Eduvest – Journal of Universal Studies
Volume 5 Number 8, August, 2025
p- ISSN 2775-3735- e-ISSN 2775-3727

The Influence of Experience, Fear, Awareness of Cyber Attacks on the Acceptance of Banking Technology Moderated by Perceived Benefits in the Development of Digital-Based Banking Services in Indonesia

Ilham Zharfan Satrya
Padjajaran University, Indonesia
Email: ilham23010@mail.unpad.ac.id

ABSTRACT

This study analyzes the influence of experience, fear, and awareness of cyberattacks on the acceptance of banking technology in Indonesia, moderated by perceived benefits. Utilizing a quantitative approach, data were collected through questionnaires distributed to users of digital banking services. The analysis results indicate that both experience and fear of cyberattacks do not significantly affect the acceptance of banking technology, with p-values of 0.414 and 0.199, respectively. In contrast, awareness of cyberattacks has a significant positive effect on the acceptance of banking technology, with a p-value of 0.039. However, perceived benefits did not successfully moderate the relationship between experience and fear of cyberattacks and the acceptance of banking technology, with all p-values exceeding 0.05. These findings suggest that public understanding of cyberattacks can enhance trust and acceptance of banking technology despite the inherent risks. This research provides important insights for the development of digital banking services in Indonesia, emphasizing the need for education on cybersecurity to improve technology acceptance.

KEYWORDS *banking technology, cyberattacks, acceptance, perceived benefits, Indonesia*

INTRODUCTION

Various technological innovations such as the *Internet of Things (IoT)*, *Cloud Computing*, *Artificial Intelligence (AI)*, and *Machine Learning* have brought the world into a new era called the *industrial revolution 4.0*. These technologies have changed the banking industry. These changes can be seen in four components, each contributing to changes in the future banking environment (Diener & Špaček, 2021; Saif-Alyousfi & Alshammari, 2025; Swinburn et al., 2019). Consumers are changing their expectations of banking goods and services. In general, consumers' needs for products and services that are convenient, secure, personalized, trend-setting, and easy to compare have increased as information technology develops. The use of data to improve the quality of products and services (data-enhanced products and services) is notable. The use of large volumes of data, also known as big data, has the ability to provide information that can be used by the banking industry to create many opportunities and develop new types of businesses (Hill, 2021).

The emergence of new working relationships with large companies and startups is significant. Banks can participate in new digital ecosystems that emerge as a result of technological advancements. By collaborating with players in the digital ecosystem, such as fintech and bigtech, banks can acquire new customers, capitalize on partners' innovations, and gain access to data needed to develop products and services. Banks must transform their operational models into digital business models due to advances in information technology

and changes in consumer behavior. Becoming a fully digital bank provides an efficient and effective business model, which is expected to increase the penetration and reach of banks to the entire community, ultimately resulting in increased profitability, inclusion, and welfare (Hill, 2021).

The COVID-19 pandemic has also accelerated changes in the banking industry. It has forced people to change their behavior and shift from the physical economy to the virtual economy. This has resulted in rapid benefits and driven changes in various aspects of people's lives, including digital behaviors such as the way financial transactions are conducted. The needs and expectations as people shift to the digital economy are definitely different from before. At this time, banks are required to accelerate digital transformation, make extraordinary innovations, and work more efficiently, effectively, and productively to meet customer expectations and needs amid increasingly fierce business competition (Hill, 2021).

Overall, global digital transactions increased by 118% from 2017 to 2021, rising from 3.09 trillion USD in 2017 to 6.75 trillion USD in 2021 (Statista, 2021). In Indonesia, digital transaction growth reached an all-time high of 1,556% in the last quarter of 2017–2020. In 2021, electronic currency transactions reached IDR 786.35 trillion. Total revenue this year reached IDR 281.39 trillion, or 55.73%, compared to only IDR 504.96 trillion in the previous year (Bank Indonesia, 2021). According to the Bank Indonesia Report (2021), the value of electronic money (EU) transactions increased by 10.34% (yoy), reaching IDR 116.54 trillion, while the value of digital banking transactions increased by 12.83% (yoy), reaching IDR 15,148.71 trillion. As a result, with 41.84 million users and 29.04 million merchants—mostly MSMEs—the nominal value of QRIS transactions reached Rp 56.92 trillion, an increase of 87.90% (yoy).

