Multinesa: Jurnal Nusantara Multidisciplinary
Volume 1, Number 2, 2025
P-ISSN: xxxx-xxxx E-ISSN : xxxx-xxxx
Open Access: https://jurnal.risetprass.com/multinesa

The Influence of Information System Security on Intention to Use Digital Health Apps in Indonesia

Prasetyo Harisandi
[1] Universitas Pendidikan Indonesia, Bandung, Indonesia
Correspondence: prasetyoharisandi@upi.ac.id

Article Info

Article history:
Received Aug 27th, 2025
Revised Aug 30th, 2025
Accepted Oct 05th, 2025

Keyword:
Information system security, trust, attitude toward use, intention to use, mobile health applications

ABSTRACT

This study examined the role of information system security in influencing the intention to use mobile health applications in Indonesia. The research employed a quantitative approach with an explanatory design, involving 250 respondents who had experience using mobile health applications. Data were collected through an online questionnaire and analyzed using structural equation modeling. The results showed that information system security had a significant positive effect on trust, which in turn influenced both attitude toward use and intention to use. Attitude was also found to significantly predict intention to use. Although information system security had a direct effect on intention, its impact was weaker compared to the indirect effects through trust and attitude. The findings suggested that security features alone were insufficient to drive adoption, as users placed greater importance on the psychological assurance of trust and favorable attitudes. The study concluded that the successful adoption of mobile health applications required not only strong technical safeguards but also effective strategies to enhance user confidence and positive perceptions.

INTRODUCTION

The development of digital technology has brought significant changes to the provision of healthcare services in Indonesia (Harisandi et al., 2023). The presence of digital health apps (mobile health apps), such as Halodoc, Alodokter, and SehatQ, has become an innovative solution to bridge the gap in access to medical services, especially in areas with uneven distribution of healthcare professionals. According to a report by (Petropoulou et al., 2023) the adoption of health apps in Southeast Asia has increased rapidly following the COVID-19 pandemic, in line with growing public awareness of the importance of digital-based health monitoring (Harisandi, Nurhidayah, et al., 2024)

However, despite this significant potential, serious challenges related to information system security lie (Harisandi, 2025). Issues of personal data protection, the risk of medical information leaks, and doubts about system reliability are often key barriers to the adoption of this technology. Previous research has shown that while the public recognises the benefits of health apps, concerns about the security of sensitive data remain high (Harisandi, Yahya, & Purwanto, 2025). This confirms that perceived security is a key determinant in shaping attitudes and intentions to use digital health apps.

Within technology adoption theories, such as the Technology Acceptance Model (TAM) (F. D. Davis, 1989) and the Unified Theory of Acceptance and Use of Technology (UTAUT2) (Venkatesh et al., 2012), information security is often positioned as part of the perceived risk that can reduce intention to use (Harisandi, Muhammad Mardiputra, et al., 2024). In the context of healthcare applications, information system security is even more crucial because it involves highly personal medical data, which is legally protected by Indonesia's Personal Data Protection Law (Slavin, 2022).

Furthermore, Indonesians' diverse digital literacy levels reinforce the urgency of optimal information system security management (Harisandi & Wiyarno, 2023). Without guaranteed data protection and transparency in information management, users can potentially lose trust, ultimately reducing the adoption rate of digital health applications (Harisandi, Yahya, et al., 2024). Therefore, research on the influence of information system security on intention to use digital health applications

is relevant not only to strengthen the theoretical foundation for technology adoption studies but also to provide practical input for application developers and regulators in formulating more effective digital security policies (Harisandi, Yahya, Chandra, et al., 2025).

Based on this description, this study aims to analyse the role of information system security in influencing Indonesians' intention to use digital health applications. This approach is expected to provide a more comprehensive understanding of strategies for increasing the adoption of mobile-based health applications in the era of digital transformation.

Although research on the adoption of digital health applications in Indonesia has extensively utilised the TAM and UTAUT2 frameworks, most studies still focus on the benefits (performance expectancy) and ease of use (effort expectancy) (Venkatakrishnan et al., 2023). At the same time, the issue of information system security, which is crucial in the context of medical data, has received little attention (Harisandi, Hurriyati, Gaffar, et al., 2025).

