Borneo International Journal eISSN 2636-9826; Vol.8 (4); 2025; 64-67
Published by *Majmuah Enterprise*
www.majmuah.com

The Effectiveness and Adoption Challenges of Multi-Factor Authentication (MFA) on Social Media Platforms

Cui Yuchong

School of Computing, Universiti Utara Malaysia, MALAYSIA
Email: cuiyuchong00@email.com | Tel: +60109753185 |

Received: December 27, 2025
Accepted: December 30, 2025
Online Published: December 31, 2025

Abstract

The contemporary digital landscape is shaped by rapid Digital Transformation (DT), in which high-stakes identity services such as financial systems, e-commerce platforms, and cloud providers collectively function as converged social media platforms. Within this ecosystem, robust authentication is the primary defense against systemic identity threats. Multi-Factor Authentication (MFA) provides statistically strong protection, preventing over 99.9% of account compromise attempts even when primary credentials are exposed. However, this technical effectiveness is undermined by low adoption and inconsistent usage, creating a critical security paradox. This paper analyzes the hierarchical vulnerabilities of MFA modalities, highlighting the elevated risks of legacy SMS-based methods prone to SIM swapping and the exploitation of human factors through sophisticated social engineering, including MFA fatigue attacks. Using an extended Unified Theory of Acceptance and Use of Technology (UTAUT) framework, the study shows that usability friction, increased cognitive load, and low user trust are dominant socio-technical barriers. The discussion advocates a mandatory shift toward phishing-resistant, FIDO2-based authentication and the deployment of adaptive authentication frameworks to align cryptographic strength with sustainable user behavioural compliance.

Keywords: Multi-Factor Authentication; Cybersecurity; User Adoption; FIDO2; Cognitive Load.

1. Introduction

The global digital economy is increasingly driven by Digital Transformation (DT), where organizational processes, communication, and commercial activities migrate to cloud infrastructures and mobile platforms (Saeed et al., 2023; Henen, 2025). As more services depend on interconnected systems, large volumes of Personally Identifiable Information (PII) and financial data become concentrated in centralized environments, creating attractive targets for cyber-criminals (Patidar, 2025; Chang et al., 2023) For the purpose of this study, the term social media platforms refers broadly to digital services in which identity and access management (IAM) is critical, including social networks, e-commerce, enterprise systems, and financial applications. Security incidents rarely remain isolated. A breach in one platform often exposes credentials or personal information that can be reused across others, contributing to cascading identity theft and compromise (Ghadge, 2024; Birchwood University, 2023). Multi-Factor Authentication (MFA) is therefore recognized as a core control within identity-centric cybersecurity architectures (Meyer et al., 2023; Kietzman, 2025). By requiring two or more independent verification factor, knowledge, possession, or inherence MFA significantly reduces the likelihood of unauthorized access (Zaky, 2022). Empirical research shows that MFA protects more than 99.99 percent of commercial accounts and remains effective even when credentials have been leaked, while also mitigating phishing attempts (Meyer et al., 2023; Kamaruddin & Zolkipli, 2024). Despite this proven strength, a persistent socio-technical paradox remains. Users frequently resist MFA due to perceived inconvenience, cognitive burden, and usability challenges, leading to risky workarounds and vulnerability to emerging attacks such as MFA fatigue or push bombing (Gupta, 2024; OIT, 2024; SoSafe Awareness, 2025). Consequently, the central issue is not only technological deployment but achieving a workable balance between usability and security within converged digital ecosystems.

2. Methodology

This study adopts a conceptual, literature-driven methodology designed to examine the effectiveness and adoption challenges of Multi-Factor Authentication (MFA) across converged digital platforms. The analysis is grounded in peer-reviewed journal articles, cybersecurity advisories, incident reports, and empirical studies published by credible institutions between 2022 and 2025, ensuring both recency and relevance to contemporary threat environments. Sources were selected using thematic criteria focusing on identity-centric attacks, MFA technology performance, phishing-resistant authentication, and user-adoption behaviour in secure systems. Special attention was given to reports

documenting real-world incidents involving SIM-swapping, MFA fatigue, and adversary-in-the-middle phishing, as these illustrate how socio-technical weaknesses persist despite strong cryptographic controls. The literature was reviewed and synthesized using a structured thematic approach. First, MFA modalities were categorized according to resilience levels, ranging from SMS-based authentication to FIDO2 passkeys. Second, adoption barriers were mapped against behavioural constructs drawn from the Unified Theory of Acceptance and Use of Technology (UTAUT), including perceived usefulness, effort expectancy, trust, and perceived risk. Finally, the findings were integrated to evaluate how usability frictions and cognitive load interact with technology design to influence real-world MFA deployment. Rather than conducting primary data collection, this methodological approach emphasizes conceptual integration and critical interpretation. It enables a comprehensive understanding of how technical safeguards, human behaviour, and organizational policies intersect to shape MFA effectiveness across social media and identity-driven digital ecosystems.