Bank Indonesia continues to encourage the digitization of payment systems and collaboration with foreign payment systems to increase understanding of the financial economy and digital currencies. However, it should be noted that the percentage of payments through ATMs, banks, and credit cards only increased by 4.94% (yoy) to Rp 2,041.72 trillion compared to the previous quarter. Nevertheless, modern society is increasingly dependent on digital banking services that can be used anywhere. *Digital Banking Services* differ from conventional banking with digital services such as mobile banking and internet banking. In most cases, digital banking services can perform all banking transactions—such as account opening, transfers, deposits, and account closures—using only a smartphone or electronic device, without the need to visit a bank in person. Additionally, another key difference is that digital-based banking services do not have physical offices (except for head offices) or use limited physical offices (Financial Services Authority Regulation No. 12 of 2021). In contrast, conventional banks usually cannot provide all their services digitally (Hill, 2021).

While Indonesia has a highly digitized economy, several factors hinder the growth of digital banking services in the country. Digital transformation poses challenges that need to be overcome compared to the potential benefits that can be harnessed by the banking industry. Some of these risks include privacy protection risks and data loss, the risk of technology investment not matching business strategy, artificial and cyber intelligence challenges, the need for digitally-oriented institutional risk management, low digital literacy, and underdeveloped information technology infrastructure in Indonesia. As a result, these risks must be minimized alongside the development of digital-based banking services. In the future, this banking transformation will inevitably face specific challenges due to the growth of such

banking and its entire infrastructure (ISACA, 2022).

In the current era of technology and digital disruption, one of the major concerns is the possibility of cyberattacks. It is well recognized that the massive use of information technology increases the risk of cyberattacks, which can lead to leakage or theft of customer data. Banks face several threats when using information technology, including cyberattacks such as cracker or hacker attacks, which can disrupt systems and even steal confidential company data, as well as errors and damage to supporting systems, like power outages. According to data collected by the National Cyber and Crypto Agency (BSSN), phishing and ransomware are some of the most common types of attacks (ISACA, 2022).

Cyberattack surveillance and technology risk are major challenges for digitally-based banking services. While cyberattacks can affect both traditional and virtualized banking, the latter may be more heavily impacted. Virtualized banking services must adopt a fit-for-purpose management approach that balances the convenience and security of digital and mobile applications with data protection, cybersecurity controls, and a highly resilient IT infrastructure. By employing the latest technologies for IT delivery and cyber defense, banks can promote trust and provide innovative, reliable, and secure banking services to their clients. The goal of digital transformation is to deliver products and services that match customer needs or to achieve a customer-centric service orientation (ISACA, 2022).

One example of a current banking cyberattack case in Indonesia is Bank BSI. For several days, all banking transactions by BSI customers experienced significant difficulties. This was very troubling to the public because BSI is the bank with the 7th largest assets in Indonesia. Thus, BSI could not avoid the cyberattack. From May 8, 2023, a number of services at BSI were disrupted, causing some customers' cash flow to stop for several days. Many customers suffered material and moral losses as a result. The bank should actively reassure the public that their funds and data remain safe, as this incident may raise customer concerns about the safety of their funds placed with BSI. A loss of customer confidence due to disruption of services and slow recovery could have long-term impacts on the bank’s reputation and lead to a decline in customers and management (OJK, 2023).

The digital maturity framework suggests four measures for assessing the maturity of organizational digitalization in the customer aspect: customer engagement, which is the dependence or attachment of customers to digital-based banking services; customer experience, which indicates the success of the services provided by the company; and banking understanding, concerning customer behavior, preferences, and needs. To increase financial inclusion, banks must ensure digital-based banking services are accessible to all levels of society. This includes ensuring accessibility for people with disabilities, who may have been marginalized by technological developments (Hill, 2021).

