Global Advances in Business Studies (GABS), 2025, 4(2), 73-81
GLOBAL ADVANCES IN BUSINESS STUDIES (GABS)
http://journal-gabs.org/gabs

Cybersecurity risk awareness in mobile banking: evidence from Sabah, Malaysia

Rosle Mohidin[1,*], Nelson Lajuni[1], Rahayu Lestari[2], Wahyu Wastuti[3], Dg Safrina Ag Budin[1], Olufemi Adewale Ogunkoya[4], Monica Dewi[3], Hari Muharam[5], Salmah[5]

[1]Faculty of Business, Economics and Accountancy Universiti Malaysia Sabah, Malaysia
[2]Faculty of Economics and Business Universitas Nasional, Indonesia
[3]Faculty of Economics and Business Universitas Negeri Jakarta, Indonesia
[4]Faculty of Administration and Management Sciences Olabisi Onabanjo University, Nigeria
[5]Faculty of Economics and Business Universitas Pakuan, Indonesia

Article info

Article history:
Received: 13 August 2025
Accepted: 19 September 2025
Published: 29 September 2025

Keywords:
cybersecurity risk awareness; mobile banking security; PLS-SEM analysis

Abstract

This study investigates how Sabahan perceive and respond to cybersecurity risks when using mobile banking. This study employed partial least squares structural equation modeling (PLS-SEM) and focused on four main factors: user awareness and behavior (UAB), mobile device security (MDS), banking app security features (BASF), and perceived cybersecurity threats (CT). A total of 350 questionnaires were distributed, and 286 valid responses were analyzed. The results indicate that UAB, MDS, and BASF all play a significant role in shaping cybersecurity risk awareness (CRA), while CT showed little to no direct effect. These findings suggest that improving user education and promoting secure practices are just as important as technical safeguards. In particular, enhancing digital literacy among less tech-savvy users, ensuring that security features are simple to use, and strengthening device protections can all help reduce risks of cybersecurity. The study concludes that a combination of user-focused education and stronger security standards is necessary to improve the overall safety of mobile banking services.

JEL classifications: G32, K24

Citation:
Mohidin, R., Lajuni, N., Lestari, R., Wastuti, W., Budin, D.S.A., Ogunkoya, O.A., Dewi, M., Muharam, H. & Salmah. (2025). Cybersecurity risk awareness in mobile banking: evidence from Sabah, Malaysia. *Global Advances in Business Studies*, 4(2), 73-81. https://doi.org/10.55584/Gabs.004.02.2

*Corresponding author: Rosle Mohidin
awgdin@ums.edu.my

1. Introduction

The rapid growth of mobile banking has transformed the financial services industry, giving users new levels of convenience and easier access to banking facilities. At this point of time, this digital shift has also brought greater exposure to cybersecurity threats such as phishing, malware, data breaches, and identity theft. As mobile banking becomes part of everyday life, the demand for stronger cybersecurity measures is more urgent than ever (Cheng et al., 2020).

Cyber risks pose a serious challenge to the stability and security of digital financial systems. They are not limited to technical weaknesses alone but also take advantage of human behavior often exploiting gaps in users' knowledge and awareness. With cybercrime evolving rapidly, safeguarding sensitive financial information has become a critical concern for banks, regulators, and individual users alike.

Sabah, a state in Malaysia, illustrates how the rise of mobile banking adoption can be accompanied by distinct cybersecurity issues. Its socio-economic and geographical diversity with urban areas like Kota Kinabalu enjoying better infrastructure, while many rural communities face poor connectivity and lower levels of digital literacy creates uneven levels of vulnerability to cybercrime (Trend Micro, 2020).

Although Malaysia has made efforts at the national level to improve cybersecurity, the challenges in Sabah show that region-specific approaches are still necessary. The growing reliance on mobile banking has not been matched by an equal rise in user awareness of cybersecurity risks. This gap leaves many users more exposed to attacks, raising the likelihood of financial losses and weakening trust in digital banking platforms.

The issue is made worse by the limited availability of high-speed internet in rural areas, which restricts access to both information and cybersecurity resources. On top of this, users demonstrate varying levels of digital literacy, creating uneven levels of vulnerability. Much of the existing research on mobile banking security tends to address cybersecurity challenges in broad terms, without giving enough attention to the specific socio-economic and technological realities of regions such as Sabah. Very little is known about how factors like user behavior, mobile device security, and banking app features interact to shape risk awareness in these diverse settings. This gap highlights the need for a focused investigation into Sabah's unique vulnerabilities in order to develop cybersecurity strategies that are better tailored to its context.

