International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Review Article)

Human factors in cybersecurity: Navigating the fintech landscape

James Olakunle Oladipo [1], Chinwe Chinazo Okoye [2], Oluwafumi Adijat Elufioye [3], Titiola Falaiye [3] and Ekene Ezinwa Nwankwo [4, *]

[1] *Independent Researcher, Lagos, Nigeria.*
[2] *Access Bank Plc, Awka, Nigeria.*
[3] *Independent Researcher Lagos, Nigeria.*
[4] *Department of Business Administration and Management, Anambra State polytechnic, Mgbakwu, Nigeria.*

International Journal of Science and Research Archive, 2024, 11(01), 1959–1967

Publication history: Received on 30 December 2023; revised on 09 February 2024; accepted on 11 February 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.11.1.0258

Abstract

The dynamic landscape of financial technology (Fintech) introduces a myriad of challenges and opportunities, with human factors playing a pivotal role in shaping the cybersecurity ecosystem within this domain. This review explores the intricate relationship between human factors and cybersecurity in the context of Fintech, aiming to navigate the evolving landscape. In the realm of Fintech, where the fusion of finance and technology is reshaping traditional banking and investment practices, understanding human behavior becomes paramount. Human factors encompass a spectrum of elements, including cognitive abilities, decision-making processes, and user behaviors, all of which significantly impact the effectiveness of cybersecurity measures. This paper delves into the nuances of these factors and their implications for securing financial transactions and sensitive data in Fintech platforms. One key aspect of human factors in Fintech cybersecurity is the user interface design. Intuitive and user-friendly interfaces enhance security by minimizing human errors and fostering a secure user experience. Conversely, poorly designed interfaces can inadvertently contribute to vulnerabilities. This paper explores the intersection of user experience design and cybersecurity protocols, aiming to strike a balance that promotes both usability and security. Moreover, the study investigates the psychological aspects of cybersecurity awareness and education in the Fintech sector. As financial transactions increasingly migrate to digital platforms, users' awareness of potential cyber threats becomes a critical line of defense. Analyzing the effectiveness of training programs and awareness campaigns, the paper explores strategies to enhance cybersecurity consciousness among Fintech users. The research illuminates the symbiotic relationship between human factors and cybersecurity within the dynamic Fintech landscape. By comprehensively understanding and addressing human elements in interface design, user awareness, and decision-making processes, the paper aims to provide insights that contribute to the development of robust cybersecurity frameworks tailored to the evolving needs of Fintech platforms.

Keywords: Cybersecurity; FinTech; Technology; Finance; Human Factor; Review

1. Introduction

The financial technology (Fintech) industry has rapidly evolved, revolutionizing the way financial services are delivered and accessed. Fintech encompasses a wide range of technological innovations, including digital currencies, cryptofinance, and AI utilization by financial institutions (Lu et al., 2020). As Fintech continues to grow, the importance of cybersecurity within this sector has become increasingly critical. The integration of technology in financial services has introduced new vulnerabilities, making the industry a prime target for cyber threats. Consequently, the significance of human factors in Fintech cybersecurity has garnered attention due to its potential to influence employees' cybersecurity behaviors and attitudes (Hadlington, 2017). This introduction will provide a background of Fintech,

[*] Corresponding author: Ekene. Ezinwa Nwankwo

discuss the increasing importance of cybersecurity in Fintech, and highlight the significance of human factors in Fintech cybersecurity.

The Fintech industry has experienced significant growth, with digital transformation and technological advancements driving its evolution. The industry encompasses a broad spectrum of financial services, including digital banking, mobile payments, and investment management, all of which are underpinned by technological innovations (Lu et al., 2020). The rapid adoption of Fintech solutions has reshaped traditional financial services, offering greater accessibility and efficiency to consumers. However, this digital transformation has also exposed the industry to cybersecurity risks, necessitating robust security measures to safeguard sensitive financial data and transactions.