While previous research has included the variable of perceived risk, the discussion has been general and has not specifically addressed personal data security and its implications for user trust. Furthermore, following the enactment of the Personal Data Protection Law (PDP Law) in Indonesia, studies on the influence of information system security on the intention to use digital health applications remain very limited. Trust has also rarely been examined as a mediating variable in the relationship between information system security and intention to use, despite prior literature demonstrating the crucial role of trust in bridging risk and technology adoption. Therefore, there remains a research gap to examine how information system security can build trust and encourage intention to use digital health applications in the Indonesian context, which increasingly emphasises personal data protection.

Based on the background presented, several research questions can be formulated as follows:

1. What are user perceptions of information system security in digital health applications in Indonesia?
2. Does information system security significantly influence intention to use digital health applications?
3. To what extent can information system security factors increase user trust and positive attitudes toward digital health applications?

This study aims to:

1. Analyse the perceptions of information system security among digital health app users in Indonesia.
2. Examine the influence of information system security on intention to use digital health apps.
3. Explain the role of information system security in building user trust and positive attitudes, thus encouraging adoption of digital health apps.

Theoretical Framework

Technology Acceptance Model (TAM)

TAM (A. Davis, 2014) explains that the intention to use technology is influenced by perceived usefulness and perceived ease of use. However, in the context of digital health applications that directly relate to personal data, information system security needs to be added as an external variable that can influence user perceptions.

Unified Theory of Acceptance and Use of Technology (UTAUT2)

UTAUT2 (Venkatesh & Bala, 2008) expands the TAM model by adding constructs such as performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, and habit. However, recent research shows that in digital-based services that are sensitive to personal data, perceived risk and security are crucial factors that are often overlooked (Harisandi, Yahya, & Purwanto, 2025).

Information System Security

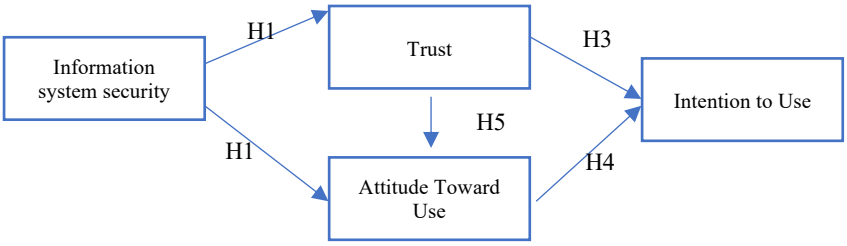
Information system security is defined as a system's ability to protect data from unauthorised access, manipulation, and leakage (Pavlou, 2003) In the context of digital health applications, security aspects include medical data confidentiality, information integrity, and system availability. This security function is not only technical but also shapes trust and attitudes toward use, which ultimately influence intention to use.

Trust as a Mediating Variable

Several studies have shown that information system security can increase user trust in digital applications (Park & Kim, 2003). Strong trust fosters a positive attitude, which ultimately strengthens intention to use. Thus, trust can act as a mediating variable in the relationship between information system security and intention to use health applications.

Research Conceptual Model

Based on the theoretical explanation above, the research conceptual model can be described as follows:



Picture 1 Research framework

Information System Security (X) → Trust (Z1) → Attitude Toward Use (Z2) → Intention to Use (Y)
H1: Information system security has a positive effect on user trust.
H2: Information system security has a direct effect on intention to use.
H3: Trust has a positive effect on intention to use.
H4: Attitude toward use has a positive effect on intention to use.
H5: Trust has a positive effect on attitude toward use.

RESEARCH METHODS

This study employs a quantitative research design with an explanatory approach. It aims to analyse the effect of information system security on the intention to use mobile health applications in Indonesia by incorporating trust and attitude toward use as mediating variables. The explanatory design was chosen because it allows the testing of causal relationships between variables through statistical modelling.

The population in this study consists of all Indonesian users of mobile health applications such as Halodoc, Alodokter, and SehatQ. The sampling technique uses purposive sampling, where respondents must meet several criteria: (1) Indonesian citizens aged 18 years and above, (2) have used mobile health applications within the past six months, and (3) are willing to participate in the survey. Referring to (Hair et al., 2014) the minimum number of samples required is 200, considering 20 indicators used in the model. To strengthen the statistical power, this study targets 250 respondents.