The main aim of this study is to analyze how user awareness and behavior, mobile device security, banking app security features, and cybersecurity threats influence risk awareness among mobile banking users in Sabah. By narrowing its focus on this region, the study hopes to add meaningful insights to the wider discussion on mobile banking security, offering findings that are especially relevant to areas with varied socio-economic backgrounds like Sabah.

2. Literature review

The rapid growth of mobile banking, particularly in developing countries like Malaysia, has enhanced financial inclusion through increased smartphone use and internet access (Omar et al., 2020). However, this expansion has also introduced significant cybersecurity risks, especially in regions like Sabah, where socio-economic challenges and limited digital literacy exacerbate vulnerabilities (CyberSecurity Malaysia, 2022). Mobile banking faces cyber threats such as zero-day vulnerabilities, ransomware, and advanced persistent threats (APTs), which target security weaknesses despite advanced protective measures by financial institutions (Kaspersky, 2021; Trend Micro, 2020; McAfee, 2021). Emerging technologies such as multi-factor authentication, blockchain, and biometrics offer potential solutions but require effective implementation and user engagement (Li et al., 2021). Additionally, limited internet infrastructure and low cybersecurity awareness in Sabah hinder the effectiveness of cybersecurity initiatives like CyberSAFE, underlining the need for localized, offline resources (CyberSecurity Malaysia, 2022).

User awareness and behavior play a critical role in reducing cybersecurity risks in mobile banking. A lack of awareness regarding threats like phishing and weak cybersecurity practices, such as the use of weak passwords, increases vulnerability (Yoon, 2021; Anderson & Agarwal, 2019). Effective user education programs can significantly improve security practices and reduce risk exposure (Nguyen et al., 2022). Moreover, the security of mobile devices is vital in protecting sensitive data. Vulnerabilities in operating systems and applications can expose financial information, which emphasizes the need for security features like biometric authentication and encryption to safeguard mobile banking (Conti et al., 2020; Bhatia & Kaushik, 2021).

Finally, banking app security features such as two-factor authentication and secure login protocols are crucial for preventing unauthorized access to mobile banking platforms (Das & Bhatnagar, 2020). Proactive strategies, including real-time monitoring, threat intelligence, and a focus on cybersecurity literacy, are essential to address the dynamic nature of cybersecurity threats (Alotaibi & Kavakli, 2021; Cheng et al., 2020; Tahir et al., 2021). These efforts will help to strengthen mobile banking security, ensuring a safer environment for users and enhancing trust in digital financial services.

3. Research methodology

This study adopts a quantitative approach to investigate cybersecurity risks awareness in mobile banking in Sabah. This study targeted 250 mobile banking users. Out of the 320 questionnaires received, only 286 were usable, representing a valid response rate of 89.4%. The data collected is analysed using SmartPLS 4.0, a tool for structural equation modeling (SEM) that is well-suited for predicting key target constructs in PLS-SEM models. The use of this software allows for a comprehensive understanding of how various factors interact within the context of mobile banking cybersecurity risks awareness.

The analysis focused on several key areas of measurement such as internal consistency that assessed using Cronbach's alpha and composite reliability (CR), where values above 0.7 indicate adequate reliability (Hair et al., 2019). Indicator reliability is used to evaluate outer loadings of each indicator, with values exceeding 0.7 considered indicative of strong reliability (Chin, 1998). Convergent validity is measured using average variance extracted (AVE), with a value above 0.5 suggesting that the latent construct explains more than half of the variance in the indicators. Discriminant validity is assessed using the Fornell-Larcker criterion and the Heterotrait-Monotrait ratio (HTMT), with HTMT values below 0.85 indicating sufficient distinctness between constructs (Henseler et al., 2015). These analyses will ensure that the constructs in the model are both reliable and valid, offering robust insights into the study's objectives.