The increasing importance of cybersecurity in Fintech is underscored by the industry's susceptibility to cyber threats. Fintech companies are attractive targets for cybercriminals due to the vast amounts of financial data they handle. Cybersecurity risks in Fintech encompass data breaches, identity theft, and financial fraud, posing significant challenges to the integrity and trustworthiness of the industry (Ng & Kwok, 2017). As a result, there is a growing recognition of the need for comprehensive cybersecurity strategies to mitigate these risks and ensure the resilience of Fintech operations. Human factors play a crucial role in shaping cybersecurity practices within Fintech organizations. Employees' cybersecurity behaviors and attitudes are influenced by various human factors, including gender differences, impulsivity, and media multitasking (Hadlington, 2017; , Hadlington & Murphy, 2018). Understanding these human factors is essential for developing effective cybersecurity training programs and policies tailored to the specific needs and behaviors of Fintech employees. Moreover, the human-centered approach to cybersecurity design and decision-making is increasingly recognized as a key factor in enhancing the overall security posture of Fintech organizations (Baumer, 2017). By integrating human factors considerations into cybersecurity practices, Fintech companies can better address the behavioral and cognitive aspects of security, ultimately strengthening their resilience against cyber threats.

In conclusion, the rapid growth of the Fintech industry has brought about a paradigm shift in financial services, driven by technological innovations. However, this digital transformation has also heightened the industry's exposure to cybersecurity risks, necessitating a heightened focus on cybersecurity measures. The significance of human factors in shaping cybersecurity behaviors and attitudes within Fintech organizations underscores the need for a human-centered approach to cybersecurity. By integrating human factors considerations into cybersecurity strategies, Fintech companies can enhance their security posture and effectively navigate the evolving landscape of Fintech cybersecurity.

2. Human Factors in User Interface Design

Human Factors in User Interface Design plays a crucial role in various domains, including cybersecurity, fintech, and overall system usability. User-friendly interfaces are essential in cybersecurity as they enhance user experience, making it easier for users to understand security warnings, leading to better decision-making and reduced security breaches (Connolly & Phillips, 2002). Conversely, poorly designed interfaces can have a detrimental impact on security, as they may lead to user errors, misunderstanding of security alerts, and ultimately compromise system security (Grahn & Kujala, 2020). Therefore, balancing usability and security in Fintech UI design is critical. It involves integrating human factors principles to ensure that the interface is intuitive and easy to use while maintaining robust security features (Fabian et al., 2023; Li, 2002).

Human Factors in User Interface Design is a critical aspect of creating effective and efficient human-computer interaction systems. Human factors considerations play a significant role in shaping the design principles related to the interface between computer-based systems and their human users (Connolly & Phillips, 2002). These considerations are essential for ensuring that the user interface strategies are effective and align with the principles of human-computer interaction (Uchechukwu et al., 2023; Shneiderman, 1987). Furthermore, the development of new user interfaces often involves the application of Universal Design principles, which aim to create interfaces that are accessible and usable by a wide range of individuals (Chaudhary & Murano, 2021).

In the context of user interface design, it is crucial to consider the impact of human factors such as cognitive psychology and user requirements. Norman (1988) emphasized the importance of orienting the design of user interfaces towards user requirements and conducting physical operational tests to reduce negligence in interface design (Adeleke et al., 2019; Chao et al., 2016). Additionally, the acceptance of user interfaces by end-users is a critical aspect that is influenced by both technical problems and human factors (Akiki et al., 2014).

The design of user interfaces for emerging technologies such as smartwatches also requires a deep understanding of human factors and usability. Designers have explored various form factors and input methods to enhance usability, such as using finger-mounted styluses and capturing finger gestures as input using mobile phone cameras (Ilugbusi et al., 2020; Chun et al., 2018). Moreover, the usability of software systems is ultimately determined by the users, and therefore, usability metrics and evaluation techniques are essential for assessing the effectiveness of user interfaces (Holcomb & Tharp, 1991; Ji et al., 2006; Vincent et al., 2021).

As technology continues to advance, the design of user interfaces for artificial intelligence systems and Internet of Things (IoT) applications presents new challenges. These challenges include the need to lower the complexity of user interfaces by leveraging familiar metaphors and addressing the difficulties associated with the development of adaptive distributed hybrid user interfaces (Zhao, 2022; Sanctorum et al., 2020; Sanctorum & Signer, 2019). Furthermore, the design of user interfaces for mobile devices and multiuser interfaces requires considerations of cognitive models, patterns of interaction among users, and even the evaluation of user experience through brain activity (Rao et al., 2005; Aggarwal et al., 2014; Meskens et al., 2009).

