monetary gains. IT experts suggest measures like stronger networks and updated protective software to control cybercrime activities and hazards (Nasser, 2020). Financial service providers in Saudi Arabia, Qatar, and Turkey are leveraging FinTech to improve accessibility and quality of services. Banking and payment services are key sectors, but legal frameworks and security risks remain. Financial and regulatory support has spurred rapid growth, with the trend expected to continue (Najafi et al., 2024). Through a range of educational programs, it is now possible to identify several actions that Qatari financial institutions have taken to increase their user's level of understanding and safe practices. The implementation of strict application security tips, social awareness creation, and user sensitization has shown moderate efficacy, as user change and promotion of a strong security culture have not always been successful (Alnoaimi, 2016). This means that an integrated system will need to be implemented to improve the levels of awareness regarding the dangers of using mobile banking facilities and how users can protect themselves from such dangers (Luo et al., 2010).

Methodology

Twelve key industry participants, including QCB representatives, cybersecurity specialists, local bankers, a mobile banking platform provider, and an academic, discussed the multidimensional security and privacy issues in mobile banking, focusing on their extensive understanding and immersion in the field. Interviews analyzed current security protocols, regulatory frameworks, user behavior, cyber threats, and future trends, lasting five to six minutes on in-person and scheduled video conferencing platforms.

Table I Source Author

Participant	Role	Affiliation
P1	Representative	IT Company
P2	Cybersecurity Specialist	IT Company
P3	Cybersecurity Specialist	IT Company
P4	Banker	Local Bank
P5	Banker	Local Bank
P6	Representative	University
P7	Academic	University
P8	Legal Expert	University
P9	Consumer Rights Advocate	Consumer Protection Organization
P10	Data Privacy Specialist	Local Bank
P11	Mobile Banking User	Local Bank

The study on mobile banking security and privacy in Qatar includes different stakeholders, including industry experts, local banks, academic and research institutions, and consumer advocates. The data is gathered from various perspectives, including industry experts, local banks, academic and research institutions, and consumer rights advocates. The study provides a comprehensive analysis of the challenges and recommendations related to mobile banking security and privacy in Qatar, ensuring a balanced and comprehensive understanding of the industry's viewpoints however the data is sourced directly from the author.

Thematic Analysis

In accordance with the guiding principles from Braun and Clarke (2006) paradigm for thematic analysis, the interviews data was reviewed with the objective of systematically uncovering and elaborating the patterns and themes (Braun et al., 2022). To begin with, we got an impression of the context and content of the interviews within the process of their textual transcription and the first screening of the materials. In the next step, we arranged the data that is most important to our research questions in relation to their salient characteristics and created the initial codes. These codes were then categorised in terms of possible themes, the essence of the finding and patterns witnessed in the studies.

Key themes in mobile banking security, including regulatory issues, technological risks, vulnerabilities, user awareness, and future trends. It highlights the need for stronger systems and measures, the insecurity of current technologies, and the importance of user behavior and education in reducing security threats. It also discusses current and future challenges in security and privacy. Thematic analysis of mobile banking themes reflects data and provides a broad perspective on security and privacy challenges. It helps identify critical areas for future enhancement and participants' experiences.

Regulatory Frameworks for Mobile Banking Security and Privacy in Qatar

"Qatar has implemented several regulatory frameworks including the Qatar Central Bank Law and the QCB regulations on electronic payment services, which align closely with international standards such as GDPR and ISO/IEC 27001. Our aim is to ensure a robust regulatory environment that safeguards user data and promotes secure banking transactions."

Current developments in Qatar include establishment of regulatory frameworks such as the Qatar Central Bank Law and on electronic payment services regulations. These frameworks are similar to the international standards like GDPR of the EU and ISO/IEC 27001 for the Information Security. The aim of these provisions is to establish a reliable and secure regulatory structure that safeguards the privacy of users and ensures safer banking in Qatar. Qatar aspires to achieve its goal of maintaining a strong and resilient financial sector in a way that is consistent with global standards while ensuring adequate consumer and commercial protection within its borders.