4. Findings

A total of 320 respondents participating in this study and out of the only 286 questionnaires are taken into consideration for data analysis. The rest of the questionnaires either incomplete or not answered. Table 1 provides a comprehensive demographic breakdown of the survey participants. Out of 286 respondents, 43% are male (123 respondents), and 57% are female (163 respondents). This balanced gender representation ensures the findings can be generalized across genders. The respondents are predominantly young, with 49% aged 25-34 years. The second-largest group comprises those below 24 years (24.1%), followed by 35-44 years (22.4%). Only a small fraction is older than 44 years, highlighting a younger demographic's focus.

Table 1. Profiling of respondents

Variable	Description	N	Frequency	Percent
Gender	Male	286	123	43
	Female		163	57
Age	< 24 years old	286	69	24.1
	25-34 years old		140	49
	35-44 years old		64	22.4
	45-54 years old		10	3.5
	> 55 years old		2	0.7
Education	SPM/O level	286	77	26.9
	Diploma/STPM/A level		106	37.1
	Degree		92	32.2
	Master		11	3.8
Income	<RM1500	286	60	21.0
	RM1501-RM5000		176	61.5
	RM5001-RM9000		39	13.6
	RM9001-RM13000		9	3.1
	>RM13001		2	0.7
Location	West coast of Sabah	286	175	61.2
	Rural area of Sabah		77	26.9
	East coast of Sabah		29	10.1
	North of Sabah		5	1.7

The data shows a diverse educational background, with the majority holding diploma/STPM/A-level qualifications (37.1%). Degree holders constitute 32.2%, while 26.9% have SPM/O level education. Master's degree holders are a minority at 3.8%. Most respondents earn between RM1501 and RM5000 (61.5%), indicating a middle-income demographic. Lower-income earners (<RM1500) constitute 21%, and a smaller segment earns above RM5000, signifying a broad range of income levels. The majority of respondents are from the west coast of Sabah (61.2%), followed by 26.9% from rural areas of Sabah, and 10.1% from the east coast, reflecting a concentration in more urbanized regions.

Table 2 presents the results of the measurement model assessment, focusing on the outer loadings of each item to its underlying construct. The outer loadings, which range from 0.501 to 0.899, measure how well each item represents its respective construct, with higher values indicating stronger relationships. For most constructs, such as "Banking app security features" (BASP), "Mobile banking cybersecurity risks awareness" (CRA), "Cybersecurity threats" (CT), "Mobile device security" (MDS), and "User awareness and behavior" (UAB), the majority of items have loadings above 0.70, which is considered acceptable (Hair et al., 2019). However, some items like BASP5, CRA5, CT5, MDS5, and UAB5 have lower loadings, suggesting they may be weaker indicators of their constructs.

The Cronbach's alpha (CA) values for all constructs range from 0.831 to 0.841, indicating strong internal consistency. The composite reliability (CR) values range from 0.884 to 0.890, further validating the reliability of the constructs (Hair et al., 2019). Additionally, the average variance extracted (AVE) values, which range from 0.610 to 0.623, confirm sufficient convergent validity, as suggested by Fornell and Larcker (1981). These metrics collectively affirm that the measurement model used in this study is reliable and valid, meeting established standards in the literature.

Table 2. Measurement model assessment

Construct	Item	Loadings	CA	CR	AVE
Banking app security features	BASP1	0.789	0.831	0.884	0.610
	BASP2	0.871			
	BASP3	0.781			
	BASP4	0.888			
	BASP5	0.520			
Mobile banking cybersecurity risks awareness	CRA1	0.798	0.838	0.888	0.620
	CRA2	0.877			
	CRA3	0.795			
	CRA4	0.886			
	CRA5	0.524			
Cybersecurity threats	CT1	0.805	0.838	0.889	0.623
	CT2	0.877			
	CT3	0.812			
	CT4	0.886			
	CT5	0.501			
Mobile device security	MDS1	0.791	0.841	0.890	0.623
	MDS2	0.874			
	MDS3	0.793			
	MDS4	0.899			
	MDS5	0.540			
User awareness and behavior	UAB1	0.796	0.837	0.888	0.619
	UAB2	0.876			
	UAB3	0.794			
	UAB4	0.887			
	UAB5	0.526			

No item was deleted as loading composite reliability > .708 (Hair et al., 2019)

Table 3 shows the criterion of HTMT to evaluate discriminant validity (Henseler et al., 2015). The result confirms that the discriminant validity is well established at HTMT 0.90 (Henseler et al., 2015). To assess reliability, this study is based on Henseler's heterotrait-monotrait ratio of correlations. All HTMT values are below the 0.90 threshold, with the highest value being 0.869 (between BASP and CT). There is no problem of multi-collinearity between the items loaded on different constructs in the outer model. This result indicates that the constructs are sufficiently distinct from each other, satisfying discriminant validity. The results pave the way to the next assessment known as a structural model assessment which means that it does not have the issue of discriminant validity as it does not violate the most conservative criterion (HTMT 0.90).