In summary, human factors play a crucial role in user interface design, influencing the principles, strategies, and evaluation methods employed in creating effective and user-friendly interfaces. Understanding human cognition, user requirements, and the impact of emerging technologies is essential for designing interfaces that meet the needs of diverse users and provide optimal usability and user experience.

3. Cognitive Factors in Fintech Cybersecurity

Understanding Cognitive Abilities in the Context of Cybersecurity is crucial for ensuring the security of Fintech systems. Research has shown that cognitive abilities, such as executive function and decision-making processes, play a significant role in cybersecurity (Alvarez & Emory, 2006; Salthouse, 2012; Alvarez & Emory, 2006) emphasize the importance of understanding cognitive abilities in the context of cybersecurity, particularly the implications of neuropsychological tests in anatomical, cognitive, and behavioral terms (Alvarez & Emory, 2006; Salthouse, 2012; Abrahams et al., 2023) further supports this by highlighting the consequences of age-related cognitive declines and their impact on activities of daily living and cognition disorders, which are essential considerations in the design of cybersecurity systems (Salthouse, 2012).

Decision-making processes significantly influence security in Fintech. Studies have shown that decision-making biases can affect cybersecurity. Gutzwiller et al. (2019) revealed evidence of decision-making biases in red teamers, indicating the importance of understanding and mitigating these biases for effective cybersecurity (Gutzwiller et al., 2019). Additionally, Hu et al. (2012) emphasized the critical role of top management and organizational culture in managing employee compliance with information security policies, highlighting the influence of decision-making processes at the organizational level on cybersecurity (Hu et al., 2012).

Mitigating cognitive biases is essential for enhanced Fintech cybersecurity. Dawson & Thomson (2018) highlighted the challenge of the paucity of quantitative assessment regarding the cognitive aptitudes required by cybersecurity professionals to be successful, indicating the need to address and mitigate cognitive biases for improved cybersecurity performance (Dawson & Thomson, 2018). Furthermore, Hadlington & Murphy (2018) expanded the understanding of the relationship between human factors and cybersecurity behaviors, providing insights that are useful for informing the design of training and intervention packages to mitigate risky cybersecurity behaviors (Hadlington & Murphy, 2018).

In conclusion, understanding cognitive abilities, decision-making processes, and mitigating cognitive biases are crucial for enhancing Fintech cybersecurity. By considering these cognitive factors, Fintech organizations can develop more robust cybersecurity measures to protect against cyber threats and ensure the integrity and security of financial technology systems.

4. Psychological Aspects of Cybersecurity Awareness

Cybersecurity awareness is crucial in fintech due to the increasing adoption of fintech services. Training programs and awareness campaigns play a significant role in enhancing cybersecurity consciousness among fintech users. These programs are effective in shaping user behavioral intention toward protective information technologies. Additionally, they are essential in motivating users to adopt cybersecurity practices. However, the fintech mobile app ecosystem faces cybersecurity challenges, and solutions such as advanced encryption and AI-driven anomaly detection are being explored to address these threats (Mustapha, 2023; Adaga et al., 2024).

Cybersecurity awareness is vital in fintech, and training programs and awareness campaigns are effective in enhancing user consciousness and behavioral intention toward protective technologies. The challenges in the fintech mobile app ecosystem necessitate the exploration of advanced cybersecurity solutions to ensure the security of fintech services.

Cybersecurity awareness is crucial in the fintech industry due to the increasing vulnerability to cybercrime (Monteith et al., 2021). User awareness plays a central role in shaping behavioral intentions towards protective technologies (Dinev & Hu, 2007). Training programs and awareness campaigns have been found effective in enhancing the security awareness level of smartphone users (Koyuncu & Pusatli, 2019). Additionally, cybersecurity awareness training has been shown to be effective against phishing attacks, a prevalent threat in the fintech sector (Back & Guerette, 2021). As the fintech industry faces cybersecurity challenges, including those related to mobile app ecosystems, strategies such as advanced encryption, biometric authentication, and AI-driven anomaly detection are being explored to address these threats (Mustapha, 2023).