"Qatar has a strong regulatory framework guided by the QCB and the National Cyber Security Agency, which is on par with international standards like GDPR and PCI DSS. These regulations are designed to ensure data protection and secure transaction processes."

Qatar has established the National Cyber Security Agency (NCA), and the Qatar Central Bank (QCB) has implemented a regulatory framework within the Qatar financial and digital sectors. These regulations can be easily related to some of the significant international standards like GDPR (general data protection regulation) of the European Union and PCI DSS (payment card industry data security standard). The effect of this stringent regulatory framework is to create more guarantees on personal information protection and safe commerce operations. Qatar also follows international standards in its endeavor to increase the trust in its financial system and protect consumers' information and secure digital banking and payment services from digital payment providers and non-bank financial service providers. This regulatory approach helps Qatar to present itself as a leader in cyber security and data privacy in the given region.

"Qatar's regulatory frameworks, driven by the QCB and complemented by national cybersecurity strategies, align with international standards such as GDPR and ISO/IEC 27001. These frameworks are designed to ensure robust security and privacy for mobile banking users."

Qatar has created regulatory policies for its financial and digital sectors that are underpinned by the Qatar Central Bank (QCB) and to some degree by national cybersecurity strategies. These regulations are similar to some of the global concerns for instance the EU's General Data Protection Regulation and the ISO/IEC 27001 Information Security. This approach's objective is to guarantee that appropriate security and privacy mechanisms are in place for Qatar consumers who use mobile banking and other digital financial services. With Qatar's adherence to global standards and guidelines, the country seeks to establish the confidence of its citizens in its financial systems, promote the protection of customer information, and facilitate safe and secure digital payments. Such a regulatory environment places the country at the top among its regional peers in terms of cybersecurity and data protection.

Prevalent Cybersecurity Threats in Mobile Banking in Qatar

"Prevalent threats include phishing, malware, and sophisticated social engineering attacks. Current protocols like multi-factor authentication and real-time monitoring are quite effective, but there's a continuous need for updates and improvements to stay ahead of these evolving threats."

According to the participant there are number of prevalent cybersecurity threats that come into form for Qatar's financial and digital services and some of the lucrative and prominent threats include the phishing, malware, and the sophisticated social engineering which are combined. In an effort to combat these dangers, the country has employed security measures such as MFA and RTD protocols. However, these current measures are quite effective to date; there is a constant need to update and keep improving the security frameworks to outcompete the continuing advancement in the threat landscape. Cybersecurity threats are evolving all the time and hackers always come up with new techniques to breach and steal information, so Qatar must remain proactive in developing new measures to safeguard users' bank data and transactions. Managing risk in this marketplace is best accomplished when the firms and institutions in the sector remain flexible and constantly able to innovate.

"Malware, and social engineering attacks. While current security protocols like encryption and authentication measures are effective to a certain extent, there's a continuous need for advancements and proactive measures to combat evolving threats."

There are several ongoing cybersecurity threats in the financial sector in Qatar including malware and social engineering attack. Another problem is the security threats posed by the country that has employed encryption and authentication to address these issues. Indeed, these current measures have to some extent been helpful, but there is still a need for intensified improvements and greater efforts towards preemptive and preventive approach to counter the continually changing threat environment. Malicious groups continue to upgrade their skills and move forward with evolving technologies, making Qatar to keep improving cybersecurity means. Qatar needs to be open towards such risks and threats and be ready to adopt a more agile and adaptive mindset to maintain the highest standards of protection for both the financial ecosystem and its customer base.

Balancing Security Measures and User Experience in Mobile Banking Applications

"Balancing security and user experience is a significant challenge. While robust security measures are essential, they must not hinder the user experience. Implementing seamless security features like biometric authentication and intelligent user behavior analytics can help maintain this balance."

Qatar's financial sector faces a balance between security and usability. To achieve this, the country has integrated advanced security tools like biometric authentication and user behavior analytics. These solutions ensure high security while maintaining customer comfort in digital banking and payment services, protecting the country's financial system.

"Striking this balance is essential. We focus on integrating security measures that operate seamlessly in the background, such as biometric authentication and AI-based anomaly detection, to ensure the user experience remains smooth and intuitive."