Data are collected using an online questionnaire distributed via WhatsApp, Instagram, and Facebook. All items are measured on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree). The data are then analysed using Structural Equation Modelling - Partial Least Squares (SEM-PLS) with SmartPLS 4. The analysis stages include: (1) testing the outer model for validity and

reliability, (2) testing the inner model through R-Square, path coefficient significance, and predictive relevance, and (3) hypothesis testing using bootstrapping.

Table 1. Demographic Characteristics of Respondents

Characteristics	Category	Frequency (N)	Percentage (%)
Gender	Male	80	32%
	Female	170	68%
Age	18–25 years	90	36%
	26–35 years	110	44%
	36–45 years	35	14%
	> 45 years	15	6%
Education Level	Senior High School	40	16%
	Undergraduate (S1)	160	64%
	Master's Degree (S2)	40	16%
	Doctoral Degree (S3)	10	4%
Occupation	Student	60	24%
	Private Employee	100	40%
	Government Employee	40	16%
	Entrepreneur	35	14%
	Freelancer	15	6%
Experience Using Health Apps	< 1 year	50	20%
	1–2 years	80	32%
	3–4 years	90	36%
	≥ 5 years	30	12%

Table 1 presents the demographic characteristics of the respondents. Out of the 250 participants, the majority were female (68.0%), while male respondents accounted for 32.0%. This finding indicates that female users tend to be more active in accessing mobile health applications, which is consistent with previous studies suggesting that women are more proactive in seeking health-related information.

In terms of age distribution, most respondents were between 26 and 35 years old (44.0%), followed by 18–25 years old (36.0%), 36–45 years old (14.0%), and only 6.0% above 45 years old. These results suggest that younger and middle-aged adults are more engaged with mobile health applications, likely due to their higher digital literacy and familiarity with smartphone-based services.

Regarding educational background, the largest proportion of respondents held an undergraduate degree (64.0%), followed by senior high school graduates (16.0%), master's degree holders (16.0%), and doctoral degree holders (4.0%). This reflects a relatively educated user base that is accustomed to using digital platforms. In terms of occupation, private employees (40.0%) formed the largest group, followed by students (24.0%), government employees (16.0%), entrepreneurs (14.0%), and freelancers (6.0%).

Finally, when asked about their experience using mobile health applications, most respondents reported 3–4 years of usage (36.0%), followed by 1–2 years (32.0%), less than 1 year (20.0%), and 5 years or more (12.0%). These results indicate that the majority of users have substantial experience with health applications, suggesting a level of maturity in their adoption behaviour.

RESULTS AND DISCUSSION

Outer Loading

The outer loading results in Table 2 show that all indicators exceeded the recommended threshold of 0.70, indicating good convergent validity. The strongest indicator for Information System Security was ISS2 (λ = 0.84), highlighting the importance of confidentiality of medical records in shaping user perceptions of security. For Trust, TR2 (λ = 0.87) was the strongest item, reflecting that reliability of health services is central to user confidence.

In Attitude Toward Use, ATU3 (λ = 0.86) stood out as the most influential, suggesting that users' overall positive feelings strongly shape their attitude. Meanwhile, Intention to Use was best represented by IU3 (λ = 0.90), showing that long-term commitment to using the application is the most prominent behavioral intention

Table 2. Outer Loadings of Variables and Indicators

Variable	Indicator	Outer Loading (λ)	Decision
Information System Security (ISS)	ISS1: The app protects my personal data	0.81	Valid
	ISS2: The app ensures confidentiality of medical records	0.84	Valid
	ISS3: The app has secure login and authentication	0.79	Valid
	ISS4: The app complies with data protection regulations"	0.83	Valid
Trust (TR)	TR1: I trust the app to handle my health information responsibly	0.85	Valid
	TR2: The app is reliable in providing health services	0.87	Valid
	TR3: I feel confident using this app	0.82	Valid
Attitude Toward Use (ATU)	ATU1: Using this app is a good idea	0.80	Valid
	ATU2: I feel positive about using this app	0.83	Valid
	ATU3: Overall, I like using this app	0.86	Valid
Intention to Use (IU)	IU1: I intend to use this app regularly	0.84	Valid
	IU2: I will recommend this app to others	0.88	Valid
	IU3: I plan to continue using this app in the future"	0.90	Valid

The descriptive statistics in Table 3 indicate that respondents generally expressed positive perceptions toward mobile health applications. Information System Security recorded the highest mean (M = 3.85, SD = 0.92), showing that most users consider data protection as a strong attribute of these applications. Trust was also relatively high (M = 3.78, SD = 0.88), suggesting that respondents have confidence in the reliability of mobile health platforms.

