Available online at
https://journal.uitm.edu.my/ojs/index.php/JIKM

e-ISSN: 2289-5337

Journal of Information and Knowledge Management (JIKM)
Vol 15 Special Issue 2 (2025)

Journal of Information and Knowledge Management

Modelling Mobile Attachment and Cyber Hygiene Behavior of Users

Ferdinand Jilan Dawie, Mohamad Noorman Masrek*, Safawi Abdul Rahman

Faculty of Information Science, Universiti Teknologi MARA, UiTM Selangor Branch, Puncak Perdana Campus, 40150 Shah Alam, Selangor, Malaysia

Corresponding author's e-mail address: mnoorman@uitm.edu.my

ARTICLE INFO

Article history:
Received: 15 Jan 2025
Revised: 28 Feb 2025
Accepted: 1 Jun 2025
Published: 1 August 2025

Keywords:
Mobile Attachment
Functional Dependence
Mobile Identity
Deep Usage

https://doi.10.24191/jikm.v16iSI2.7171

ABSTRACT

This research examines how mobile attachment relates to cyber hygiene behaviors among mobile phone users in Malaysia. We adopt Partial Least Squares Structural Equation Modelling (PLS-SEM) to analyze survey data, the study. The findings suggest that functional dependence and deep structure use positively impact cyber hygiene intentions, while mobile identity has no direct effect. Theoretically, the study extends attachment theory by linking functional dependence with proactive security behaviors. Limitations include cultural specificity and self-reported data, highlighting the need for future studies across diverse populations to explore additional influences on mobile attachment and security behaviors.

INTRODUCTION

Mobile phones have become an integral part of modern life, influencing both personal and professional spheres. With the increasing reliance on mobile devices for communication, entertainment, and productivity, users often develop attachments that extend beyond functionality, incorporating these devices into their daily routines and self-identity (Meschtscherjakov, 2011). This attachment manifests in various forms, such as mobile functional dependence, where users rely on phones for essential tasks, and mobile identity, where the phone becomes a core part of personal expression. Additionally, users often engage in mobile deep structure use, which involves exploring advanced features to maximize the utility of their devices. These dynamics highlight the complex relationship between users and their mobile phones, reflecting not only functional reliance but also emotional and identity-driven connections.

Despite this growing bond with mobile devices, there is limited understanding of how mobile attachment influences users' behaviors, particularly in the realm of cybersecurity. Existing literature has largely focused on general mobile usage patterns, overlooking how specific attachments, like mobile identity, impact proactive cybersecurity behaviors, or mobile cyber hygiene. This gap calls for a deeper examination of the role of mobile attachment in shaping user intentions and actions regarding mobile security. Therefore, this research seeks to address the following question: How do mobile functional dependence, mobile identity, and mobile deep structure use relate to mobile cyber hygiene behavior?

LITERATURE REVIEW

Figure 1 illustrates the theoretical framework proposed in this research, showing the relationships between key constructs: Mobile Functional Dependence, Mobile Identity, Mobile Deep Structure Use, and Mobile Cyber Hygiene Intention. It outlines the hypothesized linkages between these variables, indicating how mobile attachment factors like functional dependence and identity influence both the deep structure use of mobile phones and cyber hygiene intentions. In the following sections, each of these linkages will be explained in detail, along with the development of the corresponding hypotheses.

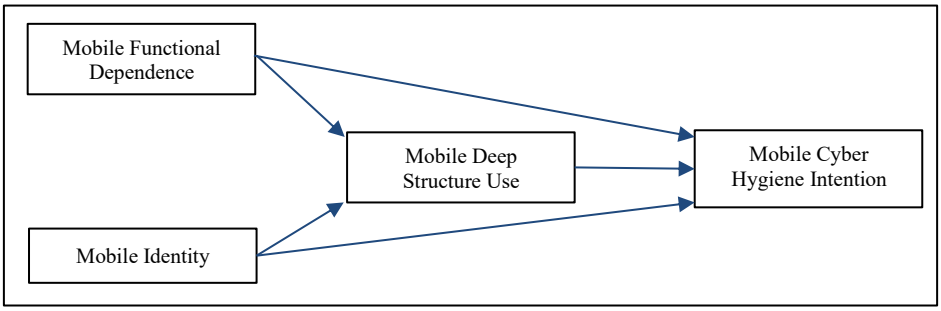

Figure 1: Theoretical Framework

Effective security behavior relies on the knowledge individuals gain about cybersecurity, which in turn fosters improved security practices (Kalhoro et al., 2021). Users are more capable of protecting themselves from threats and identifying theft when they possess a strong understanding of computer systems (Kalhoro et al., 2021). Cyber hygiene encompasses actions like scanning computers for viruses and utilizing strong passwords to ensure system security (Kalhoro et al., 2021). Cyber hygiene intention is defined as the willingness and commitment of individuals to engage in proactive behaviors aimed at maintaining and enhancing their cybersecurity posture.