3. Results and discussion

The findings reveal a clear security–usability paradox surrounding Multi-Factor Authentication (MFA). Although MFA consistently demonstrates strong protection against credential-based attacks, its effectiveness is constrained by uneven implementation and human behavioural factors. Users frequently perceive MFA as inconvenient, particularly when authentication steps interrupt routine activity or introduce additional cognitive effort. This perception encourages workarounds such as sharing authentication codes or storing tokens insecurely, weakening overall system resilience (Gupta, 2024). The analysis further highlights that attacker strategies increasingly target human decision-making rather than technical controls. MFA-fatigue attacks, for example, repeatedly trigger push notifications until users approve unauthorized access, as seen in several recent corporate breaches (OIT, 2024; SoSafe Awareness, 2025). Likewise, adversary-in-the-middle phishing kits exploit session cookies to bypass traditional verification flows even after users successfully complete MFA challenges. These incidents illustrate that cybersecurity failure often stems less from cryptographic weakness than from behavioural manipulation and process gaps. Mapping these observations to the UTAUT framework shows that performance expectancy remains high because users recognize MFA as effective. However, effort expectancy declines when authentication appears repetitive, intrusive, or confusing. Trust deficits especially concerns regarding data privacy and platform reliability further discourage consistent adoption. Meanwhile, perceived risk can paradoxically reduce usage when individuals fear losing access or mishandling biometric or hardware-based credentials. Together, these socio-technical factors mediate whether MFA is used correctly and consistently across platforms.

The findings also suggest that technological upgrades alone are insufficient. Phishing-resistant approaches such as FIDO2 significantly reduce exposure to SIM-swapping and credential replay, yet adoption remains slow when users are not supported with clear guidance, intuitive design, and institutional transparency. Adaptive authentication systems provide a promising pathway by calibrating friction to contextual risk, prompting stronger verification only when anomalies occur. This approach aligns security requirements with natural user behaviour, improving compliance while maintaining protection. The results indicate that MFA will reach its full defensive potential only when technical innovations are integrated with psychologically informed design and organizational policy. Effective strategies must simultaneously reduce cognitive burden, foster trust, and embed user education as a continuous component of identity security.

4. Conclusions

This study confirms that Multi-Factor Authentication (MFA) remains one of the most effective defenses against identity-centric cyber threats across converged digital platforms. Evidence consistently shows that MFA significantly reduces the probability of account compromise, even when primary credentials are exposed. However, the analysis also reveals a persistent implementation gap driven by the usability–security trade-off. Users often resist MFA when it increases effort or interrupts routine interaction, which in turn enables behavioural attacks such as MFA-fatigue and adversary-in-the-middle phishing. The integration of MFA effectiveness with the UTAUT framework demonstrates that adoption is influenced not only by technical capability but also by perceived effort, trust, and contextual risk. Where friction is high and confidence in platform reliability is low, correct and consistent use declines. Consequently, improving MFA outcomes requires addressing human factors alongside technological enhancements. Policy-driven migration toward phishing-resistant authentication, particularly FIDO2-based solutions, offers a critical pathway to reducing vulnerabilities associated with SMS codes and token interception. At the same time, adaptive authentication frameworks can balance protection with convenience by increasing verification thresholds only when contextual risk is elevated.

Overall, MFA will achieve its full potential only when organizations combine strong cryptographic controls with user-centred design, clear communication, and continuous education. Aligning security mechanisms with everyday user behaviour is essential for sustaining trust, improving compliance, and strengthening identity protection across digital ecosystems.

Acknowledgments

The author would like to express sincere appreciation to Universiti Utara Malaysia for providing the academic environment, resources, and opportunities that supported the completion of this study. Special gratitude is extended to the course lecturer for Cyber Security in Social Media for valuable guidance, constructive feedback, and continuous encouragement throughout the research process. The author is also grateful to classmates and peers whose discussions and shared perspectives helped refine the analytical insights presented in this paper. Finally, heartfelt appreciation is conveyed to the author's family for their patience, support, and constant motivation, which remained an important source of strength during the preparation of this work.