In the research proposed by Lestari et al. (2024), customer experiences of many cyberattacks can increase customer fear, which has great potential to reduce trust and thus minimize customer willingness to use digital-based banking services. However, this negative influence can be moderated by perceived benefits, a variable that helps reduce the negative impact of customer experience on cyberattacks. Similar research by Bajwa et al. (2023) identified a negative influence between cyberattack awareness and customer trust in cyberattack situations. Additional research by Murthy & Gopalkrishnan (2024) found that fear

of cyberattacks negatively impacts customers' use of digital-based banking services. Kaur & Arora's research (2021) explains that risk perception negatively affects one's intention to use digital-based banking services. Conversely, research by Khan et al. (2023) noted a positive influence between cyberattack awareness and customer trust in such situations. Research by Abdul Sathar et al. (2023) revealed that perceived benefits positively affect customer intentions to use digital-based banking services.

Based on previous research, a gap exists in Lestari et al.'s (2024) study, which has not been associated with customer trust to strengthen Murthy & Gopalkrishnan's (2024) findings. In this study, perceived usefulness becomes a moderating variable because of strong evidence from Lestari et al. (2024), Kaur & Arora (2021), and Abdul Sathar et al. (2023), as well as the addition of new variables such as cyberattack awareness. The study replaces customer trust with banking technology acceptance as the dependent variable because this variable incorporates technology in customer decision-making, allowing development of the Technology Acceptance Model, especially at level 3.

Based on these identified problems, this study aims to investigate the influence of cyberattack experience, fear of cyberattacks, and cyberattack awareness on the acceptance of banking technology in the development of digital-based banking services in Indonesia. Specifically, it seeks to determine the extent to which these factors impact technology acceptance and whether perceived usefulness moderates these relationships. The research objectives include examining the effects of cyberattack experience, fear, and awareness on banking technology acceptance, as well as testing the moderating role of perceived benefits in these relationships. By addressing these questions, the study aims to provide insights into how cybersecurity factors and perceived benefits shape the adoption of digital banking services in Indonesia.

The research objectives are as follows: first, to examine the effect of cyberattack experience on banking technology acceptance; second, to assess the impact of fear of cyberattacks on technology acceptance; third, to analyze the influence of cyberattack awareness on technology acceptance. Additionally, the study aims to test whether perceived benefits moderate the relationship between cyberattack experience and technology acceptance, the relationship between fear of cyberattacks and technology acceptance, and the relationship between cyberattack awareness and technology acceptance. Through these objectives, the study seeks to contribute to understanding factors driving or hindering the adoption of digital banking services in Indonesia, particularly in the context of cybersecurity concerns.

The findings of this research will provide valuable insights for banking institutions, policymakers, and cybersecurity experts in Indonesia. By understanding how cyberattack-related factors influence technology acceptance, banks can develop targeted strategies to enhance customer trust and adoption of digital services. Additionally, the study's results can inform the design of cybersecurity awareness campaigns and user education programs to mitigate fears and promote secure banking practices. Ultimately, this research supports the broader goal of fostering a safer and more resilient digital banking ecosystem in Indonesia.

METHOD

Quantitative research was the systematic study of phenomena through measurable data analyzed using statistical, mathematical, or computational techniques. Statistical methods collected quantitative data, and researchers utilized mathematical frameworks and theories to

develop and test hypotheses. Measurement was crucial as it linked empirical observations with mathematical expressions of quantitative relationships (Fadilla et al., 2021).

This study used a causal, ex-post facto quantitative approach to identify cause-and-effect relationships between variables by analyzing current results and their antecedents (Fadilla et al., 2021). The population included Indonesian users of digital banking services who had used them within the past year. Convenience sampling targeted respondents accessible through digital banking platforms, social media, and fintech communities.

Sample size was determined through a statistical power analysis aimed at achieving an 80% chance to detect a true effect with a 5% significance level, considering expected effect sizes. For structural equation modeling (SEM), the sample size was set at a minimum of 200 respondents, following the guideline of 10–20 times the number of model indicators.