The fulfillment of this balance between safety and convenience is one of the biggest issues the financial sector of Qatar is currently facing. To tackle this, the development is placing more emphasis on security solutions that are built in and work in the background to ensure minimum or no interruption from the user. This involves applying biometric verification and uses AI to recognise risks for user identification and monitoring activities. With a mandate to put in place an advanced security without undermining customer experience, Qatar has embraced disclosure as a strategy in the provision of robust security for the large number of customers using digital banking and payment services. This way of striking a balance means that Qatar sees to it that the financial ecosystem is protected without necessarily eroding the comfort factor that users enjoy.

"Balancing security and user experience is crucial. We aim to implement strong security measures like biometric authentication and seamless encryption without complicating the user interface. Continuous user feedback helps us to refine this balance."

Balancing security with expediency is an ideal for Qatar's financial services sector. The main objective is to maintain high security standards based on biometrics and encryption so as not complicate or obstruct the simplicity of the interface. Through the process, Qatar can understand what customers like or dislike about their security policies and what can be done to empower policies to improve customer experience rather that to the contrary. This even balance is a particularly helpful approach in the case of Qatar as it helps to maintain a high level of security for the financial environment, while at the same time ensuring that digital banking remains uncluttered and easy to use for the end user. In order to develop confidence and demand towards Qatar's financial services, attaining this balance is paramount.

Technological Innovations for Enhancing Security and Privacy in Mobile Banking Platforms

"We're implementing AI-driven fraud detection, block chain for secure transactions, and advanced encryption techniques. Challenges include ensuring compatibility with existing systems, managing costs, and training staff and customers on new technologies.″

Qatar is embracing AI to fight financial crimes, using the block chain to secure transactions, and cryptographic protocols to protect customers' accounts. Nevertheless some of these challenges are compatibility, costs, and training for employees and customers. It is possible to state that user-centric is a good approach to implementing e-government websites.

"Technological innovations such as AI-driven threat detection, block chain for secure transactions, and advanced encryption techniques are being adopted. Deployment challenges include integration with legacy systems, user adoption, and ensuring compliance with regulatory requirements."

Qatar is adopting disruptive technologies such as AI-based real-time threat detection, block chain for secure transactions, and sophisticated encryption that can improve the security of its financial system. However, some of the challenges present include; adoption of these technologies, posing a challenge when integrating them with current applications and even in handling the regulatory aspect.

Critical Vulnerabilities in Mobile Banking Systems

″Critical vulnerabilities include outdated software, inadequate encryption, and insufficient user authentication mechanisms. Addressing these involves regular updates, adopting advanced encryption standards, and enhancing authentication protocols."

The banking and finance sector of Qatar is at risk of threats such as the use of old software or insufficient encryption, and the use of insufficient or no authentication on the user. In addition, these challenges can be overcome by release of general software upgrades, strong encryption techniques, and new security validation procedures. This approach would allow Qatar to better address potential intrusions before they could happen, thus strengthening its cybersecurity defenses.

"Critical vulnerabilities include outdated software, weak encryption methods, and lack of user awareness. Addressing these requires coordinated efforts between regulatory bodies, financial institutions, and technology providers."

Qatar's financial sector faces vulnerabilities like outdated software, weak encryption, and user insufficient cybersecurity awareness. A coordinated, multi-stakeholder approach is needed, including regulatory bodies, financial institutions, technology providers, and regulatory bodies to strengthen the financial ecosystem and protect customer and investor trust.

“As much as it is possible to embrace the flexibility that is offered by mobile banking security concerns prevent me from fully embracing it. Though I attempt to follow good measures such as using secure passwords and regularly updating my phone’s software, I am aware this is just a drop in the bucket. Information security is crucial in today's digital age, with vulnerabilities like insecure Wi-Fi connections, phishing scams, and hacking posing significant threats to personal and financial institutions".

The benefits of mobile banking, such as flexibility and accessibility, but is hesitant due to security concerns. They acknowledge the importance of strong passwords and software updates, but acknowledge the risks of unprotected terminals, online frauds, and break-ins. Despite these precautions, they are not fully utilizing the benefits of mobile banking.