References

Birchwood University. (2023). Top 25 Real-World Case Studies Delineating Cybersecurity Incidents. https://www.birchwoodu.org/top-10-real-world-case-studies-on-cyber-security-incidents/

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), 2188122. https://doi.org/10.1080/17517575.2023.2188122

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance. Issues and Practice, 47*(3), 698. https://doi.org/10.1057/s41288-022-00266-6

Deepak Gupta. (2024). The psychology of security: Why users resist better authentication.https://guptadeepak.com/the-psychology-of-security-why-users-resist-better-authentication/

Ghadge, N. (2024). Challenges with securing digital identity. *International Journal on Cybernetics & Informatics (IJCI), 13*(13), 1. https://doi.org/10.5121/ijci.2024.130401

Henen, B. (2025). Cybersecurity in the Digital Era: Between Digital Transformation and Protection Challenges. *Law & World, 35, 117*. https://doi.org/10.36475/11.3.8

Kamaruddin, N. H. C., & Zolkipli, M. F. (2024). The Role of Multi-Factor Authentication in Mitigating Cyber Threats. *Borneo International Journal eISSN 2636-9826, 7*(4), 35–42. https://majmuah.com/journal/index.php/bij/article/view/667

Kim, J. (March 31, 2025). The pros and cons of different MFA methods. *Keeper Security*.https://www.keepersecurity.com/blog/2025/03/31/the-pros-and-cons-of-different-mfa-methods/

Lee, A. T., Ramasamy, R. K., & Subbarao, A. (2025, January). Understanding psychosocial barriers to healthcare technology adoption: A review of TAM technology acceptance model and unified theory of acceptance and use of technology and UTAUT frameworks. In *Healthcare* (Vol. 13, No. 3, p. 250). MDPI. https://doi.org/10.3390/healthcare13030250

Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Ferres, J. L. (2023). How effective is multifactor authentication at deterring cyberattacks? *arXiv preprint arXiv*:2305.00945. https://doi.org/10.48550/arXiv.2305.00945

Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. *Applied Sciences, 13*(19), 10871. https://doi.org/10.3390/app131910871

Nandi, L. A. (2022). Performance Appraisal as a Yardstick for Promotion in the Federal Capital Development Authority.*International Journal of Research Publication and Reviews*. https://doi.org/10.55248/gengpi.2022.3.10.69

Office of Innovative Technologies. (February 14, 2025). The need to replace SMS-based MFA. *University of Tennessee*. https://oit.utk.edu/security/learning-library/article-archive/the-need-to-replace-sms-based-mfa/

Olaniyi, O. (2025). A quantitative approach to understanding machine learning adoption for cybersecurity in e-commerce through the UTAUT model. *Unpublished dissertation*. https://doi.org/10.9734/jerr/2025/v27i111701

Patidar, A. (July 26, 2023). Learn the impact of identity theft on businesses in 2023. *LoginRadius*.https://www.loginradius.com/blog/identity/identity-theft-impact-on-businesses-in-2023

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666

Schuster, F., & Habibipour, A. (2024). Users' privacy and security concerns that affect IoT adoption in the home domain. *International Journal of Human–Computer Interaction, 40*(7), 1632–1643. https://doi.org/10.1080/10447318.2022.2147302

SoSafe Awareness. (2025). MFA fatigue attack. https://sosafe-awareness.com/en-us/glossary/mfa-fatigue-attack/

Syteca. (February 28, 2024). 7 real-life examples of insider threats caused by breaches. https://www.syteca.com/en/blog/real-life-examples-insider-threat-caused-breaches/

Ted Kietzman. (March 27, 2025). MFA adoption: The most important security metric. https://duo.com/blog/mfa-adoption-most-important-security-metric

Tsoloane, M., Thibela, A. B., & Maseko, P. H. (2025). Mobile transactions and financial services: Security, adoption and financial inclusion. *Businesses, 4*, Firstpage–Lastpage. https://doi.org/10.5281/zenodo.17372726

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets, 19*(2), 137–144. https://doi.org/10.1007/s12525-009-0012-4

Zaky, K., & Saxe, D. H. (2022). Multi-factor authentication. *IDPro Body of Knowledge, 1*(10). https://doi.org/10.55621/idpro.92