Asia Pacific Science Press

Asia Pacific Economic and Management Review
ISSN(O):3005-9275
ISSN(P):3005-9267
Vol. 3 No.1 (2026)

Unveiling Willingness to Adopt Online Privacy Control Measures in Tanzanian Higher Learning Institutions: A Gender-Based Multi-group Analysis Approach

Daniel Koloseni[1], Herman Mandari[2]*

1.Department of Information Technology, Institute of Finance Management, Dar es Salaam, Tanzania

2.Department of Computer Science, Institute of Finance Management, Dar es Salaam, Tanzania

Corresponding author: Herman Mandari, mandariherman@gmail.com

Abstract: The internet is among the primary learning resources, attracting students to use it for educational and social purposes. Observing privacy when using the internet is essential, especially for students in HLIs, given the privacy and security threats. This research examines the adoption of privacy control measures among students in HLIs. The study employed Structural Equation Modeling (SEM) to identify factors influencing willingness to adopt privacy control measures and to examine gender differences in this regard. Data were collected from 11 HLIs in Tanzania, comprising 390 males and 286 females. The findings for the full sample revealed that risk perceptions, privacy concerns, and perceived trust positively influence students' willingness to adopt privacy control measures. Furthermore, social influence and perceived security awareness positively influenced perceived trust. Additionally, the study found that convenience negatively affects users' willingness to adopt privacy control measures and that perceived risk negatively affects users' trust in the internet. However, neither social influence nor perceived security awareness affects willingness to adopt privacy control measures. The study also found a significant difference in perceived security awareness between genders regarding willingness to adopt privacy control measures. The study ultimately offers implications for researchers, practitioners, and managers seeking to promote the adoption of privacy control measures among students.

Keywords: Privacy; Control Measures; Gender; Tanzania; Multi-Group Analysis

Published: Jan 15, 2026

DOI: https://doi.org/10.62177/apemr.v3i1.1006

1.Background

Cases of privacy evasion have increased worldwide, causing chaos in society. The increase has been primarily attributed to the growth of internet use and the proliferation of social media. These technological advancements have created additional privacy challenges beyond the existing landscape (Bélanger & Xu, 2015). On the other hand, users have not been adequately informed about privacy risks and how to protect themselves against them. The built privacy enforcement strategies in internet applications are optional for users to activate. Therefore, users who are not well-informed are likely to jeopardise their privacy because they are unaware of how to activate privacy settings. While system owners are responsible for protecting users' privacy, users should also learn how to control the circulation of information about themselves (Berkman, 1971; Senarath & Arachchilage, 2018; Tahaei & Vaniea, 2021).

Most internet applications require users to register, and in the process, they are asked to grant the system access to some personal information. Driven by the need and sometimes the urgency to access services, users comply with access requests. Ultimately, users disclose a significant amount of information, jeopardising their privacy. Despite efforts to ensure that information systems comply with privacy laws, users should also take precautions to safeguard their privacy. Privacy concerns have received much attention in the information security literature, with most previous studies focusing on addressing privacy issues using the privacy calculus theory (Fernandes & Costa, 2023; Jabbar et al., 2023a; Meier & Krämer, 2024). However, some areas remain unaddressed. First, individual characteristics have received little attention, with only a few studies addressing this topic, such as Sun et al (2025). However, gender is the most influential individual aspect in technology adoption (Sun et al., 2015); thus, investigating it is worthwhile. Moreover, previous studies have confirmed that individual factors, such as gender, play a significant role in technology adoption (Alesanco-Llorente et al., 2023; Chen et al., 2023; Park et al., 2019; Venkatesh et al., 2000). Similarly, privacy calculus differs among genders (Sun et al., 2015). Previous studies argue that females are vulnerable to privacy concerns compared to males because they are inferior, safer targets, and are being held more accountable for their private conduct (Allen, 1999). Additionally, females are more likely than males to express privacy concerns on social networks (Tifferet, 2019). Further, while previous studies, such as (Baruh et al., 2017; Ho et al., 2015; Jabbar et al., 2023b; Koloseni & Sedoyeka, 2019; Xu et al., 2013), focused on adopting security or privacy controls in a general population, the current research delves into understanding whether adopting online privacy control measures differs among females and males in HLIs.

Second, previous studies using the privacy calculus theory have focused little on perceived trust effects. Nevertheless, when conducting the cost-benefit analysis, users may also consider their trust in the internet. Perceived trust is a crucial consideration for internet users when deciding whether to use an online resource or consent to a system accessing private information (Jang, 2024). Because it is linked to the system's security, reliability, availability, and ability (Fortino et al., 2020). Moreover, deploying privacy measures may require privacy self-efficacy (i.e., skills, knowledge, and confidence to protect privacy) and is time-consuming (Kang, 2023). Therefore, the internet user may perceive it as inconvenient. For the purposes of this study, individuals may weigh the benefits of using the internet for learning against the privacy risks and concerns, and decide whether to apply privacy control measures.

Against this backdrop, the current study employs an extended privacy calculus theory to investigate the adoption of privacy control measures while online among HLI students. The privacy calculus has been widely used to study privacy disclosure behaviours (Akter et al., 2025; Ashrafi et al., 2024; Dinev et al., 2006; Lu, 2024). Specifically, the study advances the privacy calculus theory by integrating it with users' perceived trust, social influence, and perceived convenience in predicting willingness to adopt privacy control measures. Additionally, it analyses the gender differences in individual willingness to adopt privacy-protective measures when using the internet.

2.Literature Review

The advent and proliferation of social media, artificial intelligence (AI), the Internet of Things (IoT), mobile applications, and mobile devices have increased the volume of information generated and shared among applications, users, and the public. From the perspective of system developers and business strategists, the massive amount of data generated has accelerated the need to package the information in a way that enables it to power business processes in a sophisticated manner. As a result, there is a growing concern among internet users about the potential for their private information to be collected and used without their consent (Esmaeilzadeh, 2020). However, to comply with privacy laws and regulations, systems seek permission or consent to collect users' information (Tahaei et al., 2023). Since privacy control is about notice and choice (Feng et al., 2021), users may consent to disclose or not disclose the information the system requests (Elbitar et al., 2021; Wijesekera et al., 2018). Additionally, based on the risks or benefits gained, users may disregard privacy warnings or bypass privacy control measures to optimise the convenience or benefits of using the internet without restrictions. Studies on users' privacy behaviour have used the privacy calculus theory.