5. Behavioral Analysis in Fintech Cybersecurity

Behavioral analysis in Fintech cybersecurity plays a crucial role in understanding user behavior and its implications for security, analyzing patterns of behavior in Fintech transactions, and implementing adaptive security measures based on behavioral analysis. The adoption of Fintech services is influenced by the user's trust in the service provider, which in turn affects their willingness to use the service (Zhong-qing et al., 2019). Additionally, factors such as perceived ease of use, usefulness, credibility, and social influence significantly impact user acceptance and behavioral intention to use Fintech services (Wang et al., 2003; Singh et al., 2020). Moreover, the emergence of Fintech has led to the need for comprehensive risk-based mechanisms to embrace exposures to cyber risks while promoting institutionalization of cybersecurity among regulated firms with strategic controls (Ng & Kwok, 2017).

Security, prestige, user-friendliness, and aesthetics in accessing Fintech services are key factors that determine individuals' intentions to use Fintech, highlighting the importance of security in influencing user behavior (Darmansyah et al., 2020). Furthermore, the review of extant literature on Fintech emphasizes the need for a high security level in wired and wireless networks to protect users' systems from harmful viruses and malware when accessing Fintech services (Hwang et al., 2021; Suzianti et al., 2021). The study also suggests that the higher the security features provided by a mobile payment service, the higher the ease of use for users to transact, indicating the significant role of security in shaping user behavior (Novika et al., 2021).

In the context of cybersecurity, the literature emphasizes the importance of data security, customer trust, and user design interface in influencing the adoption of Fintech (Stewart & Jürjens, 2018). Additionally, the theoretical construct for future Fintech industry development should ensure sound security mechanisms based on observed security and privacy concerns and their solutions (Dorfleitner et al., 2021). Moreover, the effects of trust, security, and privacy are crucial in understanding the pattern of adoption, indicating the significance of these factors in shaping user behavior (Shin, 2010).

In conclusion, behavioral analysis in Fintech cybersecurity is essential for understanding user behavior and its implications for security, analyzing patterns of behavior in Fintech transactions, and implementing adaptive security measures. The literature underscores the critical role of trust, perceived ease of use, social influence, and security features in influencing user behavior and acceptance of Fintech services. These insights are valuable for developing adaptive security measures and enhancing cybersecurity in the Fintech domain.

6. Case Studies and Examples

In the successful integration of human factors in Fintech cybersecurity, it is crucial to understand the characterization and measurement of maliciousness for cybersecurity risk assessment (King et al., 2018). This involves considering the rationality, expertise, malevolence, and insider access of individuals involved in cybersecurity (King et al., 2018). Additionally, leveraging human factors in cybersecurity through an integrated methodological approach is essential for comprehensive management of cybersecurity in organizations (Pollini et al., 2021). This approach involves moving from a 'human-as-problem' to a 'human-as-solution' mindset, emphasizing the importance of understanding users' perspectives and designing interfaces with humans in mind (Zimmermann & Renaud, 2019).

In contrast, instances of cybersecurity failures due to ignoring human factors can be observed in retrospectives of FinTech projects, where the success and failure factors of FinTech applications adopted by non-financial organizations are explored (Jinasena et al., 2020). Additionally, data security and consumer trust in FinTech innovation in Germany highlight the importance of examining how online vendors are performing with regard to FinTech to satisfy the needs of customers via case studies (Stewart & Jürjens, 2018). These examples underscore the significance of considering human factors in the design and implementation of cybersecurity measures within the FinTech industry.

Lessons learned and best practices from these case studies and examples emphasize the need for an integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviors in various contexts, including school environments (Antunes et al., 2021). This strategy aims to address the human factor's key role in information security and cybersecurity, highlighting the importance of understanding attitudes and behaviors towards cybersecurity (Antunes et al., 2021). By integrating these insights and best practices, organizations can develop more effective cybersecurity strategies that account for human factors and promote a 'human-as-solution' mindset.