"The risks associated with mobile banking, including malware, unsecured connections, and data leakage. They acknowledge the need for education in computer security and more comprehensive security measures for their mobile banking".

The risks of mobile banking, such as malware and unsecured connections, and emphasizes the need for education on computer security best practices. They acknowledge the need for a comprehensive approach to protect sensitive financial information.

Impact of User Behaviors and Awareness on Mobile Banking Security and Privacy

"Key vulnerabilities include outdated software, weak user authentication, and susceptibility to social engineering attacks. Addressing these requires regular system updates, stronger authentication methods, and comprehensive user training programs."

Qatar financial institutions' vulnerabilities included past and present software issues, user authentication deficiencies, and social engineering threats. Although these institutions ought to better their software support, use strong authentication modes and provide extensive training to the users. This will increase security for Qatari financial system.

"Critical vulnerabilities include weak user authentication, outdated software, and vulnerability to social engineering attacks. Addressing these involves regular updates, implementing stronger authentication methods, and continuous user education on recognising and avoiding cyber threats."

Participant has declared that the financial sector in Qatar has its own risks such as poor user authentication and account verification, legacy systems and applications as well as social engineering tactics. To deal with these, there should be regular software releases, as well as better password requirements and more general awareness campaigns for users of any new service. This approach will also enhance the security of the Qatari financial ecosystem.

Insights on Recent Cyber Incidents in Mobile Banking in Qatar

"User behavior significantly impacts security. Common issues include weak passwords and susceptibility to phishing scams. We regularly conduct awareness campaigns and provide educational resources to help users understand and implement best security practices."

User behaviour characteristics have an impact on the security of Qatar's financial Ecosystem with common vulnerabilities such as weak passwords and phishing attacks. To deal with these, the country implements awareness of and provides information as well as rights that enable customers and employees to protect their digital identity.

"Recent cyber incidents have underscored the importance of real-time monitoring and rapid response capabilities. Lessons learned include the need for robust incident response plans, regular security audits, and continuous user education to help users recognise and avoid potential threats."

There has been an increasing number of cybercrimes within Qatar's financial sector, which has also demonstrated the need for real-time cyber monitoring and quick response functions. Among others, several conclusions can be derived from the incident response plan; security audits should be implemented; and security awareness training is a must. An effective IR process can help FI entities rapidly identify software attacks and limit the damage. In addition, continuous security audits ensure the discovery and elimination of possible threats and weaknesses long before they can be turned into security attacks by a malicious intruder. Qatar's financial ecosystem must be resilient against cyber threats like phishing and social engineering. A multi-disciplinary approach is the most suitable strategy for development and management, ensuring awareness and prevention of these risks.

"Common mobile banking security threats like phishing and malware, employs advanced multi-factor authentication, updates banking apps, avoids public Wi-Fi, and focuses on data breaches from banks, staying updated through notifications, cyber news, and trainings".

Mobile banking has become influential in today's society, and there is a need to have strong security. A few suggestions for tackling these risks include practicing multi-factor authentication, ensuring that your banks applications are updated frequently, and not connecting banking apps to public Wi-Fi. Finally, one must always monitor data breaches involving financial institutions as one receives a notification or read it in the news, or even after taking cyber-security courses. Mobile banking systems must continuously monitor new risks and incorporate proper security measures to ensure the safety and soundness of transactions, utilizing biometric identification and cautious device use.

"My knowledge in the security of mobile banking is fairly average – having a strong password and utilizing a password manager. They express a liking for computer transactions, and generally shun large transactions. They are concerned with computer virus and take care of the software of their phone". In terms of security, the knowledge of mobile banking is rather elementary, and it is protected only by a password, and an application to manage it. They fall under the category of those who are more comfortable entering into transactions using the computer rather than using a mobile phone and rarely engage in large financial transactions on the mobile phone. A person fears viruses and upgrades their phone's software to combat malware. They should learn about security options like two-factor identification and mobile banking security, which can help establish security in their country.