The privacy calculus theory assumes that individuals disclose private information after weighing the costs against the benefits (Schomakers et al., 2022). The benefits include social capital, system utility, convenience, and ease of use (Hsuan-ting Chen, 2018; Hauff & Nilsson, 2023), while the costs may include risks associated with the misuse of personal information. The outcome of the user's decision may lead to either the preservation or disclosure of personal information. The theory has been widely applied in research on privacy disclosure behaviours and, therefore, aligns well with the current study's agenda.

3.Proposed Model and Hypotheses Development

Perceived risk is widely linked to information systems (IS) usage behaviours, such as security protection efforts (Nguyen & Kim, 2017), information security awareness (McCormac et al., 2017), and information security compliance (Ferrante & Ajani, 2024). In a situation where an individual believes the internet is risky, the intention to use protective measures increases to safeguard their privacy.

As theorised in the Technology Threat Avoidance Theory (TTAT) and the Protection Motivation Theory (PMT), individuals are inclined to use protective measures if they believe there is a higher risk of threats (Liang & Xue, 2010; Rogers, 1975). Therefore, in the context of the current study, it is expected that individuals whose perception of risk is high are likely to adopt privacy control measures, such as, set privacy control features, use encryption, and apply a two-factor authentication approach when using the internet, thus positively influencing the adoption of privacy control measures. Moreover, they will likely perceive the internet as untrustworthy (Almaiah et al., 2023). Hence, the hypothesis;

H1: Individual perceived risk negatively influences the users’ perceived trust in the internet.

H2: Individual perceived risk has a positive influence on the adoption of privacy control measures when using the internet.

Perceived security awareness refers to users’ awareness of online security threats and their potential consequences (Haeussinger & Kranz, 2013). It plays a vital role in positioning users to combat online security threats. Previous studies indicate that security-aware users will likely comply with acceptable protective behaviours and security technologies (Dinev & Hu, 2007; Koloseni & Sedoyeka, 2019), such as avoiding security threats like phishing attacks and using antivirus software. The linkage between security awareness and users’ intentions to adopt security measures, such as using strong passwords, reviewing privacy settings, using a VPN, and encryption, has been well-documented in the IS literature (Koloseni & Sedoyeka, 2019; Ngoqo & Flowerday, 2015; van der Schyff & Flowerday, 2021). Additionally, security awareness educates users about the risks associated with the internet. As users become security-aware and competent in navigating internet security risks, their trust in the internet increases. Based on the discussion above, the study proposes that:

H3: Perceived security awareness positively influences the users’ perceived trust in the internet.

H4: Perceived security awareness positively influences users’ intention to adopt privacy control measures.

Privacy concerns refer to users’ worries about how unauthorised entities collect, store, and use personal information (ElShahed, 2023). When using the internet, a significant amount of information may be collected, with or without the user’s consent, including personally identifiable information, user behaviour, and site visits. The illegal collection of this information may infringe on user privacy. Therefore, these privacy concerns may encourage users to employ privacy control measures. As observed in past studies, privacy concerns have a positive impact on the intention to use security measures (Chen & Chen, 2015). Additionally, it may decrease trust in the safety of the internet. Thus, the current study postulates that:

H5: Privacy concerns negatively influence the perceived trust in privacy control measures.

H6: Privacy concerns have a positive influence on users’ intention to adopt privacy control measures.

Convenience is the minimum effort and time required to access the service (Benoit et al., 2017). In the context of this study, convenience refers to how easily and effectively an individual access the internet without being hampered by privacy and security controls. The system’s or internet’s built-in privacy and security controls may discourage users from applying these controls due to the difficulty or ease with which they have been deployed (Reeves et al., 2021). These controls may lead to privacy fatigue, which can prevent internet usage (Cheng et al., 2024). Therefore, users may opt for convenience over privacy control measures, a decision that may lead to disclosure. Consequently, it is reasonable to hypothesise that:

H7: The Convenience negatively influences the willingness to adopt privacy control measures.

Perceived trust entails confidence in individuals’ integrity and reliability (Mutimukwe et al., 2022). The perception of integrity and reliability of the third party increases individuals’ urge to engage in or use the services. For instance, as the trust in integrity and reliability (i.e., perceived trust) increases, the intention to use the Internet of Things (IoT), the intention to continue purchasing online, and payment systems also increases (Gong et al., 2023; Jaspers & Pearson, 2022; Tan et al., 2025). Users trust the privacy and security mechanisms deployed to safeguard their transactions, despite the associated privacy, security, and financial risks. Therefore, it is reasonable to postulate that:

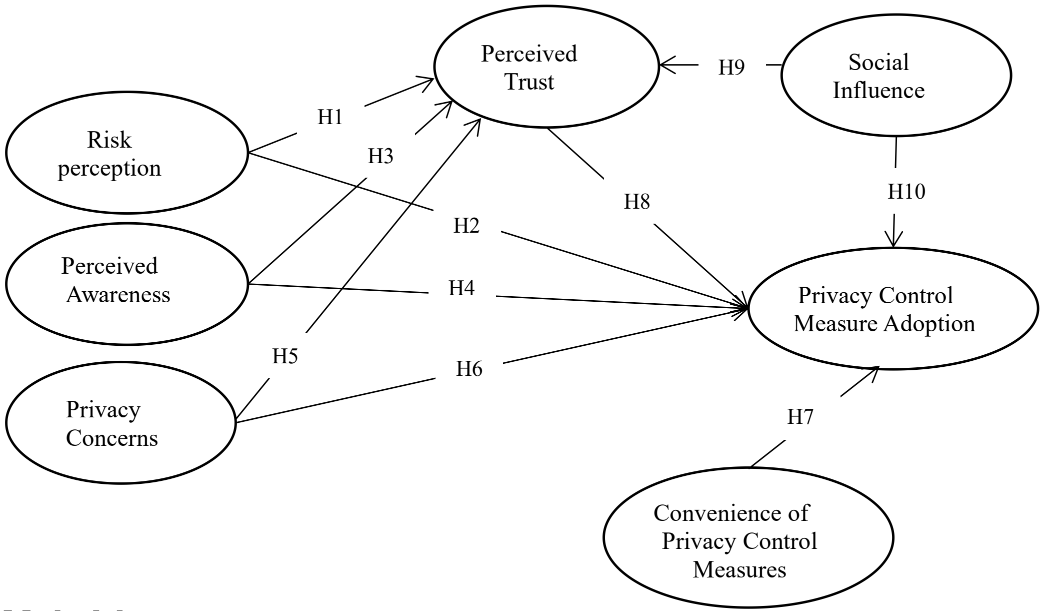
H8: Perceived trust positively influences the intention to adopt privacy control measures.