Mobile deep structure use" refers to the utilization of various functions to carry out a range of tasks, indicating how extensively users make use of a system's features for activities such as communication, entertainment, socialization, and studying. This concept evaluates not only the number of features accessed but also how effectively these features are employed to assist with different tasks (Lou, Deng & Wang, 2022). Mobile deep structure use involves engaging with various functions on devices, which enhances users' awareness of security features and potential threats. As users explore these features, they are more likely to develop habits that prioritize cyber hygiene, such as using strong passwords and regularly updating software. This deeper engagement creates a positive feedback loop, reinforcing their intention to adopt proactive cybersecurity behaviors. Hence, the following hypothesis is established: H1-There is a positive and significant relationship between mobile deep structure use and mobile cyber hygiene intention.

Mobile functional dependence refers to the extent to which users rely on specific mobile phones to fulfill their functional needs, indicating a sustained interaction and close bond between users and their devices (Lou, Deng & Wang, 2022). This reliance goes beyond basic usage, reflecting a deeper connection where users often turn to their phones as an essential tool for daily activities. Over time, this relationship can foster a sense of attachment, as users integrate these devices into various aspects of their personal and social lives, highlighting the psychological and functional significance of mobile phones.

A high dependence on mobile devices inclines individuals to explore and utilize advanced features and functionalities, aiming to maximize the utility of these devices (Wehmeyer, 2007). This dependence fosters a deeper interaction with mobile technology, encouraging users to tap into sophisticated applications, settings, and tools that align with their specific needs. Moreover, as mobile functional dependence grows, users are likely to seek more efficient and comprehensive ways to integrate their devices into their daily

routines. This often leads to the adoption of advanced capabilities such as productivity tools, data management features, and customized applications that are characteristic of mobile deep structure use. To this effect, the study hypothesizes: H2-There is a positive and significant relationship between mobile functional dependence and mobile deep structure use

As users form a closer attachment to their devices due to reliance on them for both personal and professional tasks, they become more motivated to safeguard them against cyber threats (Lou et al., 2022). Mobile cyber hygiene practices become not only a protective measure but also a way for users to maintain the functionality and reliability of their devices. Thus, the more dependent users are on their mobile devices, the more likely they are to engage in cyber hygiene behaviors to preserve the integrity of their trusted devices. Based on this premise, the following hypothesis is established: H3-There is a positive and significant relationship between mobile functional dependence and mobile cyber hygiene intention.

Mobile identity refers to the extent to which users perceive their mobile phones as essential parts of their self-identity, a connection that goes beyond functional use and emphasizes the device's role in defining and sustaining personal identity while serving as an emotional anchor that provides meaning and purpose in life (Lou, Deng & Wang, 2022). This sense of identity connection allows users to express themselves through their mobile phones, as personal choices regarding apps, wallpapers, and customization reflect individual preferences and values. Additionally, this attachment fosters a deeper emotional bond, where the mobile phone becomes a source of comfort and personal significance, reinforcing its role in users' everyday lives and sense of self.

When a mobile phone becomes a core aspect of an individual's identity, they are likely to seek ways to maximize its utility, immersing themselves in its deeper functionalities (Trub & Barbot, 2016). This exploration may lead users to adopt more sophisticated tools and settings, allowing them to tailor the device to align more closely with their personal preferences and lifestyle. Additionally, users who view their mobile phones as part of their self-identity are more inclined to invest time in understanding and leveraging complex features that enhance their experience and further personalize the device. This drive to customize and engage with the phone at a deeper level results in increased mobile deep structure use, as users strive to make the device not only a reflection of themselves but also a versatile and integral part of their daily activities. Therefore, as mobile identity strengthens, users are more motivated to uncover and engage with advanced functionalities that allow for a more meaningful and individualized interaction with their devices. Accordingly, the following hypothesis is established: H4-There is a positive and significant relationship between mobile identity and mobile deep structure use.