Discussion

The study highlights the broad concern of security and privacy in mobile banking in Qatar, addressing regulatory issues, technology risks, user awareness, training, and future developments (Abu-Taieh et al., 2022). It is critical to have a sound law to react to cyber threats, Respondents pointed out that although Qatar mat laws that are equivalent to global laws like GDPR and standard ISMS ISO/IEC 27001 constantly we need to upgrade these laws since the number of threats is increasing (Diamantopoulou et al., 2020). Mobile commerce is transforming the global marketplace, but trust in online shopping remains low in Qatar. This study explores factors promoting consumer trust in mobile commerce. Results show perceived security is the most significant positive relationship with trust formation, followed by social media influencers, localisation, luxury brands, perceived usability, and privacy (Al-Khalaf & Choe, 2020). The Qatari banking industry is utilising AI to improve cybersecurity, but faces challenges such as potential destructiveness, vulnerabilities, and potential regulatory changes and the rise of AI-powered malware (AL-Dosari et al., 2024). Technological threats include outdated software, weak encryption methods, and user behavior in mobile banking. Frequent system upgrades, stronger encryption, and improved user identification are needed to combat cybercriminals and protect users (Yeng et al., 2022). Participants emphasised the importance of balancing security measures with user experience, advocating for integrated features like biometric ID and AI for anomaly detection (Olabanji et al., 2024). Future advancements in mobile banking could include AI threat detection and block chain for secure transactions. The need for continuous comprehensive attack on mobile banking security in Qatar, addressing issues like integration with existing systems, cost, and user training, while ensuring the application's convenience for users (Khan et al., 2023). Service quality, perceived usefulness, and ease of use significantly influence mobile banking intention in Qatar, while trust, system quality, and information quality are insignificant (AL-NAIMI, 2022). The study has shown that the mobile self-reliance, and social domination are key factors influencing mobile banking adoption in Delhi-NCR, with customer support mediating this trend (Asif et al., 2023). The impact of value, risk, image, cost, and usage barriers on mobile banking adoption in millennial customers. Risk barriers, perceived cost barriers, barriers to use, and value barriers significantly influenced adoption intentions (Rombe et al., 2021).

Implications

The study also calls for increased commitment in the development of laws, policies, and strategies that would improve Qatar's defense against cyber threats based on international benchmarks while at the same time considering key issues unique to the country. Banks need to incorporate complex technologies such as encryption, Artificial Intelligence and Block chain in their operations as they help in discrediting risks, and reinforcing security against cybercrimes. It is highly recommended that financial institutions invest in user education programs to ensure that their mobile banking systems are secure since all it takes is for one person to fall for a scam for the system to be compromised. Biometric identification and AI-based anomaly identifiers are application security elements that should be incorporated into financial services with the ability to give a smooth experience to its users while keeping security details watertight by conducting security improvements recurrently from user feedback.

Conclusion

The study discusses the significance of the development of the multi-faceted approach in relation to security and privacy in the context of mobile banking in Qatar. It points towards such goals as constant updates, incorporation of additional layers of protection, and user awareness as the critical factors for maintaining security while still being consumer-friendly. The consumer protection effectively proposes cooperation with regulators and the banking industry as well as IT suppliers. The upcoming years, the representatives of the Qatar state should enhance cyber defense mechanisms with the help of leading technologies such as encryption, AI, and block chain, initiate user education programs, and adopt biometric identification in finance, as well as AI-based anomaly detection. Such a user- friendly business approach will ensure the safety of customers' assets and their information, creating a secure financial industry. Qatar will need to strengthen its cybersecurity by reconsideration of the existing frameworks and the application of the proper measures. To reduce the chances of risk and ensure that the bank or finical institute's information is not easily accessed by the wrong people, new technologies like encryption, Artificial intelligence and block chain should be adopted. To some extent, the practice of social engineering could be mitigated through user education programs that can address the risk of attacks that may be in direct-mail format. Combining the biometric identification method with the breakdown of AI-based anomalous behaviour can further improve the approach and strengthen its security points without compromising the ease of use.

Reference

1. Abdul-Wahab, A.-H., & Haron, R. (2017). Efficiency of Qatari banking industry: an empirical investigation. *International Journal of Bank Marketing*, *35*(2), 298-318.
2. Abu-Taieh, E. M., AlHadid, I., Abu-Tayeh, S., Masa'deh, R. e., Alkhawaldeh, R. S., Khwaldeh, S., & Alrowwad, A. a. (2022). Continued intention to use of M-Banking in Jordan by integrating UTAUT, TPB, TAM and service quality with ML. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(3), 120.
3. Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A survey on 5G networks for the Internet of Things: Communication technologies and challenges. *Ieee Access*, *6*, 3619-3647.