The pressure exerted by peers, friends, mentors, etc, may play a key role in shaping individual behaviours. Social influence has been documented to impact numerous behaviours in many fields, including health, education, ICT, finance, human resources, etc. Accordingly, the impact of social influence is also manifested in information security-related behaviours. For instance, previous studies have confirmed that it influences authorised access to data in healthcare (Vrhovec et al., 2024), general security behaviour (Berthevas, 2021), security policy compliance (Ifinedo, 2014), and the use of password managers (Tian, 2025), among other studies. Additionally, previous findings suggest a connection between social influence and perceived trust (X. Tian, 2025). In the current study context, peers, friends, etc, may influence each other to trust and adopt privacy control measures. Therefore, the hypothesis:

H9: Social influence has a positive impact on the perceived trust in privacy control measures.

H10: Social influence positively impacts the adoption of privacy control measures.

Figure 1: Theoretical Framework



4.Methodology

The study used a quantitative approach to identify the predictors of willingness to adopt privacy control measures while using the internet. To ensure the reliability and validity of the research instrument, the questionnaires for data collection were developed using measurement items from previous studies. Specifically, risk perception (RP) was adapted from Koloseni and Sedoyeka (2019); perceived security awareness (PA) was adapted from Koloseni et al (2018) and Mahabi (2010); privacy concerns (PC) were adapted from Buchanan et al (2007) and Mwesiumo et al (2021); perceived trust (PT) was adapted from Kim et al. (2011) and Wu et al. (2011); social influence (SI) was adapted from Zhang et al (2020); the convenience of privacy control measures (CON) was adapted from Chang et al (2012); and willingness to adopt privacy control measures (ADP) was adapted from Dinev and Hu (2007) and Safa et al (2016). To enhance the validity of the instrument, four academics contacted via email were requested to assess face and content validity of the research questionnaire, ensuring that terminologies were used correctly, texts were relevant, sentences were proper, and items aligned with the variables (Bhatnagar & Rajesh, 2024; Memon et al., 2023). Based on their recommendations, the questionnaire items were refined for better logical flow and clarity. The developed questionnaire was pre-tested on 30 students to identify misunderstandings and ambiguities (Perneger et al., 2015). A few sentences were amended based on the results of this evaluation. Furthermore, the questionnaire was piloted to test the reliability of the measurement items for assessing the unmeasurable variables. Using 40 respondents (Bhatnagar &

Rajesh, 2024), the results indicated that two items had loading values below 0.7 (Alford & Teater, 2025), which is below the threshold; consequently, they were removed one by one.

The participants for the main survey were selected from eleven (11) public and private HLIs in Tanzania, including undergraduate and postgraduate students. They were selected using a convenience sampling technique, a non-probability sampling method, due to the nature of HLI activities, which are guided by schedules. Hence, the data collection process followed the convenience of the respondents participating in the study. Research assistants visited the selected HLI's library entry and distributed the questionnaire face-to-face. They then requested that the respondents fill it out and return it to the collection point, where research assistants were stationed. A total of 1100 questionnaires were distributed within the first month. The data collection process took four (4) months, from December 2024 to March 2025. The sample description of the respondents is reported in Table 1. Out of 1100 distributed questionnaires, 711 were returned, denoting a 64.6% response rate. However, after careful screening, which included removing responses with large missing values and those with suspicious patterns, only 676 questionnaires were deemed suitable for subsequent data analysis.

Table 1: Sample Description of the Respondents

Variable	Category	Frequency	Percentage
Gender	Male	390	57.7
	Female	286	42.3
Academic Level	Certificate	89	13.2
	Diploma	133	19.7
	Bachelor	383	56.7
	Postgraduate	71	10.5
Age	16-25	461	68.2
	26 -36	142	21.0
	Above 36	73	10.8

The sample size indicates that male respondents are 15.4% larger than female respondents; this difference accurately reflects the gender distribution of students in higher learning institutions in Tanzania. The academic level and age distribution also represent the student population in higher learning institutions. To determine whether the sample sizes of 390 and 286 for males and females, respectively, are sufficient to test the research model, G*Power statistical software was utilised (Benhissi & Hamouda, 2025). Findings from G*Power analysis indicate that a minimum sample size of 277 for the female group and 309 for the male group is required to achieve an effect size (f2) of 0.15 at a 0.05 significance level and 0.8 as statistical power. Therefore, the obtained sample sizes of 390 for females and 286 for males are adequate to produce sufficient statistical power for the study.

5.Non-response Bias

To generalise the findings from this study, the non-response bias was evaluated as suggested by Senior et al. (2002). Response bias tends to have an effect when the responses received are consistently different from those of people who were issued the questionnaire but did not respond (Bhatnagar & Rajesh, 2024). Wave analysis was adopted, and the received data were divided into two sets (early versus late respondents). The data obtained in the first month were categorised as early respondents, while the data received in the last month were classified as late respondents (Armstrong & Overton, 1977). The two datasets were further analysed to examine for non-response bias. The t-test analysis results show no statistically significant difference between early and late respondents (p = 0.74); these findings indicate that non-response bias is not a substantial issue in this study.

6.Common method variance

To address the potential effect of common method variance, which may be attributed to the use of a self-administered questionnaire, the following procedures were implemented to minimise the common method variance (CMV) effects. Firstly, respondents were asked to sign the consent form to participate in the study using the questionnaire. Secondly, they were assured of the confidentiality of the data collected and the anonymity of the respondents, and that the data collected would be safely stored and securely destroyed after the research. Additionally, the data collected will be used solely for the current study. Since the survey employed self-reported measures and applied a non-probability sampling technique (convenience sampling), there is a possibility of common method bias during data collection, despite the use of the control measures discussed above. Therefore, the study employed statistical techniques to assess the presence of common method bias. First, Harman's unrotated factor analytic technique was used. The result shows that the dominant factor produced variation below 50% which is the acceptable threshold (Rahi & Abd. Ghani, 2018). Second, the VIF produced by all constructs were below the threshold of 3.3 (Lim, 2024). All these tests produced the evidence that common method bias is not an issue in this study.