Table 3. HTMT criterion

	BASP	CRA	CT	MDS	UAB
BASP	■				
CRA	0.788	■			
CT	0.869	0.769	■		
MDS	0.854	0.868	0.833	■	
UAB	0.780	0.793	0.860	0.861	■

Criteria: Discriminant validity is established at HTMT 0.90 (Gold et al., 2001)

Table 4. Path coefficients and model quality assessment

Direct effect	Beta	S.E.	t-value	p-value	Decision	f^2	R^2	VIF
H1: UAB -> CRA	0.385	0.044	8.695	0.000	Supported	1.116	0.730	1.810
H2: MDS -> CRA	0.439	0.055	7.980	0.000	Supported	0.165		2.967
H3: BASP -> CRA	0.131	0.062	2.122	0.034	Supported	0.332		2.927
H4: CT -> CRA	-0.011	0.034	0.311	0.756	Not supported	0.046		1.030

Note: *p<0.05, **p<0.01, bias corrected, LL=lower limit, UL=upper limit p-value of 0.01, 0.05 (Hair et al., 2019)
$f^2 \geq 0.35$ consider substantial, $R^2 \geq 0.26$ consider substantial, VIF ≤ 5.0 (Hair et al., 2019)

The structural model assessment examines the proposed relationship between the variables in the research framework. Before measuring the structural model, this study addresses the issue of multi-collinearity using collinearity test. The VIF values below 5.5 for each of the constructs suggest that the problem of multi-collinearity is not a concern. Next, a 5000-bootstrap resampling of data is conducted to examine the hypotheses of this study (Hair et al., 2019).

The relationship between UAB and CRA ($\beta = 0.385$, $t = 8.695$, $p < 0.01$) is strong and positive, indicating that higher user awareness and behavior positively impact cybersecurity risk awareness. Similarly, MDS positively influences CRA ($\beta = 0.439$, $t = 7.980$, $p < 0.01$). The effect of BASP on CRA is weaker but still significant ($\beta = 0.131$, $t = 2.122$, $p < 0.05$). However, the relationship between CT and CRA is not supported ($\beta = -0.011$, $p = 0.756$). The R^2 value of 0.730 for CRA indicates that 73% of the variance in CRA is explained by UAB, MDS, BASP, and CT. The VIF values, all below 3.3, suggest that multicollinearity is not a concern.

Table 5. Result of PLS predict

Construct	Items	PLS-RMSE	MAE	LM-RMSE	MAE	PLS-LM RMSE	MAE	Q^2 predict	Predict power
Cybersecurity risks awareness	CRA1	0.720	0.543	0.740	0.558	-0.020	-0.015	0.547	Moderate
	CRA2	0.646	0.504	0.677	0.514	-0.031	-0.010	0.572	
	CRA3	0.657	0.521	0.603	0.464	0.054	0.057	0.571	
	CRA4	0.821	0.647	0.839	0.658	-0.018	-0.011	0.395	
	CRA5	0.802	0.636	0.597	0.440	0.205	0.196	0.489	

Table 5 evaluates the predictive accuracy of the model using PLS-Predict, to assess the out-of-sample prediction power of partial least squares (PLS) models. The analysis focused on key metrics such as PLS-RMSE (root mean square error), MAE (mean absolute error), LM-RMSE (linear model RMSE), LM-MAE, and Q^2 predict, which measure the accuracy of the model's predictions against actual values. In general, lower values of these metrics indicate better predictive performance. CRA1 exhibited a PLS-RMSE of 0.720 and an MAE of 0.543, while CRA2 demonstrated a PLS-RMSE of 0.646 and an MAE of 0.504, suggesting moderate prediction accuracy.