Viewing mobile phones as integral to personal identity leads individuals to become more invested in protecting these devices, perceiving any threat to the device as a threat to a part of themselves (Roy, Ponnam & Mandal, 2017). This personal connection drives users to adopt cyber hygiene practices to safeguard their mobile devices, maintaining their emotional well-being and preserving their sense of identity. Furthermore, users who identify strongly with their mobile phones are more likely to feel a heightened responsibility to care for these devices, including securing them against potential cyber threats. By engaging in regular mobile security behaviors—such as updating software, using security apps, and avoiding risky online activities—these users not only protect their phones but also reinforce the stability and safety of this essential part of their identity. Given this background, we develop the following hypothesis: H5-There is a positive and significant relationship between mobile identity and mobile cyber hygiene intention.

METHODOLOGY

This study adopted a survey research methodology to examine the relationships between mobile attachment constructs and cyber hygiene behaviors among mobile phone users in Malaysia. Data were gathered using an online questionnaire created with Google Forms, which facilitated easy distribution and access for participants nationwide. The questionnaire items were adapted from well-established sources in

the literature, aligning each question with the constructs under investigation to ensure the measures accurately reflected the variables of interest.

To enhance the robustness of the instrument, the questionnaire was subjected to both pre-testing and pilot testing phases. These preliminary tests were conducted to evaluate the validity and reliability of the items, with results showing satisfactory levels in both aspects, thereby confirming the appropriateness of the instrument for the main study. The target population consisted of all mobile phone users in Malaysia, making the study highly relevant in a context where mobile devices are integral to daily life. A purposive and convenient sampling strategy was employed, allowing the research to capture data from individuals who were readily accessible and willing to participate.

Data analysis was conducted using Partial Least Squares Structural Equation Modeling (PLS-SEM), which provided a comprehensive means to assess the hypothesized relationships within the theoretical framework. This method was chosen for its ability to handle complex models and provide insights into both direct and indirect effects, enabling a detailed examination of the dynamics between mobile functional dependence, mobile identity, mobile deep structure use, and mobile cyber hygiene intention.

STUDY FINDINGS

Demographic

In terms of gender, 52.6% of participants are male, and 47.4% are female. The age distribution is diverse, with 13.1% aged 18-22, 19.2% aged 23-27, 20.8% aged 28-32, and smaller percentages in older age groups, such as 11.5% aged 33-37 and 9.5% aged 38-42. For academic qualifications, the majority hold a degree (39.3%), followed by certificate holders (24.4%), diploma holders (22.6%), master's degree holders (11.5%), and a small portion with doctorates (2.3%). Employment status is primarily split between government employees (35.7%) and non-government employees (36.8%), with 19.4% being students and smaller percentages in categories like retired (3.2%) and unemployed (4.7%). Regarding smartphone usage duration, nearly half of the participants (48.8%) have been using smartphones for over 10 years. Daily usage patterns reveal that 26.2% use their devices for 10-12 hours, 22.6% for 13-15 hours, and 18.1% for 7-9 hours, while fewer participants report lower or higher daily usage times. These statistics provide a comprehensive view of the participants.

Measurement Model Assessment

Table 1 provides an overview of the measurement model assessment, showing that all constructs surpass the recommended thresholds for factor loadings (≥0.6), composite reliability (≥0.7), and average variance extracted (AVE ≥0.5). These results confirm that each construct displays strong factor loadings, reliability, and convergent validity, supporting their suitability for further structural model analysis.

Table 1: Factor Loading, Composite Reliability & Average Variance Extracted

	Item Code	Factor Loading	Composite Reliability	Average Variance Extracted
Mobile Cyber Hygiene Intention	MCHI_1	0.644	0.855	0.599
	MCHI_2	0.833		
	MCHI_3	0.771		
	MCHI_4	0.832		
Mobile Deep Structure Use	MDSU_1	0.751	0.870	0.527
	MDSU_2	0.73		
	MDSU_3	0.626		
	MDSU_4	0.728		

	MDSU_5	0.76		
	MDSU_6	0.754		
Mobile Functional Dependence	MFD_1	0.836	0.893	0.676
	MFD_2	0.853		
	MFD_3	0.773		
	MFD_4	0.824		
Mobile Identity	MI_1	0.787	0.854	0.596
	MI_2	0.821		
	MI_3	0.807		
	MI_4	0.661		

Table 2 presents the discriminant validity assessment based on the Heterotrait-Monotrait Ratio (HTMT) criteria, ensuring that the constructs are distinct from one another. All HTMT values are below the recommended threshold of 0.85, which confirms that each construct—Mobile Cyber Hygiene Intention, Mobile Deep Structure Use, Mobile Functional Dependence, and Mobile Identity—demonstrates adequate discriminant validity, allowing for reliable differentiation between constructs in the model.