Overall, the successful integration of human factors in Fintech cybersecurity requires a comprehensive understanding of maliciousness characterization, leveraging human factors through an integrated methodological approach, and adopting an integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviors. By learning from instances of cybersecurity failures due to ignoring human factors and implementing best practices, organizations can enhance their cybersecurity measures and mitigate potential risks associated with human factors.

7. Future Trends and Challenges

The future of financial technology (Fintech) is poised to be shaped by emerging technologies such as mobile payments, artificial intelligence, blockchain, and machine learning. These technologies are expected to revolutionize the financial landscape, offering increased efficiency, accessibility, and customer experience in financial services (Li & Zhang, 2021). However, the integration of these emerging technologies in Fintech also brings forth significant cybersecurity implications. Ensuring consumer safety, avoiding information leakage, and addressing cybersecurity risks are becoming paramount tasks for enterprises and banks in the Fintech sector (Awaliyah, 2023; Alexandri et al., 2023). The rapid expansion of Fintech, particularly in the Asia-Pacific region, has raised concerns about cybersecurity, digital identity, and electronic know-your-customer utilities, especially with the rise of "TechFins" such as Alibaba and Tencent (Susantono & Park, 2020).

Anticipated changes in user behavior are expected to have a profound impact on security in the Fintech sector. The adoption of Fintech presents challenges such as regulatory compliance, consumer protection, and cybersecurity risks (Alexandri et al., 2023). Moreover, the increasing reliance on mobile apps for financial transactions introduces a broad spectrum of cybersecurity threats, including data breaches, malware attacks, phishing schemes, and identity theft (Buckley et al., 2020). As user behavior continues to evolve towards digital financial interactions, the need to address these cybersecurity challenges becomes increasingly critical.

Addressing the evolving challenges in the Fintech cybersecurity landscape requires the development of practical and systematic frameworks for Fintech (Mustapha, 2023). Additionally, there is a need for a global view and future insights into Fintech and cybersecurity, leveraging emerging technologies such as blockchain and artificial intelligence to enhance security measures (Suryono et al., 2020). Furthermore, the impact of Fintech on corporate technology innovation and banking service transformation necessitates a balance between increasing financial inclusion and effective risk management, infrastructure development, and data protection for consumers (Awaliyah, 2023; Rai, 2023).

In conclusion, the future trends in Fintech are closely intertwined with the adoption of emerging technologies and the evolving behavior of users. While these trends offer significant opportunities for innovation and transformation in the financial sector, they also present complex challenges, particularly in cybersecurity. As Fintech continues to reshape the financial services landscape, it is imperative to proactively address these challenges to ensure the security and integrity of Fintech applications and platforms.

8. Recommendation

This investigation into the intersection of human factors and cybersecurity within the rapidly evolving fintech landscape has revealed several crucial insights. Firstly, human errors and behaviors significantly contribute to cybersecurity vulnerabilities. Users' lack of awareness, susceptibility to social engineering, and suboptimal cybersecurity practices can pose substantial threats. Moreover, the complexity of fintech systems often leads to user confusion, increasing the likelihood of security breaches. Understanding and addressing these human-centric challenges is paramount in fortifying fintech cybersecurity.

The findings underscore the need for continuous research and development in the field of human factors in cybersecurity, especially within the fintech sector. Future studies should delve deeper into user behavior patterns, cognitive biases, and the impact of human-machine interactions on cybersecurity. Additionally, investigating the efficacy of current educational programs and awareness campaigns is essential. As technology evolves, so do cyber threats, necessitating ongoing R&D efforts to adapt and enhance security measures.

Fintech platforms must adopt a user-centric approach in their design, focusing on simplicity and clarity. Interfaces should be intuitive, reducing the likelihood of user errors and enhancing overall cybersecurity. Launch comprehensive educational initiatives to enhance user awareness of cybersecurity risks and best practices. Training programs should be accessible, engaging, and regularly updated to reflect evolving threats. Implement advanced behavioral analytics to detect abnormal user activities and potential security threats. Monitoring user behavior patterns can aid in early identification of suspicious activities, allowing for timely intervention. Foster effective collaboration between humans and machines. Leverage artificial intelligence and machine learning algorithms to automate routine security tasks, allowing human experts to focus on more complex and strategic aspects of cybersecurity. Regularly assess and update cybersecurity protocols, considering the dynamic nature of cyber threats. Periodic evaluations should include user feedback and experiences to ensure that security measures remain effective and user-friendly.