Most CRA items displayed PLS-RMSE and MAE values close to those of the linear model, indicating that the PLS model performs similarly or slightly better than the linear model. CRA3 had a PLS-RMSE of 0.657 and an LM-RMSE of 0.603, showing comparable prediction accuracy. Negative PLS-LM differences in both RMSE and MAE suggest that the PLS model offers slightly more robust predictive performance, as seen in CRA1, which shows a PLS-LM RMSE difference of -0.020 and an MAE difference of -0.015.

The Q^2 predict metric further evaluates the model's predictive relevance, with values above 0.35 indicating moderate predictive power (Shmueli et al., 2016). CRA1 and CRA3 recorded Q^2 predict values of 0.547 and 0.571, respectively, indicating moderate predictive relevance. However, the predictive power for other CRA items was lower, with CRA4 and

CRA5 showing Q² predict values of 0.395 and 0.489, respectively. Overall, the model demonstrated moderate predictive accuracy for most items within the cybersecurity risks awareness (CRA) construct, with some items performing more robustly compared to the linear model baseline. The range of Q² predict values from moderate to low points to potential areas for improvement in the model's predictive capabilities, suggesting that further refinement of the model could enhance its overall performance in future studies.

5. Discussion

The study reveals several critical insights into the cybersecurity dynamics in mobile banking within Sabah. The analysis demonstrates that user awareness and behavior (UAB), mobile device security (MDS) and banking app security features (BASP), have significant positive effects on cybersecurity risk awareness (CRA). These findings suggest that when users are more aware of cybersecurity practices and engage in secure behaviors, their ability to recognize and mitigate potential risks increases. The strong link between UAB and CRA highlights the importance of user education in cybersecurity. Users who are well-informed about threats like phishing and malware are better at avoiding risky behaviors, such as clicking on suspicious links or using weak passwords (Yoon, 2021). This supports previous research on the role of cybersecurity literacy in improving digital safety (Nguyen et al., 2022). The challenge is ensuring this knowledge leads to consistent, proactive behavior across different demographics.

The significant impact of MDS on CRA shows the importance of device-level security in protecting user data. Mobile devices are crucial for mobile banking, making their security essential (Conti et al., 2020; Bhatia & Kaushik, 2021). The study shows that users with strong security features, like biometric authentication and encryption, are more aware of and responsive to threats. This emphasizes the need for ongoing user education on keeping security software updated and following best device security practices. Although banking app security features (BASP) positively impact CRA, the effect is smaller than that of UAB and MDS. This suggests that while bank-provided technical safeguards are important, users may not fully understand or use them, which reduces their effectiveness. These features could be more useful if made user-friendly and accompanied by clear guidance (Das & Bhatnagar, 2020).

Interestingly, the direct impact of perceived cybersecurity threats (CT) on CRA is not significant. This could imply that users might not fully comprehend the severity or implications of these threats until they encounter or hear about specific incidents (Cheng et al., 2020). It suggests a potential gap in the communication and perception of cybersecurity risks, which could be bridged by more vivid and relatable threat communication strategies, such as real-life scenarios and interactive training. The demographic breakdown reveals that younger users (aged 25-34) dominate the respondent group, suggesting a younger demographic's inclination toward mobile banking. This demographic is likely to be more tech-savvy but might also be overconfident, potentially leading to negligence in cybersecurity practices (Anderson & Agarwal, 2019). Additionally, the lower engagement in rural areas points to digital literacy and infrastructural disparities, further emphasizing the need for targeted educational efforts (CyberSecurity Malaysia, 2022).

The moderate predictive power of the model for CRA suggests that while the current variables explain a significant portion of variance in cybersecurity risk awareness, there may be other unexamined factors influencing user behavior and awareness. This calls for future research to explore additional variables such as cultural attitudes towards technology, the influence of peer networks, and the role of government regulations in shaping cybersecurity practices (Shmueli et al., 2016). Overall, these findings reinforce the multifaceted nature of cybersecurity in mobile banking, where user behavior, device security, and app features interact in complex ways. The implications point to a holistic approach that combines technical safeguards with robust user education and community engagement to create a secure mobile banking environment.