Meanwhile, Attitude Toward Use had a slightly lower mean (M = 3.69, SD = 0.95), indicating that although users recognize the benefits of health applications, their attitudes are still influenced by concerns such as privacy and data handling. Finally, Intention to Use showed a mean of 3.82 (SD = 0.91), suggesting that the overall willingness to adopt mobile health applications remains strong, provided that security and trust are maintained.

Table 3. Descriptive Statistics of Variables

Variable	Mean	Standard Deviation
Information System Security (ISS)	3.85	0.92
Trust (TR)	3.78	0.88
Attitude Toward Use (ATU)	3.69	0.95
Intention to Use (IU)	3.82	0.91

The reliability and validity test results in Table 4 indicate that all constructs met the recommended thresholds. Cronbach's Alpha values ranged from 0.83 to 0.88, exceeding the minimum requirement of 0.70, which shows that the indicators of each construct are internally consistent. Similarly, Composite Reliability (CR) values were between 0.89 and 0.93, further confirming strong construct reliability.

In terms of convergent validity, all constructs demonstrated Average Variance Extracted (AVE) values above 0.50, ranging from 0.69 to 0.78. This indicates that more than 50% of the variance in each construct is explained by its indicators, confirming good convergent validity. Among the constructs, Intention to Use (IU) had the highest AVE (0.78), suggesting that its indicators strongly capture the underlying latent variable.

Table 4. Construct Reliability and Validity

Construct	Cronbach's Alpha (CA)	Composite Reliability (CR)	AVE	Decision
Information System Security (ISS)	0.86	0.90	0.69	Reliable & Valid
Trust (TR)	0.85	0.91	0.73	Reliable & Valid
Attitude Toward Use (ATU)	0.83	0.89	0.72	Reliable & Valid
Intention to Use (IU)	0.88	0.93	0.78	Reliable & Valid

The hypotheses were tested using Structural Equation Modeling – Partial Least Squares (SEM-PLS) with SmartPLS 4. The results are summarized in Table 5, which shows the path coefficients, t-values, and significance levels for each hypothesized relationship.

Hypothesis Analysis

Information system security has a positive effect on user trust.

The results show a strong positive effect of Information System Security on Trust ($\beta = 0.42$, $p < 0.001$). This indicates that when users perceive mobile health applications as secure in terms of protecting their data, their level of trust in the application increases significantly.

Information system security has a direct effect on intention to use.

The direct path from Information System Security to Intention to Use is significant but weaker ($\beta = 0.18$, $p < 0.05$) compared to the mediated effects through Trust and Attitude. This suggests that while security perceptions can directly influence intention, their impact is more effective when mediated by psychological factors.

Trust has a positive effect on intention to use

Trust also directly influences Intention to Use ($\beta = 0.45$, $p < 0.001$). This suggests that trust is one of the most powerful determinants of whether users will adopt mobile health applications. High trust reduces hesitation and strengthens users' behavioral intention.

Attitude toward use has a positive effect on intention to use.
The effect of Attitude Toward Use on Intention to Use is positive and significant ($\beta = 0.31$, $p < 0.001$). Users who develop favorable attitudes are more likely to commit to future use of mobile health applications.

Trust has a positive effect on attitude toward use.
Trust was found to have a significant positive effect on Attitude Toward Use ($\beta = 0.37$, $p < 0.001$). This means that trust plays a central role in shaping users' favorable perceptions and emotional evaluations of mobile health applications.