Table 2: Discriminant Validity Based on HTMT

	Mobile Cyber Hygiene Intention	Mobile Deep Structure Use	Mobile Functional Dependence	Mobile Identity
Mobile Cyber Hygiene Intention				
Mobile Deep Structure Use	0.618			
Mobile Functional Dependence	0.526	0.791		
Mobile Identity	0.384	0.806	0.737	

Structural Model Assessment & Hypothesis Testing

Table 3 presents the results of bootstrapping and blindfolding analyses conducted via the PLS-algorithm to assess the hypothesized relationships. The significance of each hypothesis is evaluated through path coefficients (β), t-values, and p-values, with a threshold of $t > 1.96$ and $p < 0.05$ required to support a hypothesis. Additional indicators, including effect sizes (f^2), explained variance (R^2), and predictive relevance (Q^2), are provided to illustrate the model's explanatory and predictive capacity.

The results indicate that most hypotheses are supported. The positive relationship between Mobile Deep Structure Use and Mobile Cyber Hygiene Intention is significant, confirming the importance of deep engagement with mobile features in promoting cyber hygiene behaviors. Similarly, Mobile Functional Dependence is positively related to Mobile Deep Structure Use, and it also significantly impacts Mobile Cyber Hygiene Intention, underscoring the role of reliance on mobile devices in fostering both advanced usage and proactive security practices. Furthermore, Mobile Identity shows a significant positive association with Mobile Deep Structure Use, suggesting that users who integrate their mobile phones into their self-identity are more likely to explore advanced functionalities.

However, the analysis reveals that the relationship between Mobile Identity and Mobile Cyber Hygiene Intention is not significant, indicating that while identity attachment may influence feature engagement, it does not directly drive intentions to engage in cyber hygiene behaviors. Overall, these findings highlight the critical role of mobile attachment constructs in understanding cyber hygiene behaviors, with the exception of the unsupported relationship in H5.

Table 3: Path Analysis

	β	T value	P values	f^2	R^2	Q^2	Hypothesis
H1: Mobile Deep Structure Use → Mobile Cyber Hygiene Intention	0.43	6.21	0	0.12	0.291	0.161	Supported
H2: Mobile Functional Dependence → Mobile Deep Structure Use	0.405	6.995	0	0.223	0.541	0.282	Supported
H3: Mobile Functional Dependence → Mobile Cyber Hygiene Intention	0.228	3.048	0.002	0.037	0.291	0.161	Supported
H4: Mobile Identity → Mobile Deep Structure Use	0.414	7.255	0	0.234	0.541	0.282	Supported
H5: Mobile Identity → Mobile Cyber Hygiene Intention	-0.1	1.592	0.112	0.007	0.291	0.161	Not Supported

DISCUSSION

The findings of this study provide insights into the complex relationships between mobile attachment constructs—such as mobile functional dependence and mobile identity—and cyber hygiene behaviors. This discussion section will explore how these results answer the research questions and align with existing literature.

The positive relationship between mobile deep structure use and mobile cyber hygiene intention (H1) indicates that users who engage deeply with mobile features are more likely to adopt cyber hygiene practices. This finding aligns with previous studies, which suggest that users who explore and utilize advanced functions of their devices develop a heightened awareness of security features and potential risks (Lou et al., 2022). Such engagement reinforces security behaviors, as users recognize the importance of protecting the functionalities they depend on. By understanding how to navigate these features, users are more equipped to implement security measures, confirming the significant role of deep feature usage in fostering proactive cybersecurity behaviors.

The significant association between mobile functional dependence and mobile deep structure use (H2) further supports the notion that reliance on mobile devices encourages users to explore advanced functionalities. This finding corroborates the work of Wehmeyer (2007), who emphasized that users highly dependent on mobile devices are motivated to integrate these devices into various facets of their daily lives, leading to a more sophisticated and comprehensive use of device features. As users rely on mobile devices for personal and professional needs, they naturally explore additional functionalities, enhancing their engagement and proficiency in using their devices at an advanced level.

The study also found a positive relationship between mobile functional dependence and cyber hygiene intention (H3), suggesting that as users become more reliant on their mobile devices, they are more inclined to protect them. This is consistent with Lou et al. (2022), who highlighted that attachment to mobile devices prompts users to adopt protective measures to maintain the reliability and integrity of their devices. Users dependent on mobile functions are likely to view security practices as essential for ensuring their devices remain functional and safe, reinforcing the link between functional dependence and cyber hygiene behaviors.