7.Data Analysis Results

7.1Measurement Model

The measurement model was evaluated using two quality criteria: reliability and validity. Reliability was assessed through composite reliability (CR), as recommended by Cheung et al. (2024). CR is regarded as a better measure of the reliability of latent constructs compared to Cronbach’s alpha (Cheung et al., 2024). The results in Table 2 indicate that the composite reliability values exceed 0.7, suggesting that the measurement items consistently assess the constructs of the study (Hair et al., 2013). Additionally, as shown in Table 2, the Average Variance Extracted (AVE) values are above 0.5, confirming the convergent validity of the models (Hair et al., 2019).

Table 2: Reliability and Convergent Validity Results for Male and Female Groups

Construct	CR	AVE
ADP	0.781	0.544
CON	0.880	0.710
PA	0.774	0.534
PC	0.845	0.645
PT	0.760	0.514
RP	0.757	0.610
SI	0.808	0.585

Regarding convergent validity, the HTMT coefficients reported in Table 3 are all within the acceptable range of higher than 0.90, as per Henseler et al. (2015). The findings indicate that the measurements truly capture the constructs of the study.

Table 3: HTMT Ratio Results of Female and Male Groups

Construct	ADP	CON	PA	PC	PT	RP	SI
ADP							
CON	0.430						
PA	0.341	0.844					
PC	0.352	0.343	0.364				
PT	0.390	0.731	0.758	0.289			
RP	0.513	0.881	0.857	0.449	0.784		
SI	0.406	0.833	0.849	0.442	0.779	0.839	

7.2 Structural Model

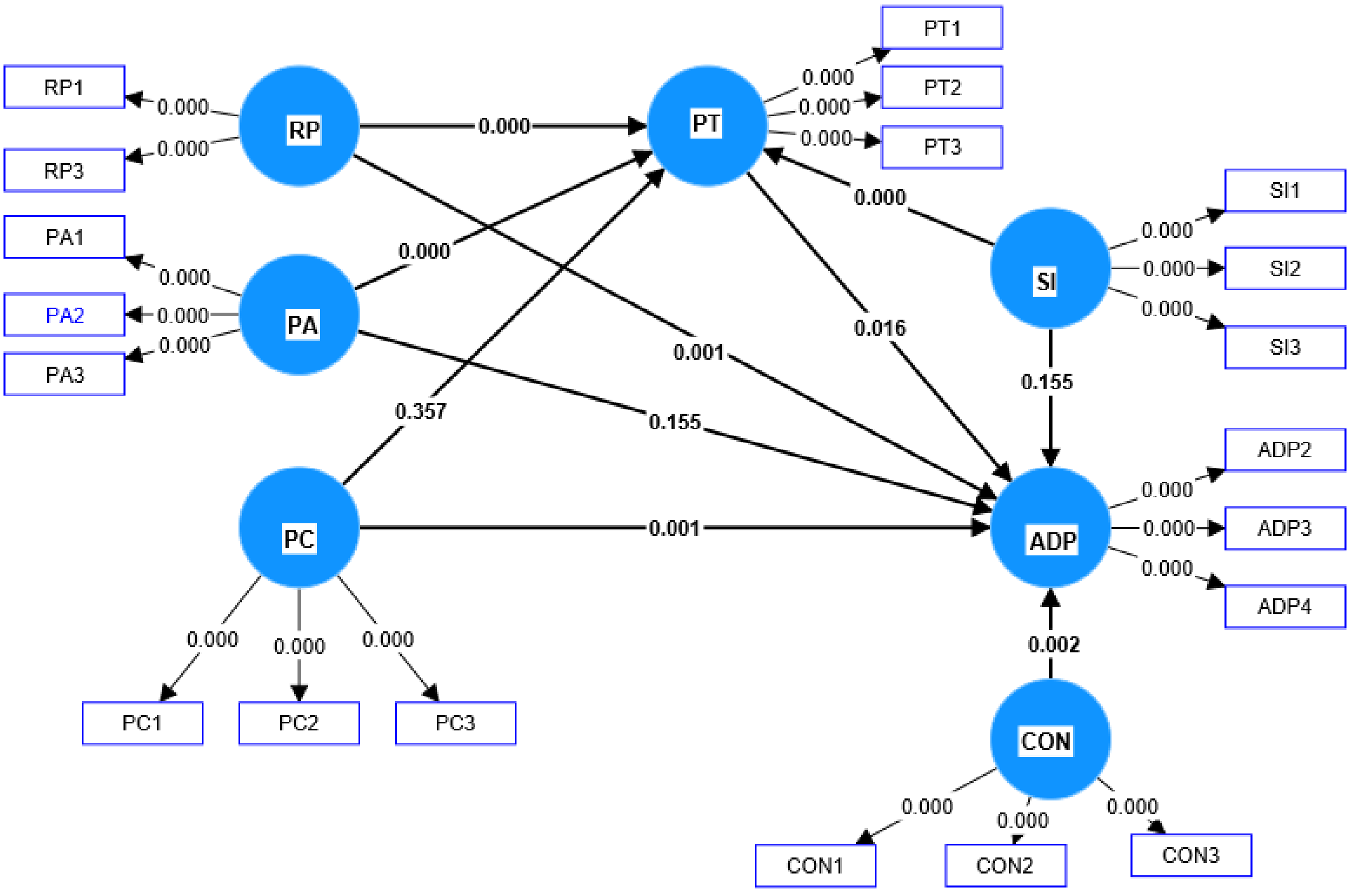
The structural model assessment evaluated the models’ explanatory power, predictive relevance, and ability to test hypotheses. The study found that the explanatory powers of the models are R^2 = 51.2, 34.6, and 46.7 for the complete sample model, the female group, and the male group, respectively. The findings suggest that all three models adequately explained the dependent variable (i.e., the adoption of privacy control measures). Moreover, the models’ predictive relevance (Q^2) is greater than zero, indicating that the models are relevant to predicting the study outcomes (Henseler et al., 2009).