4. Al-Delayel, S. A. (2022). Security Analysis of Mobile Banking Application in Qatar. *arXiv preprint arXiv:2202.00582*.
5. AL-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and systems*, *55*(2), 302-330.
6. Al-Hababi, A., & Tokgoz, S. C. (2020). Man-in-the-middle attacks to detect and identify services in encrypted network flows using machine learning. 2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet),
7. Al-Khalaf, E., & Choe, P. (2020). Increasing customer trust towards mobile commerce in a multicultural society: A case of Qatar. *Journal of Internet Commerce*, *19*(1), 32-61.
8. Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2018). Cyber-security incidents: a review cases in cyber-physical systems. *International Journal of Advanced Computer Science and Applications*, *9*(1).
9. Al-Naimi, L., & Abu-Shanab, E. A. (2024). Factors influencing the intention to use mobile banking. *International Journal of Electronic Banking*, *4*(2), 120-137.
10. AL-NAIMI, L. N. N. (2022). *FACTORS INFLUENCING THE INTENTION TO USE MOBILE BANKING IN QATAR*
11. Albinali, A. A. (2023). *Three Essays on Banking in Qatar* Hamad Bin Khalifa University (Qatar)].
12. Alnoaimi, S. (2016). DETERMINANTS OF SUCCESS USAGE OF INFORMATION SYSTEMS IN PUBLIC SECTOR IN THE STATE OF QATAR.
13. Alsalem, A., & Abu-Shanab, E. A. (2022). Challenges and Factors Influencing the Adoption of Internet Banking in Qatar. *International Journal of Web Portals (IJWP)*, *14*(1), 1-20.
14. Alsayed, A., & Bilgrami, A. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and advanced engineering*, *7*(1), 109-115.
15. Apaua, R., & Lallie, H. S. (2022). Measuring user perceived security of mobile banking applications. *arXiv preprint arXiv:2201.03052*.
16. Asif, M., Khan, M. A., Alhumoudi, H., & Wasiq, M. (2023). Examining the Role of Self-Reliance, Social Domination, Perceived Surveillance, and Customer Support with Respect to the Adoption of Mobile Banking. *International journal of environmental research and public health*, *20*(5), 3854.
17. Au, Y. A., & Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications*, *7*(2), 141-164.
18. Badran, A. (2023). Developing smart cities: Regulatory and policy implications for the State of Qatar. *International Journal of Public Administration*, *46*(7), 519-532.
19. Bassolé, D., Koala, G., Traoré, Y., & Sié, O. (2020). Vulnerability analysis in mobile banking and payment applications on android in African Countries. Innovations and Interdisciplinary Solutions for Underserved Areas: 4th EAI International Conference, InterSol 2020, Nairobi, Kenya, March 8-9, 2020, Proceedings 4,
20. Braun, V., Clarke, V., & Hayfield, N. (2022). 'A starting point for your journey, not a map': Nikki Hayfield in conversation with Virginia Braun and Victoria Clarke about thematic analysis. *Qualitative research in psychology*, *19*(2), 424-445.
21. Council, F. F. I. E. (2005). Authentication in an internet banking environment. *Retrieved June*, *28*, 2006.
22. Das, S., & Ganguly, D. (2024). Protecting Your Assets: Effective Use of Cybersecurity Measures in Banking Industries. In *Next-Generation Cybersecurity: AI, ML, and Blockchain* (pp. 265-286). Springer.
23. Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls. *Information & Computer Security*, *28*(4), 645-662.
24. Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. Proceedings of the second symposium on Usable privacy and security,
25. Javed, Y., Al Qahtani, E., & Shehab, M. (2021). Privacy policy analysis of banks and mobile money services in the middle east. *Future Internet*, *13*(1), 10.
26. Khan, H., Talib, F., & Faisal, M. N. (2015). An analysis of the barriers to the proliferation of M-Commerce in Qatar: A relationship modeling approach. *Journal of Systems and Information Technology*, *17*(1), 54-81.
27. Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilising bio metric system for enhancing cyber security in banking sector: a systematic analysis. *Ieee Access*.
28. Kruse, L., Wunderlich, N., & Beck, R. (2019). Artificial intelligence for the financial services industry: What challenges organisations to succeed.
29. Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multidimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision support systems*, *49*(2), 222-234.
30. Merhi, M., Hone, K., Tarhini, A., & Ameen, N. (2021). An empirical examination of the moderating role of age and gender in consumer mobile banking use: a cross-national, quantitative study. *Journal of Enterprise Information Management*, *34*(4), 1144-1168.
31. Millett, L. I., & Pato, J. N. (2010). Biometric recognition: Challenges and opportunities.
32. Musa, A., Khan, H. U., & AlShare, K. A. (2015). Factors influence consumers' adoption of mobile payment devices in Qatar. *International journal of mobile communications*, *13*(6), 670-689.