6. Conclusion

This study sheds light on the critical factors influencing cybersecurity risk awareness among mobile banking users in Sabah. The significant positive relationships between user awareness and behavior (UAB), mobile device security (MDS), and cybersecurity risk awareness (CRA) highlight the importance of educating users and promoting secure practices. Although banking app security features (BASP) play a role, their impact is less pronounced, suggesting the need for better user engagement and understanding of these features. The negligible effect of perceived cybersecurity threats (CT) on CRA indicates a gap in risk perception that requires targeted communication strategies. Overall, the findings emphasize that while technical security measures are vital, the human factor remains crucial in mitigating cybersecurity risks. By enhancing user education and promoting robust security practices, financial institutions can significantly improve the security posture of mobile banking services.

To enhance cybersecurity in mobile banking, it is crucial to implement comprehensive education programs that raise awareness about common threats and best practices. These programs should cater to diverse demographic groups, particularly focusing on those with lower digital literacy in rural areas. Financial institutions should also improve the user interface of banking apps to make security features like two-factor authentication more accessible and easier to use. Additionally, targeted awareness campaigns using real-life scenarios can help users better understand and respond to cybersecurity risks. Strengthening mobile device security by encouraging practices such as regular updates and the use of antivirus software is essential. Policymakers should support these efforts by enforcing strict security standards and providing incentives for adopting advanced cybersecurity technologies. Engaging community leaders in education initiatives can further extend the reach of cybersecurity awareness, creating a more secure environment for mobile banking users.

References

Alotaibi, M. & Kavakli, E. (2021). Threat intelligence in cybersecurity: a survey. *Computer Science Review*, 41, 100393. https://doi.org/10.1016/j.cosrev.2021.100393

Anderson, C.L. & Agarwal, R. (2019). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469-490.

Bhatia, S. & Kaushik, S. (2021). Security and privacy challenges in mobile banking applications: a review. *International Journal of Engineering and Advanced Technology*, 10(3), 198-203.

Cheng, L., Liu, F., Yao, D. & Sun, J. (2020). Enterprise cybersecurity threat analysis and modeling: a holistic view. *Journal of Computer Security*, 28(1), 89-116.

Chin, W.W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295–336). Lawrence Erlbaum Associates.

Conti, M., Kumar, M., Lal, C. & Ruj, S. (2020). A survey on security and privacy issues of TikTok. *arXiv preprint arXiv:2011.03958*.

CyberSecurity Malaysia. (2022). CyberSAFE (cyber security awareness for everyone): enhancing digital hygiene in Malaysia. *CyberSecurity Malaysia Reports*.

Das, S. & Bhatnagar, N. (2020). Enhancing security in mobile banking using AI-based two-factor authentication. *Journal of Digital Banking*, 4(3), 245-262.

Fornell, C. & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50.

Hair, J.F., Hult, G.T.M., Ringle, C.M. & Sarstedt, M. (2019). *A primer on partial least squares structural equation modeling* (PLS-SEM) (2nd ed.). Sage Publications.

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

Kaspersky. (2021). The rise of zero-day vulnerabilities in mobile banking. *Cybersecurity Insights*, 15(1), 7-9.

Li, X., Zhang, W. & Chen, Y. (2021). The role of blockchain in enhancing mobile banking security. *International Journal of Information Security*, 27(2), 141-156.

McAfee. (2021). Advanced persistent threats (APTs) targeting the financial sector. *McAfee Threat Intelligence Report*, 21(4), 8-13.

Nguyen, D.T., Pham, L.N., & Tran, H.N. (2022). Cybersecurity awareness training: an experimental study. *Journal of Information Security and Applications*, 64, 102994.

Omar, N., Abdullah, M. & Zakaria, Z. (2020). Financial inclusion through mobile banking in Malaysia: Opportunities and challenges. *Journal of Financial Technology*, 6(4), 205-220.

Shmueli, G., Ray, S., Estrada, J.M.V. & Chatla, S.B. (2016). The elephant in the room: Evaluating the predictive performance of PLS models. *Journal of Business Research*, 69(10), 4552-4564.

Tahir, M., Ayub, S. & Yasir, A. (2021). The impact of cybersecurity awareness on the secure use of online banking services. *Journal of Banking and Financial Services*, 27(1), 109-125.

Trend Micro. (2020). Ransomware attacks on banking systems: a global overview. *Trend Micro Security News*, 19(3), 3-5.

Yoon, C. (2021). Cybersecurity practices and awareness: a case study on mobile banking users. *Journal of Information Security*, 10(1), 25-37.