Next, after assessing the models' explanatory power and predictive relevance and verifying the quality of the measurement model, the structural model was determined. The primary purpose of the structural model assessment is to determine whether there is a statistically significant relationship between the study's constructs. The current research assesses three sets of structural models. The first is the complete sample model, which assesses all hypotheses for both male and female groups regarding the adoption of privacy control measures. The second structural model evaluated the hypothetical relationships for the female group, and the third evaluated those for the male group regarding the adoption of privacy control measures. The results of all three structural models are indicated in Tables 4, 5, and 6. The study found that out of ten (10) hypotheses, seven (7) were supported across the samples (i.e., in each sub-group: complete sample, female, and male group).

Table 4: Results for the Complete Sample Structural Model

Paths/Hypotheses	Coefficients	t-statistics	p-values	Remarks
H1:RP -> PT	-0.040	5.237	0.000*	Supported
H2: RP -> ADP	0.052	3.082	0.001*	Supported
H3: PA -> PT	0.041	6.299	0.000*	Supported
H4: PA -> ADP	0.049	1.013	0.155	Not Supported
H5: PC -> PT	-0.033	0.366	0.357	Not Supported
H6: PC -> ADP	0.040	3.202	0.001*	Supported
H7: CON -> ADP	-0.147	2.847	0.002*	Supported
H8: PT -> ADP	0.045	2.145	0.016*	Supported
H9:SI->PT	0.046	6.592	0.000*	Supported
H10:SI -> ADP	0.055	1.017	0.155	Not Supported

Figure 2: Structural Model Results for the Complete Sample



As indicated in Tables 4, 5, 6, and Figure 2, the study found that the results for H1, H2, H3, H5, H6, H8, H9, and H10 for both female and male groups are consistent with those of the complete sample. Specifically, risk perception negatively affects users' trust in privacy control measures (H1) and their willingness to adopt privacy control measures (H2), and perceived security awareness positively affects users' perceived trust in the internet (H3). Furthermore, the effect of perceived security awareness on the willingness to adopt privacy control measures (H5) was no longer significant across all samples. The effects of privacy concerns (H6) and perceived trust (H8) on willingness to adopt privacy control measures were significant across all groups. Social influence had a positive and significant effect on perceived trust in privacy control measures (H9), whereas its effect on the willingness to adopt privacy control measures (H10) was insignificant.

Nevertheless, the H4 and H7 results were inconsistent across all three samples. For instance, while H4 was insignificant in the male group, it was significant in the female group and the complete sample. This means that the impact of perceived security awareness on the adoption of privacy control measures for male respondents is insignificant for the complete sample and the male group. Furthermore, the effect of user convenience on internet use is significant among male respondents and the complete sample (H7). Contrary to expectations, it is insignificant for the female respondents.

Table 5: Structural Model Results for the Female Group

Paths/Hypotheses	Coefficients	t-statistics	p- values	Remarks
H1:RP -> PT	-0.233	4.071	0.000*	Supported
H2: RP -> ADP	0.205	2.358	0.009*	Supported
H3: PA -> PT	0.244	3.915	0.000*	Supported
H4: PA -> ADP	0.035	2.154	0.016*	Supported
H5: PC -> PT	-0.025	0.474	0.318	Not Supported
H6: PC -> ADP	0.201	2.895	0.002*	Supported
H7: CON -> ADP	-0.128	1.534	0.063	Not Supported
H8: PT -> ADP	0.152	2.148	0.016*	Supported
H9: SI -> PT	0336	4.776	0.000*	Supported
H10:SI -> ADP	0.003	0.031	0.488	Not Supported

Table 6: Structural Model Results for the Male Group

Paths/Hypotheses	Coefficients	t-statistics	p-values	Remarks
H1:RP -> PT	-0.196	3.691	0.000*	Supported
H2: RP -> ADP	0.128	1.949	0.026*	Supported
H3: PA -> PT	0.271	5.030	0.000*	Supported
H4: PA -> ADP	0.174	0.535	0.296	Not Supported
H5: PC -> PT	-0.010	0.214	0.415	Not Supported
H6: PC -> ADP	0.086	1.992	0.043*	Supported
H7: CON -> ADP	-0.163	2.549	0.005*	Supported
H8: PT -> ADP	0.065	1.997	0.041	Supported
H9: SI -> PT	0.277	4.662	0.000*	Supported
H10:SI -> ADP	0.093	1.333	0.091	Not Supported

7.3 The Multi-group Analysis Results

The final part of the analysis examined whether there were notable differences between genders in the adoption of online privacy security measures. The results showed significant differences in perceived security awareness when adopting these measures by gender ($\beta = -0.139$, $p = 0.022$). This suggests that security awareness has a greater impact on the adoption of privacy security measures among males than among females. However, the study found no significant differences between genders in terms of privacy concerns, perceived trust, risk propensity, convenience, or social influence in adopting online privacy security measures. Similarly, there are no significant differences in privacy concerns, perceived trust, or risk propensity in how these factors affect perceived trust in using privacy controls between genders.

Table 7: Multi-group Analysis Results

Path	Difference (Female - Male)	p-value
HI: RP -> PT	-0.429	0.319
H2: RP -> ADP	-0.333	0.242
H3: PA -> PT	-0.027	0.369
H4: PA -> ADP	-0.139	0.022*
H5: PC -> PT	-0.035	0.308
H6: PC -> ADP	0.115	0.087
H7: CON -> ADP	-0.035	0.372
H8: PT -> ADP	0.088	0.171
H9: SI -> PT	0.058	0.261
H10: SI -> ADP	-0.091	0.204

8.Discussion of the Results

The study investigated the drivers of willingness and gender differences in the willingness to adopt privacy control measures while accessing the internet among students in HLI, Tanzania. To achieve this objective, the study employed a multi-group analysis (MGA) technique in Smart PLS 4. Across all samples, the study found that risk perception negatively impedes user trust in using privacy control measures. The study conducted by Liu et al. (2023) suggests that the finding can be explained by the fact that individuals between 20 and 30 years of age, similar to respondents of this study, exhibit higher risk-taking behaviours, such as risk driving, occupational risks, financial risks, and general risks. Thus, in the context of this study, they are likely to use the internet without ensuring that privacy control measures are in place. Also, their trust in the internet is depressed because of their high-risk perception. Females are generally considered lower risk-takers (Harris & Jenkins, 2006); however, they exhibit similar behaviour in their willingness to use and trust privacy control measures when using the internet. Enabling privacy settings using VPN and encryption methods requires technical skills, which a larger portion of females are short of, as documented by McGill and Thompson (2021). Therefore, low technical skills may substantially affect their level of risk aversion. Further, across all samples, security awareness substantially influences their trust in privacy control measures. The finding aligns with the conclusions of past studies (Ara et al., 2022; Koohang et al., 2021). The finding suggests that security awareness education could substantially increase users' trust in privacy control measures.