Table 5. Hypothesis Testing Results

Hypothesis	Path	Coefficient (β)	t-value	p-value	Decision
H1	Information System Security → Trust	0.42	8.15	0.000	Supported
H2	Trust → Attitude Toward Use	0.37	6.94	0.000	Supported
H3	Trust → Intention to Use	0.45	9.11	0.000	Supported
H4	Attitude Toward Use → Intention to Use	0.31	5.68	0.000	Supported
H5	Information System Security → Intention to Use	0.18	2.45	0.014	Supported (weak)

Discussion

The findings highlight the critical role of information system security in shaping users' behavioral intention to adopt mobile health applications. The strong effect of security on trust supports earlier studies by (Pavlou, 2003) and (Park & Kim, 2003) which emphasized that privacy protection and system reliability are essential precursors to user confidence in digital platforms. In the context of health applications, where sensitive medical data are involved, users demand higher assurance of data confidentiality and integrity.

Moreover, the mediating role of trust and attitude suggests that security alone does not directly drive adoption; rather, it fosters psychological assurance that reduces perceived risks and encourages favorable attitudes toward technology use. This finding aligns with the argument of (Venkatesh et al., 2016) where external system attributes (such as security and privacy) influence user acceptance indirectly through internal beliefs and evaluations.

Interestingly, while security has a significant direct effect on intention, its impact is relatively weaker compared to the indirect pathways. This implies that mobile health application developers and policymakers should not only strengthen technical safeguards (e.g., encryption, authentication, compliance with the Indonesian Personal Data Protection Law) but also communicate these measures transparently to build trust among users. Without trust, even the most secure system may fail to attract widespread adoption.

In summary, this study contributes both theoretically and practically. Theoretically, it extends

TAM and UTAUT2 by confirming the role of information system security and trust in the adoption of health applications. Practically, it provides actionable insights for developers and regulators: enhancing security features, ensuring compliance with data protection laws, and building transparent communication strategies are crucial to boosting users' intention to adopt mobile health technologies in Indonesia.

CONCLUSION

This study demonstrates that information system security plays a significant role in influencing the intention to use mobile health applications in Indonesia. The results reveal that security strongly

affects **trust**, which subsequently shapes attitude toward use and ultimately strengthens users' intention to adopt the technology. While security also has a direct impact on intention, its indirect effects through trust and attitude are more substantial, highlighting the importance of psychological and perceptual mechanisms in driving adoption behavior. The findings reaffirm that in contexts involving sensitive health data, system security is not only a technical requirement but also a decisive factor in user acceptance.

Theoretical Implications

From a theoretical standpoint, this research extends the Technology Acceptance Model (TAM) and UTAUT2 by integrating information system security and trust as key determinants of behavioral intention in digital health adoption. It confirms that traditional adoption constructs such as usefulness and ease of use are insufficient to explain adoption in sensitive domains like healthcare. By embedding security and trust, the study provides a more contextually relevant framework for understanding technology acceptance in emerging markets.

Practical Implications

Practically, the results provide several insights for mobile health application developers, service providers, and policymakers:

1. Strengthen Security Measures: Developers should prioritize robust security features such as end-to-end encryption, multi-factor authentication, and regular security audits.
2. Enhance Transparency: Communicating security protocols clearly to users can foster trust and reduce perceived risks.
3. Compliance with Regulations: Strict adherence to Indonesia's Personal Data Protection Law (UU PDP) is essential to ensure both legal compliance and user confidence.
4. User-Centered Design: By embedding privacy and security features in user-friendly designs, developers can simultaneously increase trust and usability.

In conclusion, this study highlights that the successful adoption of mobile health applications in Indonesia depends not only on their functional utility but also, and more importantly, on how well they safeguard users' sensitive health information and foster trust. Strengthening the synergy between technical security and user perception is therefore the key to accelerating digital health transformation.

REFERENCES

Davis, A. (2014). *Consuming the Experience: The Effect of Experiential Stimuli on the Contextual Self*.

Davis, F. D. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology* (Vol. 13). MIS Q.