Mobile identity was found to have a significant positive relationship with mobile deep structure use (H4), indicating that users who view their mobile phones as extensions of their self-identity are more likely to explore advanced features. This aligns with findings by Trub and Barbot (2016), who observed that when mobile devices become integral to users' self-concept, they are motivated to tailor the device to meet their personal preferences, often by leveraging complex functionalities. This engagement enhances the device's utility, allowing users to further personalize it and integrate it into various aspects of their identity expression.

Finally, the relationship between mobile identity and cyber hygiene intention (H5) was not supported, indicating that while mobile identity influences advanced feature engagement, it does not directly drive intentions to adopt cyber hygiene practices. This suggests that emotional and identity-based attachment does not necessarily translate to protective behaviors, potentially because the emotional value placed on the device may not inherently involve security considerations. Previous research by Roy et al. (2017) also reflects this divergence, suggesting that identity-based attachment may prioritize personalization over security concerns. This finding highlights a gap where identity-driven mobile use does not naturally extend to proactive security practices, which could have implications for future research on motivating cyber hygiene behaviors among identity-driven users.

CONCLUSION & RECOMMENDATIONS

This study makes significant theoretical and practical contributions by examining how mobile attachment constructs—specifically, mobile functional dependence and mobile identity—relate to cyber hygiene behaviors. Theoretically, it extends attachment theory within the mobile context, demonstrating that functional dependence and deep structure use are key drivers of cybersecurity intentions, whereas identity-based attachment does not necessarily lead to proactive security practices. This suggests that reliance on device functionality has a stronger influence on security behaviors than emotional attachment alone, providing a nuanced understanding of mobile attachment's role in cybersecurity.

Practically, the findings offer insights for enhancing mobile device security through targeted strategies. Recognizing that users who deeply engage with their devices are more likely to adopt cyber hygiene behaviors suggests that promoting feature-oriented engagement can support cybersecurity efforts. This information is useful for cybersecurity educators, app developers, and mobile device manufacturers, who can design features that not only increase user attachment but also encourage security practices, ultimately contributing to safer mobile usage.

This study has certain limitations that provide avenues for future research. Firstly, the sample was restricted to mobile phone users in Malaysia, which may limit the generalizability of the findings to other cultural contexts. Future research could replicate this study in different regions to examine potential cultural influences on mobile attachment and cyber hygiene behaviors. Secondly, the use of self-reported data may introduce response biases, as participants could overestimate their security practices. Future studies might incorporate behavioral data or longitudinal designs to gain a more accurate view of cyber hygiene behaviors over time.

Additionally, while this study focused on mobile functional dependence and mobile identity, other factors such as mobile device type, usage patterns, or specific apps that could influence attachment and security practices. Future research could explore these variables to provide a more comprehensive understanding of the factors that drive mobile attachment and cyber hygiene intentions. This broader perspective could enhance the development of interventions that promote safer mobile device usage in various user segments.

ACKNOWLEDGEMENT

This paper was presented at the 6th International Conference of Information Science 2025. The authors would like to thank to the Institute of Postgraduate Studies (IPSis). and Universiti Teknologi MARA, Puncak Perdana Campus of UiTM Selangor Branch for research support and opportunities.

REFERENCES

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access*, *9*, 99339-99363.

Lou, J., Deng, L., & Wang, D. (2022). Understanding the deep structure use of mobile phones–an attachment perspective. *Behaviour & Information Technology*, *41*(15), 3191-3209.

Lou, J., Han, N., Wang, D., & Pei, X. (2022). Effects of mobile identity on smartphone symbolic use: An attachment theory perspective. *International Journal of Environmental Research and Public Health*, *19*(21), 14036.

Wehmeyer, K. (2007, July). Assessing users' attachment to their mobile devices. In *International conference on the management of mobile business (ICMB 2007)* (pp. 16-16). IEEE.

Meschtscherjakov, D. A. (2011). *Mobile attachment: Investigating emotional attachment to mobile devices and services from an HCI perspective* (Doctoral dissertation). Faculty of Natural Sciences, Paris Lodron University of Salzburg, Austria.

Roy, S., Ponnam, A., & Mandal, S. (2017). Comprehending technology attachment in the case of smart phone-applications: an empirical study. *Journal of Electronic Commerce in Organizations (JECO)*, *15*(1), 23-43.

Trub, L., & Barbot, B. (2016). The paradox of phone attachment: Development and validation of the Young Adult Attachment to Phone Scale (YAPS). *Computers in Human Behavior*, *64*, 663-672.