Data were collected via Likert-scale questionnaires measuring cyberattack experience, fear, awareness, perceived benefits, and banking technology acceptance. The Likert scale ranged from 1 (Strongly Disagree) to 5 (Strongly Agree), designed to capture variations in participant opinions across six categories, including demographics.

Data analysis involved converting collected data into interpretable information to address research questions. Inferential statistics, both parametric and non-parametric, were used to analyze the data, enabling hypothesis testing and conclusions (Fadilla et al., 2021).

RESULT AND DISCUSSION

Data Analysis Results

Data processing using SEM - PLS uses a 2-step approach. The first step is the Measurement Model / Outer Model and the second is the Structural Model / Inner Model.

Evaluation of Goodness of Fit of the outer model

Outer model analysis is used to ensure that the measurements used are worthy of being considered valid. Convergent Validity, Discriminant Validity, and Composite Reliability are some of the indicators in the outer model analysis. The validity test determines the validity of the research instrument, i.e. the statements in the questionnaire, to measure what it is supposed to measure. A higher validity value indicates that the research is more valid.

- Convergent Validity Testing

  A convergent validity indicator reflective measurement model is assessed based on the correlation between the item or component score and the construct score calculated by PLS, which is used in this study with a loading scale of 0.50.

Table 1. Testing loading factor (outer loading)

Variable	Indicator	*Loading Factor (Outer Loading)*	Description
Cyber Attack Experience (X1)	EX1	0.895	Valid
	EX2	0.819	Valid
	EX3	0.601	Valid
	EX4	0.821	Valid
Fear of Cyber Attack (X2)	FE1	0.823	Valid
	FE2	0.809	Valid

	FE3	0.807	Valid
	FE4	0.940	Valid
Cyber Attack Awareness (X3)	AW1	0.828	Valid
	AW2	0.820	Valid
	AW3	0.842	Valid
	AW4	0.665	Valid
Perceived Benefits (M)	PU1	0.901	Valid
	PU2	0.903	Valid
	PU3	0.923	Valid
	PU4	0.800	Valid
Acceptance of Banking Technology (Y)	ATM1	0.781	Valid
	ATM2	0.775	Valid
	ATM3	0.890	Valid
	ATM4	0.904	Valid

Source: Primary data analysis using SEM-PLS (SmartPLS 4), 2024

In the indicators above, all indicators have an Outer Loading value> 0.5, which means that each indicator used successfully measures the concept to be measured or the indicators are reliable (valid).

- Discriminant Validity Testing

  To evaluate the validity of the indicator's reflective measurement model, cross-loading greater than 0.50 is used to evaluate the construct. If the correlation of the construct with the measurement item is greater than that of other block measures, then the construct predicts the block measure better.

Table 2. Cross loading test

Indicator	Cyber Attack Experience (X1)	Cyber Attack Fear (X2)	Cyber Attack Awareness (X3)	Perceived Benefits (M)	Acceptance of Banking Technology (Y)
EX1	**0.895**	0.116	-0.077	-0.250	-0.189
EX2	**0.819**	0.204	-0.059	-0.207	-0.159
EX3	**0.601**	0.107	-0.011	-0.075	-0.063
EX4	**0.821**	-0.037	-0.115	-0.262	-0.212
FE1	0.160	**0.823**	0.084	0.101	0.046
FE2	0.135	**0.809**	0.097	0.119	0.025
FE3	0.146	**0.807**	0.074	0.139	0.013
FE4	0.039	**0.940**	0.131	0.182	0.092
AW1	-0.065	0.114	**0.828**	0.346	0.283
AW2	-0.051	0.117	**0.820**	0.154	0.254
AW3	-0.120	0.208	**0.842**	0.374	0.296
AW4	-0.061	-0.117	**0.665**	0.095	0.186
PU1	-0.276	0.236	0.328	**0.901**	0.662
PU2	-0.308	0.161	0.250	**0.903**	0.601
PU3	-0.234	0.138	0.328	**0.923**	0.695
PU4	-0.152	0.056	0.234	**0.800**	0.612
ATM1	-0.257	0.086	0.187	0.614	**0.781**
ATM2	-0.097	-0.003	0.212	0.467	**0.775**
ATM3	-0.139	0.114	0.366	0.646	**0.890**
ATM4	-0.215	0.037	0.312	0.693	**0.904**

Source: Data processing results with SmartPLS 4, 2024

The Cross Loading value of each indicator on its own latent variable is higher than other

latent variables, meaning that the indicator is discriminantly valid or the indicator can distinguish one component from another.