9. Conclusion

In conclusion, the symbiotic relationship between human factors and cybersecurity in fintech necessitates a holistic and proactive approach. By integrating human-centric strategies, fostering user awareness, and leveraging advanced technologies, the fintech industry can enhance its cybersecurity posture in the face of evolving threats. This journey demands ongoing collaboration between researchers, developers, and end-users to create a resilient and secure fintech landscape.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2023. Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security.

[2] Adaga, E.M., Egieya, Z.E., Ewuga, S.K., Abdul, A.A. and Abrahams, T.O., 2024. Philosophy In Business Analytics: A Review Of Sustainable And Ethical Approaches. *International Journal of Management & Entrepreneurship Research*, *6*(1), pp.69-86.

[3] Adeleke, O.K., Segun, I.B. and Olaoye, A.I.C., 2019. Impact of internal control on fraud prevention in deposit money banks in Nigeria. *Nigerian Studies in Economics and Management Sciences*, *2*(1), pp.42-51.

[4] Aggarwal, A., Niezen, G., & Thimbleby, H. (2014). User experience evaluation through the brain's electrical activity. https://doi.org/10.1145/2639189.2639236

[5] Akiki, P. and Bandara, A. (2014). Adaptive model-driven user interface development systems. Acm Computing Surveys, 47(1), 1-33. https://doi.org/10.1145/2597999

[6] Alexandri, M., Usman, I., Narimawati, U., & Taryana, A. (2023). Unraveling the fintech landscape: a systematic mapping study on the impact of financial technology innovation on investment decision-making in asean banking. Khazanah Sosial, 5(1), 113-124. https://doi.org/10.15575/ks.v5i1.24555

[7] Alvarez, J. and Emory, E. (2006). Executive function and the frontal lobes: a meta-analytic review. Neuropsychology Review, 16(1), 17-42. https://doi.org/10.1007/s11065-006-9002-x

[8] Antunes, M., Silva, C., & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. Applied Sciences, 11(23), 11269. https://doi.org/10.3390/app112311269

[9] Awaliyah, T. (2023). The impact of financial technology innovation on banking service transformation: a case study in the fintech industry. Global, 1(3), 306-313. https://doi.org/10.59613/global.v1i3.47

[10] Back, S. and Guerette, R. (2021). Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing attacks. Journal of Contemporary Criminal Justice, 37(3), 427-451. https://doi.org/10.1177/10439862211001628

[11] Baumer, E. (2017). Toward human-centered algorithm design. Big Data & Society, 4(2), 205395171771885. https://doi.org/10.1177/2053951717718854

[12] Buckley, R., Avgouleas, E., & Arner, D. (2020). Three decades of international financial crises: what have we learned and what still needs to be done?.. https://doi.org/10.22617/wps200171-2

[13] Chao, J., Chao, S., Yao, L., & Liu, C. (2016). A case study of design and usability evaluation of the collaborative problem solving instructional platform system. Eurasia Journal of Mathematics Science and Technology Education, 12(10). https://doi.org/10.12973/eurasia.2016.1278a

[14] Chaudhary, K. and Murano, P. (2021). The design and evaluation of a new smartwatch user interface. International Journal of Interactive Mobile Technologies (Ijim), 15(13), 128. https://doi.org/10.3991/ijim.v15i13.22701

[15] Chun, J., Dey, A., Lee, K., & Kim, S. (2018). A qualitative study of smartwatch usage and its usability. Human Factors and Ergonomics in Manufacturing & Service Industries, 28(4), 186-199. https://doi.org/10.1002/hfm.20733

[16] Connolly, J. and Phillips, I. (2002). User-system interface design., 119-132. https://doi.org/10.1007/978-0-387-35611-2_8

[17] Dawson, J. and Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. Frontiers in Psychology, 9. https://doi.org/10.3389/fpsyg.2018.00744

[18] Dinev, T. and Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 386-408. https://doi.org/10.17705/1jais.00133

[19] Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2021). Promise not fulfilled: fintech data privacy, and the gdpr. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3950094

[20] Fabian, A.A., Uchechukwu, E.S., Okoye, C.C. and Okeke, N.M., (2023). Corporate Outsourcing and Organizational Performance in Nigerian Investment Banks. *Sch J Econ Bus Manag, 2023Apr*, *10*(3), pp.46-57.