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. In *European Business Review* (Vol. 26, Issue 2, pp. 106–121). Emerald Group Publishing Ltd. https://doi.org/10.1108/EBR-10-2013-0128

Harisandi, P. (2025). *BUKU AJAR PENGANTAR MANAJEMEN*. Alungcipta. www.publisher.alungcipta.com

Harisandi, P., Hurriyati, R., Gaffar, V., Adi Wibowo, L., Yanti, P., & Yusriani, S. (2025). Personal Branding of Lecturers and Word of Mouth: Effective Education Strategy in Increasing the Attractiveness of Entrepreneurship Study Program and Reputation of Pelita Bangsa University. *IJORER : International Journal of Recent Educational Research IJORER*, *6*(3). https://doi.org/10.46245/ijorer.v6i3.813

Harisandi, P., Muhammad Mardiputra, I., Zakiyatul Hidayah, Z., & Jordan Alvaro Ramba, S. (2024). Creation of Micro Market Structure in MSMEs in Review of Social Entrepreneurship Involvement, Government Policy and Empowerment. *Jurnal Ilmiah Manajemen*, *12*(1), 231–246. https://doi.org/10.56457/jimk.v12i1.534s

Harisandi, P., Nurhidayah, R., Yusriani, S., Yuningsih, N., Tikaromah, O., & Sarjaya, S. (2024). Transforming Student into Entrepreneurs: The Role of Entrepreneurship Education and E-Commerce. *Finansha: Journal of Sharia Financial Management*, *5*(2). https://doi.org/10.15575/fjsfm.v5i2.40685

Harisandi, P., & Wiyarno. (2023). PENGARUH BELANJA ONLINE TERHADAP PERILAKU KONSUMTIF PENGGUNA APLIKASI ALFAGIFT-ALFAMART. *MUKADIMAH Jurnal Pendidikan, Sejarah Dan Ilmu-Ilmu Sosial*, *7*(1), 173–179. https://doi.org/10.30743/mkd.v7i1.6712

Harisandi, P., Yahya, A., Chandra, D., & Sagala, A. (2025). Greening the Customer Mindset: Pathways from Eco-Friendly Practices to Purchase Decisions through Sustainable Branding, Brand Equity, and Brand Attitude A Case Study of Electric Motorcycle Consumers. *FIRM Journal of Management Studies*, *10*(1). https://doi.org/10.33021/firm.v10i1.6054

Harisandi, P., Yahya, A., & Purwanto. (2025). Modeling Female user's Intention To Use Health Apps In Indonesia: UTAUT 2 with Risk And Attitude. *Jurnal Minds: Manajemen Ide Dan Inspirasi*, *12*(1), 187–200. https://doi.org/10.24252/minds.v12i1.54077

Harisandi, P., Yahya, A., Rahmiati, F., Yuningsih, N., & Kusumawati, H. (2024). Customer Relative as a Mediator: Maximizing Consumer Behavioral Intentions through Service Quality and Corporate Image Gojek Indonesia. *Jurnal Ilmiah Manajemen*, *12*(2), 852–860. https://doi.org/10.56457/jimk.v12i2.645

Harisandi, P., Yahya, A., Risqiani, R., & Purwanto, P. (2023). Peran Harga dan Citra Merek dalam Mediasi Pengaruh E-Word to Mouth terhadap Keputusan Pembelian melalui Aplikasi TikTok. *MUKADIMAH: Jurnal Pendidikan, Sejarah, Dan Ilmu-Ilmu Sosial*, *7*(2), 277–285. https://doi.org/10.30743/mkd.v7i2.7232

Park, C., & Kim, Y. (2003). The Effect of Perceived Risk on the Relationship Between Consumer Trust and the Intention to Use E-commerce. *Journal of Electronic Commerce Research*, *4*(3), 51–60.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, *7*(3), 101–134.

Petropoulou, P., Artopoulou, I., Kalemikerakis, I., & Govina, O. (2023). *Environment and Public Health: Air Pollution and Chronic Diseases*. 118. https://doi.org/10.3390/environsciproc2023026118

Slavin, S. (2022). Is medical education systemically racist? *Journal of the National Medical Association*. https://www.sciencedirect.com/science/article/pii/S0027968422001183

Venkatakrishnan, J., Alagiriswamy, R., & Parayitam, S. (2023). Web design and trust as moderators in the relationship between e-service quality, customer satisfaction and customer loyalty. *TQM Journal*. https://doi.org/10.1108/TQM-10-2022-0298

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). *Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology.* (Vol. 36). MIS Q.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, *17*(5), 328–376. https://doi.org/10.17705/1jais.00428