Table 3. Testing Fornell Larcker criteria

Variable	Cyber Attack Experience (X1)	Cyber Attack Fear (X2)	Cyber Attack Awareness (X3)	Perceived Benefits (M)	Banking Technology Acceptance (Y)
Cyber Attack Experience (X1)	**0.792**				
Fear of Cyber Attack (X2)	0.104	**0.846**			
Cyber Attack wareness (X3)	-0.096	0.125	**0.792**		
Perceived Benefits (M)	-0.275	0.169	0.325	**0.883**	
Acceptance of Banking Technology (Y)	-0.215	0.074	0.327	0.730	**0.840**

Source: Output of discriminant validity analysis, SmartPLS 4, 2024

The fornell larcker criterion value obtained for each construct is higher than the value of other constructs, which means that it is valid or has good discriminant validity.

- Reliability Testing

  In addition, the reliability value of a structure and the AVE value of each structure can be used to determine its validity and reliability. Construction is considered to have high reliability if the reliability value is 0.70 and the AVE value is above 0.50. Composite Reliability and AVE values for all variables will be presented in Table 4.

Table 4. Composite Reliability and AVE Values

Variable	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
X1 (Pengalaman...)	0.806	0.861	0.868	0.627
X1 * Z	1.000	1.000	1.000	1.000
X2 (Ketakutan...)	0.889	1.287	0.910	0.717
X2 * Z	1.000	1.000	1.000	1.000
X3 (Kesadaran...)	0.802	0.824	0.870	0.628
X3 * Z	1.000	1.000	1.000	1.000
Y (Penerimaan...)	0.860	0.877	0.905	0.705
Z (Prespsi Ma...)	0.905	0.909	0.934	0.780

Source: Converged reliability and validity test results, SmartPLS 4, 2024

Table 5. Testing the average variance extracted (AVE)

Variable	AVE	Description
Cyber Attack Experience (X1)	0.627	Valid

Fear of Cyber Attack (X2)	0.717	Valid
Cyber Attack Awareness (X3)	0.628	Valid
Perceived Benefits (M)	0.780	Valid
Acceptance of Banking Technology (Y)	0.705	Valid

Source: AVE analysis based on the recommendations of Fornell & Larcker (1981), processed with SmartPLS 4

The AVE value of all variables is> 0.5, which means that the variable is able to explain more than 50% of the indicator variance.

Table 6. Composite Reliability Testing

Variable	*Composite Reliability*	Description
Cyber Attack Experience (X1)	0.868	Valid
Fear of Cyber Attack (X2)	0.910	Valid
Cyber Attack Awareness (X3)	0.870	Valid
Perceived Benefits (M)	0.934	Valid
Acceptance of Banking Technology (Y)	0.905	Valid

Source: Composite reliability testing follows the standards of Hair et al. (2017), treated with SmartPLS 4

Composite reliability value of all variables > 0.7, which means that all indicators are quite consistent when measuring the same concept or all constructs are reliable. A reliable construct value indicates more accurate and reliable results.

Table 7. Cronbach's Alpha Testing

Variable	*Cronbach's Alpha*	Description
Cyber Attack Experience (X1)	0.806	Valid
Fear of Cyber Attack (X2)	0.889	Valid
Cyber Attack Awareness (X3)	0.802	Valid
Perceived Benefits (M)	0.905	Valid
Acceptance of Banking Technology (Y)	0.860	Valid

Source: Cronbach's Alpha internal consistency test results, SmartPLS 4, 2024

The Cronbach's Alpha value of all variables is> 0.7, which means that the measurement tool used is reliable / reliable or all variables measured in the study have a good level of consistency.

According to the questionnaire results, this variable has a high reliability value. This is in accordance with the fact that cyberattacks have an impact on the acceptance of modern banking technology in Indonesia.