Furthermore, the study found that the perceptions of information security awareness impact females' willingness to adopt privacy control measures. The findings suggest that enhancing information security awareness among female students may motivate them to implement privacy control measures when using the internet. As indicated by Saritepeci et al (2024), digital skills and information security awareness are crucial in addressing online privacy concerns. Previous findings suggest that males are generally IT-savvy and more security-aware than females in Tanzania (Lubua et al., 2023; Malero, 2015). However, the current study's findings suggest that being security-aware was insufficient to influence males' willingness to use privacy control measures.

The overall results also revealed that privacy concerns are essential in predicting the willingness to adopt privacy control measures. The finding suggests that regardless of gender, privacy concerns are a nuisance for every group; thus, applying privacy control measures is not an option. This finding supports previous studies, such as those by Chen et al (2017), which have found that privacy concerns impact several security behaviours, including the installation and updating of antivirus software and the frequency of password changes. Nevertheless, the impact of privacy concerns on users' perceived trust in privacy control measures was insignificant. The finding suggests that users prioritise securing their privacy over trusting the measures. Further assessment of the results suggests that the convenience of using the system, combined with the privacy control measures in place, influences the willingness to use these measures among males and the overall sample. The findings support the notion that inconvenient privacy control measures can lead to privacy fatigue, causing users to lose interest in using them (Choi et al., 2018). Therefore, they may trade off convenience for privacy control measures. On the contrary, findings suggest that females don't consider convenience a driving factor in applying privacy control measures. The reason could be that females are more concerned about data privacy than males (Ti, 2019); therefore, they would rather apply privacy control measures, regardless of the convenience they offer, when using the internet.

Moreover, the findings indicate that as perceived trust in the privacy control measures increases, the willingness to use these measures also increases across all samples. This finding is consistent with that of Alodhyani et al. (2020) and Farooq et al. (2021), who also found the same outcome in password manager adoption. Regarding the impact of social influence, the findings confirmed that it positively affects trust in privacy control measures. On the contrary, its impact on willingness to use privacy control measures is insignificant. The finding implies that social influence helps build user trust, but doesn't extend to enticing users to apply privacy control measures. The findings on the impact of social influence on perceived trust support are supported by Tian et al (2023).

A multi-group analysis was conducted to examine whether the influence of the study's variables on perceived trust in privacy control measures and willingness to adopt privacy control measures varies. The results of the multi-group analysis (see Table 7) indicate significant differences in perceived security awareness between females and males. The finding further reveals that the perception of security awareness is higher among both male and female respondents. This discovery aligns with Alotaibi and Alshehri (2020) and McGill and Thompson (2021). However, the study found no significant differences in willingness to adopt privacy control measures and perceived trust between male and female students in terms of risk perception, privacy concerns, perceived trust, convenience, and social influence.

9.Implications

The current study has substantive implications for researchers, practitioners, and managers. For researchers, this study presents a pioneering effort to identify gender differences in the adoption of privacy control measures among students in HLIs in Tanzania, leveraging a multi-group analysis approach. Moreover, the study enriched the privacy calculus theory by incorporating the dimensions of social influence and convenience within the context of HLIs. Notably, social influence plays a vital role in shaping behaviour in a community-oriented environment, such as higher learning institutions. For practitioners, the findings highlight actionable insights for ICT security personnel or those responsible for information security governance and implementation in higher learning institutions. Emphasising factors that facilitate the adoption of privacy control measures among students, particularly those linked to risk perceptions, perceived security awareness, and perceived trust in the general population. This strategy increases the likelihood that students will use the internet safely. Additionally, targeted interventions are needed to enhance the perceptions of information security awareness among female students and motivate them to adopt privacy measures. This will promote equitable female engagement in using online learning resources while safeguarding their privacy and data.

From a managerial standpoint, the study calls for a systematic rollout of security awareness and training programmes across higher learning institutions (HLIs) in Tanzania. Overall, the Findings suggest that risk perception, privacy concerns, trust in the internet, and privacy settings in web-based applications influence the adoption of privacy control measures. Therefore, policy frameworks and interventions should be strategically aligned with these findings to promote privacy awareness at HLIs.

10.Conclusions, Limitations, and Future Studies

Despite the study’s practical and theoretical implications, it has some limitations. First, the study only sampled students from higher learning institutions in Tanzania, so the findings may not apply to other population groups. Future research could replicate similar studies in the general population. Second, various demographic factors, such as the adoption of privacy control measures, might influence information security behaviours. Although this study focused on gender, future research would be valuable to examine other demographic traits, such as education level, income, and age. Third, the results may be specific to Tanzania. Future studies should encompass a broader range of countries to gain a deeper understanding of how privacy control measures are adopted across different cultures.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interests

The authors declare that there is no conflict of interest regarding the publication of this paper.

Reference

[1] Akter, M., Park, J. K., Headrick, C., Page, X., & Wisniewski, P. J. (2025). Calculating Connection vs. Risk: Understanding How Youth Negotiate Digital Privacy and Security with Peers Online. ArXiv Preprint ArXiv:2503.22993.

[2] Alesanco-Llorente, M., Reinares-Lara, E., Pelegrín-Borondo, J., & Olarte-Pascual, C. (2023). Mobile-assisted showrooming behavior and the (r) evolution of retail: The moderating effect of gender on the adoption of mobile augmented reality. Technological Forecasting and Social Change, 191, 122514.

[3] Allen, A. L. (1999). Gender and privacy in cyberspace. Stan. L. Rev., 52, 1175–1200.