33. Najafi, B., Amra, M., & Najafi, A. (2024). Exploring Global Fintech Advancement and Application: Case of Saudi Arabia, Turkey, and Qatar. In *Exploring Global FinTech Advancement and Applications* (pp. 158-211). IGI Global.
34. Nasser, A. (2020). Cybercrime: theoretical determinants, criminal policies, prevention & control mechanisms. *International Journal of Technology and Systems*, *5*(1), 34-63.
35. Olabanji, S. O., Olaniyi, O. O., Adigwe, C. S., Okunleye, O. J., & Oladoyinbo, T. O. (2024). AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorisation, and access control within cloud-based systems. *Authorisation, and Access Control within Cloud-Based Systems (January 25, 2024)*.
36. Omeleze, S., & Venter, H. S. (2013). Testing the harmonised digital forensic investigation process model-using an Android mobile phone. 2013 Information Security for South Africa,
37. Pearce, M., Zeadally, S., & Hunt, R. (2013). Virtualisation: Issues, security threats, and solutions. *ACM computing surveys (CSUR)*, *45*(2), 1-39.
38. Rojas, J. (2021). *Inconsistencies in Data Privacy Regulation: Financial Institution and Individual Customer Risks* Utica College].
39. Rombe, E., Zahara, Z., Santi, I., & Rahadhini, M. (2021). Exploring e-mobile banking implementation barriers on Indonesian millennial generation consumers. *International Journal of Data and Network Science*, *5*(4), 579-586.
40. Sangwan, Y. S., Lal, S., Bhambri, P., Kumar, A., & Dhanoa, I. S. (2021). Advancements in social data security and encryption: A review. *NVEO-Natural Volatiles & Essential Oils Journal| NVEO*, 15353-15362.
41. Sharma, A., Singh, S. K., Kumar, S., Chhabra, A., & Gupta, S. (2021). Security of android banking mobile apps: Challenges and opportunities. International Conference on Cyber Security, Privacy and Networking,
42. Sharma, M., Banerjee, S., & Paul, J. (2022). Role of social media on mobile banking adoption among consumers. *Technological Forecasting and Social Change*, *180*, 121720.
43. Sun, G. (2020). Banking institutions and banking regulations. *The handbook of China's financial system*, 9-37.
44. Team, C. (2014). Unintentional insider threats: A review of phishing and malware incidents by economic sector.
45. Tsobdjou, L. D., Pierre, S., & Quintero, A. (2024). A Framework for Security Assessment of Android Mobile Banking Applications. *Computer Networks and Communications*, 49–61-49–61.
46. Weichbroth, P., & Łysik, Ł. (2020). Mobile security: Threats and best practices. *Mobile Information Systems*, *2020*, 1-15.
47. Wheeb, H. F. (2023). THE LEGAL SYSTEM OF BANKING INSPECTION LEGAL STUDY. *Russian Law Journal*, *11*(11S), 368-380.
48. Yeng, P. K., Fauzi, M. A., Yang, B., & Nimbe, P. (2022). Investigation into phishing risk behaviour among healthcare staff. *Information*, *13*(8), 392.