[21] Fianto, B., Hendratmi, A., & Aziz, P. (2020). Factors determining behavioral intentions to use islamic financial technology. Journal of Islamic Marketing, 12(4), 794-812. https://doi.org/10.1108/jima-12-2019-0252

[22] Grahn, H. and Kujala, T. (2020). Impacts of touch screen size, user interface design, and subtask boundaries on in-car task's visual demand and driver distraction. International Journal of Human-Computer Studies, 142, 102467. https://doi.org/10.1016/j.ijhcs.2020.102467

[23] Gutzwiller, R., Ferguson-Walter, K., & Fugate, S. (2019). Are cyber attackers thinking fast and slow? exploratory analysis reveals evidence of decision-making biases in red teamers. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 427-431. https://doi.org/10.1177/1071181319631096

[24] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[25] Hadlington, L. and Murphy, K. (2018). Is media multitasking good for cybersecurity? exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cybersecurity behaviors. Cyberpsychology Behavior and Social Networking, 21(3), 168-172. https://doi.org/10.1089/cyber.2017.0524

[26] Holcomb, R. and Tharp, A. (1991). What users say about software usability. International Journal of Human-Computer Interaction, 3(1), 49-78. https://doi.org/10.1080/10447319109525996

[27] Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organizational culture*. Decision Sciences, 43(4), 615-660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

[28] Hwang, Y., Park, S., & Shin, N. (2021). Sustainable development of a mobile payment security environment using fintech solutions. Sustainability, 13(15), 8375. https://doi.org/10.3390/su13158375

[29] Ilugbusi, S., Akindejoye, J.A., Ajala, R.B. and Ogundele, A., 2020. Financial liberalization and economic growth in Nigeria (1986-2018). *International Journal of Innovative Science and Research Technology*, *5*(4), pp.1-9.

[30] Ji, Y., Park, J., Lee, C., & Yun, M. (2006). A usability checklist for the usability evaluation of mobile phone user interface. International Journal of Human-Computer Interaction, 20(3), 207-231. https://doi.org/10.1207/s15327590ijhc2003_3

[31] Jinasena, D., Spanaki, K., Papadopoulos, T., & Balta, M. (2020). Success and failure retrospectives of fintech projects: a case study approach. Information Systems Frontiers, 25(1), 259-274. https://doi.org/10.1007/s10796-020-10079-4

[32] King, Z., Henshel, D., Flora, L., Cains, M., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in Psychology, 9. https://doi.org/10.3389/fpsyg.2018.00039

[33] Koyuncu, M. and Pusatli, O. (2019). Security awareness level of smartphone users: an exploratory case study. Mobile Information Systems, 2019, 1-11. https://doi.org/10.1155/2019/2786913

[34] Li, B. and Zhang, X. (2021). Insights into financial technology (fintech): a bibliometric and visual study. Financial Innovation, 7(1). https://doi.org/10.1186/s40854-021-00285-7

[35] Li, Q. (2002). An integrated methodology for user interface design: human factors in use case driven development process. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 46(5), 675-679. https://doi.org/10.1177/154193120204600516

[36] Lu, H., wang, B., Wu, Q., & Ye, J. (2020). Fintech and the future of financial service: a literature review and research agenda. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3600627

[37] Meskens, J., Luyten, K., & Coninx, K. (2009). Plug-and-design.. https://doi.org/10.1145/1570433.1570461

[38] Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P., & Glenn, T. (2021). Increasing cybercrime since the pandemic: concerns for psychiatry. Current Psychiatry Reports, 23(4). https://doi.org/10.1007/s11920-021-01228-w

[39] Mustapha, I. (2023). Cybersecurity challenges and solutions in the fintech mobile app ecosystem. International Journal of Interactive Mobile Technologies (IJIM), 17(22), 100-116. https://doi.org/10.3991/ijim.v17i22.45261