[4] Almaiah, M. A., Al-otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the Role of Perceived Risk , Perceived Security and Perceived Trust on Smart m-Banking Application Using SEM. 1–17.

[5] Ara, A., Zainol, Z., & Duraisamy, B. (2022). The effects of privacy awareness, security concerns and trust on information sharing in social media among public university students in Selangor. International Business Education Journal, 15(2), 93–110.

[6] Armstrong, J. S., & Overton, T. S. (1977). Estimating non-response bias in mail surveys. Journal of Marketing Research, 14(3), 396–402.

[7] Ashrafi, D. M., Ahmed, S., & Shahid, T. S. (2024). Privacy or trust: understanding the privacy paradox in users' intentions towards e-pharmacy adoption through the lens of privacy-calculus model. Journal of Science and Technology Policy Management.

[8] Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. Journal of Communication, 67(1), 26–53. https://doi.org/10.1111/jcom.12276

[9] Bélanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. Information Systems Journal, 25(6), 573–578.

[10] Benhissi, M., & Hamouda, M. (2025). Investigating consumers' slow fashion purchase decision: role of lack of information and confusion. European Business Review, 37(3), 575–595.

[11] Benoit, S., Klose, S., & Ettinger, A. (2017). Linking service convenience to satisfaction: Dimensions and key moderators. Journal of Services Marketing, 31(6), 527–538.

[12] Berkman, B. A. (1971). The Assault on Privacy: Computers, Data Banks, and Dossiers, by Arthur R. Miller. Case Western Reserve Law Review, 22(4), 808.

[13] Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. Cyberpsychology, Behavior, and Social Networking, 18(1), 13–19.

[14] Chen, S., Doerr, S., Frost, J., Gambacorta, L., & Shin, H. S. (2023). The fintech gender gap. Journal of Financial Intermediation, 54, 101026.

[15] Cheng, X., Qiao, L., Yang, B., & Zhang, X. (2024). Investigation on users' resistance intention to facial recognition payment : a perspective of privacy. Electronic Commerce Research, 24, 275–301.

[16] Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42–51.

[17] Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a

study of Italy and the United States. European Journal of Information Systems, 15(4), 389–402.

[18] Dinev, T., & 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), 23.

[19] Elbitar, Y., Schilling, M., Nguyen, T. T., Backes, M., & Bugiel, S. (2021). Explanation beats context: The effect of timing & rationales on users' runtime permission decisions. 30th USENIX Security Symposium (USENIX Security 21), 785–802.

[20] ElShahed, H. (2023). Privacy Paradox Amid E-Commerce Epoch: Examining Egyptian Youth's Practices of Digital Literacy Online. In Marketing and Advertising in the Online-to-Offline (O2O) World (pp. 45–64). IGI Global.

[21] Esmaeilzadeh, P. (2020). The impacts of the privacy policy on individual trust in health information exchanges (HIEs). Internet Research, 30(3), 811–843. https://doi.org/10.1108/INTR-01-2019-0003

[22] Feng, Y., Yao, Y., & Sadeh, N. (2021). A design space for privacy choices: Towards meaningful privacy control in the internet of things. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–16.

[23] Fernandes, T., & Costa, M. (2023). Privacy concerns with COVID-19 tracking apps: A privacy calculus approach. Journal of Consumer Marketing, 40(2), 181–192.

[24] Ferrante, T., & Ajani, T. (2024). Risk-Taking Propensity and Information Security Compliance Behavior in Government Workers: A Quantitative Correlational Study. Issues in Information Systems, 25(3), 1–12.

[25] Fortino, G., Fotia, L., Messina, F., Rosaci, D., & Sarné, G. M. L. (2020). Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges. IEEE Access, 8, 60117–60125. https://doi.org/10.1109/ACCESS.2020.2982318

[26] Gong, J., Said, F., Ting, H., Firdaus, A., Ali, I., & Jinghong, A. (2023). Do Privacy Stress and Brand Trust still Matter ? Implications on Continuous Online Purchasing Intention in China. Current Psychology, 42(18), 15515–15527. https://doi.org/10.1007/s12144-022-02857-x

[27] Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. Thirty Fourth International Conference on Information Systems.

[28] Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135.

[29] Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The Use of Partial Least Squares Path Modeling in International Marketing. In R. . Sinkovics & P. . Ghauri (Eds.), New challenges to international marketing (pp. 277–319). Emerald Group Publishing Limited. https://doi.org/https://doi.org/10.1108/S1474-7979(2009)0000020014

[30] Ho, S., Lwin, M., Yee, A., & Lee, E. (2015). Understanding Factors Associated with Singaporean Adolescents' Intention to Adopt Privacy Protection Behavior Using an Extended Theory of Planned Behavior. Cyberpsychology, Behavior, and Social Networking, 1–24.

[31] Jabbar, A., Geebren, A., Hussain, Z., Dani, S., & Ul-Durar, S. (2023a). Investigating individual privacy within CBDC: A privacy calculus perspective. Research in International Business and Finance, 64, 101826.

[32] Jabbar, A., Geebren, A., Hussain, Z., Dani, S., & Ul-Durar, S. (2023b). Investigating individual privacy within CBDC: A privacy calculus perspective. Research in International Business and Finance, 64(May 2022), 101826. https://doi.org/10.1016/j.ribaf.2022.101826

[33] Jang, C. (2024). Coping with vulnerability: the effect of trust in AI and privacy-protective behaviour on the use of AI-based services. Behaviour & Information Technology, 43(11), 2388–2400.

[34] Jaspers, E. D. T., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things : The role of trust and privacy concerns. Journal of Business Research, 142(January 2021), 255–265. https://doi.org/10.1016/j.jbusres.2021.12.043

[35] Kang, H. (2023). Communication privacy management for smart speaker use : Integrating the role of privacy self-efficacy and the multidimensional view. New Media & Society, 25(5), 1153–1175. https://doi.org/10.1177/14614448211026611

[36] Koloseni, D., & Sedoyeka, E. M. (2019). The Adoption of Security Control Apps among Smartphone Users in Tanzania. International Journal of Technology Diffusion (IJTD), 10(4), 1–18.

[37] Koohang, A., Floyd, K., Yerby, J., & Paliszkiewicz, J. (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. Issues in Information Systems, 22(2), 133–145. https://doi.org/10.48009/2_iis_2021_136-149

[38] Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 1.

[39] Lim, W. (2024). A typology of validity: content, face, convergent, discriminant, nomological and predictive validity. Journal of Trade Science, 12(3), 155–179. https://doi.org/10.1108/jts-03-2024-0016

[40] Liu, Y., Bagaïni, A., Son, G., Kapoor, M., & Mata, R. (2023). Life-Course Trajectories of Risk-Taking Propensity: A Coordinated Analysis of Longitudinal Studies. The Journals of Gerontology: Series B, 78(3), 445–455. https://doi.org/10.1093/geronb/gbac175

[41] Lu, C.-H. (2024). The moderating role of e-lifestyle on disclosure intention in mobile banking: A privacy calculus perspective. Electronic Commerce Research and Applications, 64, 101374.

[42] Lubua, E. W., Semlambo, A. A., & Mkude, C. G. (2023). Factors Affecting the Security of Information Systems in Africa: A Literature Review. University of Dar Es Salaam Library Journal, 17(2), 94–114. https://doi.org/10.4314/udslj.v17i2.7

[43] Malero, A. (2015). Measuring security awareness on mobile money users in Tanzania. International Journal of Engineering Trends and Technology, 20(1), 44–47.

[44] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual Differences and Information Security Awareness. Computers in Human Behavior, 69, 151–156.

[45] McGill, T., & Thompson, N. (2021). Exploring potential gender differences in information security and privacy. Information and Computer Security, 29(5), 850–865. https://doi.org/10.1108/ICS-07-2020-0125

[46] Meier, Y., & Krämer, N. C. (2024). The privacy calculus revisited: an empirical investigation of online privacy decisions on between-and within-person levels. Communication Research, 51(2), 178–202.

[47] Mutimukwe, C., Viberg, O., Oberg, M., & Pargman, T. C.-. (2022). Students' privacy concerns in learning analytics : Model development. British Journal of Educational Technology, 53, 932–951. https://doi.org/10.1111/bjet.13234

[48] Ngoqo, B., & Flowerday, S. V. (2015). Exploring the relationship between student mobile information security awareness and behavioural intent. Information & Computer Security, 23(4), 406–420.

[49] Nguyen, Q. N., & Kim, D. J. (2017). Enforcing Information Security Protection : Risk Propensity and Self-Efficacy Perspectives. Proceedings of the 50th Hawaii International Conference on System Sciences, 4947–4956.

[50] Park, C., Kim, D., Cho, S., & Han, H.-J. (2019). Adoption of multimedia technology for learning and gender difference. Computers in Human Behavior, 92, 288–296.

[51] Rahi, S., & Abd. Ghani, M. (2018). The role of UTAUT, DOI, perceived technology security and game elements in internet banking adoption. World Journal of Science, Technology and Sustainable Development, 15(4), 338–356.

[52] Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity : How to Tackle Cyber Fatigue. Sage Open, 1–18. https://doi.org/10.1177/21582440211000049

[53] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. The Journal of Psychology, 91(1), 93–114.

[54] Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2022). The role of privacy in the acceptance of smart technologies: Applying the privacy calculus to technology acceptance. International Journal of Human–Computer Interaction, 38(13), 1276–1289.

[55] Senarath, A. R., & Arachchilage, N. A. G. (2018). Understanding user privacy expectations: A software developer's perspective. Telematics and Informatics, 35(7), 1845–1862.

[56] Senior, V., Smith, J. A., Michie, S., & Marteau, T. M. (2002). Making sense of risk: An interpretative phenomenological

analysis of vulnerability to heart disease. Journal of Health Psychology, 7(2), 157–168.

[57] Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. Computers in Human Behavior, 52, 278–292.

[58] Tahaei, M., Abu-Salma, R., & Rashid, A. (2023). Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications. In Conference on Human Factors in Computing Systems - Proceedings (Vol. 1, Issue 1). Association for Computing Machinery. https://doi.org/10.1145/3544548.3581060

[59] Tahaei, M., & Vaniea, K. (2021). “developers are responsible”: What ad networks tell developers about privacy. Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, 1–11.

[60] Tan, K., Leong, C., Richter, N. F., & Tan, K. (2025). Navigating Trust in Mobile Payments : Using Necessary Condition Analysis to Identify Must- Have Factors for User Acceptance Navigating Trust in Mobile Payments : Using Necessary Condition Analysis to Identify Must-Have Factors for User Acceptance. International Journal of Human–Computer Interaction, 41(5), 3325–3339. https://doi.org/10.1080/10447318.2024.2338319

[61] Ti, S. (2019). Gender differences in privacy tendencies on social network sites : A meta- analysis. Computers in Human Behavior, 93(June 2018), 1–12. https://doi.org/10.1016/j.chb.2018.11.046

[62] Tian, X. (2025). Unraveling the dynamics of password manager adoption : a deeper dive into critical factors. Information & Computer Security, 33(1), 117–139. https://doi.org/10.1108/ICS-09-2023-0156

[63] Tian, Y., Chan, T. J., Suki, N. M., & Kasim, M. A. (2023). Moderating role of perceived trust and perceived service quality on consumers’ use behavior of Alipay e-wallet system: the perspectives of technology acceptance model and theory of planned behavior. Human Behavior and Emerging Technologies, 2023.

[64] Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. Computers in Human Behavior, 93, 1–12.

[65] van der Schyff, K., & Flowerday, S. (2021). Mediating effects of information security awareness. Computers & Security, 106, 102313.

[66] Venkatesh, V., Morris, M. G., & Ackerman, P. L. (2000). A longitudinal field investigation of gender differences in individual technology adoption decision-making processes. Organisational Behavior and Human Decision Processes, 83(1), 33–60.

[67] Wijesekera, P., Reardon, J., Reyes, I., Tsai, L., Chen, J. W., Good, N., Wagner, D., Beznosov, K., & Egelman, S. (2018). Contextualising privacy decisions for better prediction (and protection). Conference on Human Factors in Computing Systems - Proceedings, 2018-April, 1–12. https://doi.org/10.1145/3173574.3173842

[68] Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. Electronic Commerce Research, 13(2), 151–168. https://doi.org/10.1007/s10660-013-9111-6