[40] Ng, A. and Kwok, B. (2017). Emergence of fintech and cybersecurity in a global financial centre. Journal of Financial Regulation and Compliance, 25(4), 422-434. https://doi.org/10.1108/jfrc-01-2017-0013

[41] Novika, F., Halim, R., & Setyawan, A. (2021). The effect of technological and behavioral on the adoption of the shopeepay mobile payment. Journal of Entrepreneur & Business, 2(2), 106. https://doi.org/10.24123/jeb.v2i2.4641

[42] Pollini, A., Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., … & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition Technology & Work, 24(2), 371-390. https://doi.org/10.1007/s10111-021-00683-y

[43] Rai, S. (2023). A study on financial technology &amp; cyber security in india. International Scientific Journal of Engineering and Management, 02(04). https://doi.org/10.55041/isjem00350

[44] Rao, V., Luk, W., & Warren, J. (2005). Issues in building multiuser interfaces. International Journal of Human-Computer Interaction, 19(1), 55-74. https://doi.org/10.1207/s15327590ijhc1901_5

[45] Salthouse, T. (2012). Consequences of age-related cognitive declines. Annual Review of Psychology, 63(1), 201-226. https://doi.org/10.1146/annurev-psych-120710-100328

[46] Sanctorum, A. and Signer, B. (2019). A unifying reference framework and model for adaptive distributed hybrid user interfaces.. https://doi.org/10.1109/rcis.2019.8877048

[47] Sanctorum, A., Kieffer, S., & Signer, B. (2020). User-driven design guidelines for the authoring of cross-device and internet of things applications.. https://doi.org/10.1145/3419249.3420136

[48] Shin, D. (2010). The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption. Interacting With Computers, 22(5), 428-438. https://doi.org/10.1016/j.intcom.2010.05.001

[49] Shneiderman, B. (1987). Designing the user interface strategies for effective human-computer interaction. Acm Sigbio Newsletter, 9(1), 6. https://doi.org/10.1145/25065.950626

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

[51] Stewart, H. and Jürjens, J. (2018). Data security and consumer trust in fintech innovation in germany. Information and Computer Security, 26(1), 109-128. https://doi.org/10.1108/ics-06-2017-0039

[52] Suryono, R., Budi, I., & Purwandari, B. (2020). Challenges and trends of financial technology (fintech): a systematic literature review. Information, 11(12), 590. https://doi.org/10.3390/info11120590

[53] Susantono, B. and Park, C. (2020). Future of regional cooperation in asia and the pacific.. https://doi.org/10.22617/tcs200336-2

[54] Suzianti, A., Haqqi, F., & Fathia, S. (2021). Strategic recommendations for financial technology service development: a comprehensive risk-benefit ipa-kano analysis. Journal of Modelling in Management, 17(4), 1481-1503. https://doi.org/10.1108/jm2-11-2020-0297

[55] Uchechukwu, E.S., Amechi, A.F., Okoye, C.C. and Okeke, N.M., 2023. Youth Unemployment and Security Challenges in Anambra State, Nigeria. *Sch J Arts Humanit Soc Sci*, *4*, pp.81-91.

[56] Vincent, A.A., Segun, I.B., Loretta, N.N. and Abiola, A., 2021. Entrepreneurship, agricultural value-chain and exports in Nigeria. *United International Journal for Research and Technology*, *2*(08), pp.1-8.

[57] Wang, Y., Wang, Y., Lin, H., & Tang, T. (2003). Determinants of user acceptance of internet banking: an empirical study. International Journal of Service Industry Management, 14(5), 501-519. https://doi.org/10.1108/09564230310500192

[58] Zhao, Y. (2022). Interaction design system for artificial intelligence user interfaces based on uml extension mechanisms. Mobile Information Systems, 2022, 1-8. https://doi.org/10.1155/2022/3534167

[59] Zhong-qing, H., Ding, S., Li, S., Chen, L., & Yang, S. (2019). Adoption intention of fintech services for bank users: an empirical examination with an extended technology acceptance model. Symmetry, 11(3), 340. https://doi.org/10.3390/sym11030340

[60] Zimmermann, V. and Renaud, K. (2019). Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. International Journal of Human-Computer Studies, 131, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005