2 Goddness of Fit evaluation of the inner model

Coefficient of Determination (R2) and Predictive Relevance (Q2) are included in the Inner Model, which is used to ensure that the structural model built is robust and accurate.

- Testing r-square

  To start the model assessment with PLS, each dependent variable's R Square is observed. R-Square values of 0.75, 0.5, and 0.25 indicate that the model is "strong", "moderate", and "weak". The following presents the results of r square in tabular form as follows.

Table 8. R-Square Testing

	R Square	R Square Adjust
Y (Acceptance…	**0.559**	**0.544**

Variable	*R-square*	*Adjusted R-square*
Acceptance of Banking Technology (Y)	0.559	0.554

Source: Determination coefficient (R^2) analysis output, SmartPLS 4, 2024

The r-square and r-square adjusted values for the banking technology acceptance variable are 0.559 and 0.554, respectively. The r-square value of 0.559 explains the percentage of the magnitude of banking technology acceptance can be explained by the variables of cyber attack experience, cyber attack fear, cyber attack awareness, and moderation of perceived benefits by 55.9%. This means that the Banking Technology Acceptance model is in the "moderate" range. The test results of the R-Square value for the banking technology acceptance variable show that it is "moderate". In this case, it is in accordance with field evidence that Variable X has a significant influence on the acceptance of banking technology in Indonesia today. Indonesian people today can still use banking technology if there is still knowledge about cyber attacks.

- Q-square test

  A Q2 value greater than 0 indicates that the model has predictor relevance, while a lower Q2 value indicates that the model does not have predictor relevance.

Table 9. Q- Square Testing

Variable	*q-square*
Acceptance of Banking Technology (Y)	0.363

Source: Results of predictive relevance (Q^2) test based on Stone-Geisser, SmartPLS 4, 2024

The q-square value for the banking technology acceptance variable is 0.363. The higher the q-square value, the better the model or fit. The q-square value of 0.363 explains that the amount of diversity of the data explained by the model is 36.3%. While the remaining 63.7% is explained by other variables outside the model.

It was shown that the construct variables are relevant to the predictor variables and the acceptance of banking technology, based on the questionnaire results and Q-Square test. This is consistent with the research data, which shows that when the general public is aware of cyberattacks, banking technology is well accepted.

Testing path coefficients

Table 10. Results of Path Coefficients

Hypothesis	*Original Sample / O*	*Sample Mean / M*	*Standard Deviation / STDEV*	t-stats [O/STDEV]	p-values
H1: X1 > Y	-0.011	-0.014	0.052	0.218	0.414
H2: X2 > Y	-0.054	-0.050	0.064	0.844	0.199

H3: X3 > Y	0.100	0.111	0.056	1.765	**0.039**
H4: Moderation M Between X1 > Y	0.027	0.020	0.086	0.318	**0.375**
H5: Moderation M Between X2 > Y	0.051	0.043	0.074	0.690	**0.245**
H6: Moderation M Between X3 > Y	0.100	0.088	0.072	1.383	**0.083**

Source: Path analysis with SmartPLS 4, 2024

In testing the above hypotheses, the experience of cyber attacks on the acceptance of banking technology obtained a negative original sample value (O) of -0.011 and p-values = 0.414 > 0.05, so H1: Cyber Attack Experience negatively affects the Acceptance of Banking Technology is rejected. Fear of cyber attacks on the acceptance of banking technology obtained a negative original sample value (O) of -0.054 and p-values = 0.199 > 0.05, so H2: Fear of Cyber Attacks negatively affects the Acceptance of Banking Technology is rejected. Cyber attack awareness on banking technology acceptance obtained a positive original sample value (O) of 0.100 and p-values = 0.039 <0.05, so H3: Cyber Attack Awareness has a positive effect on Banking Technology Acceptance is accepted. Perceived benefits as moderation between cyber attack experience and banking technology acceptance, the original sample value (O) is positive at 0.027 and p-values = 0.375> 0.05, so H4: Perceived Benefits can moderate the influence between Cyber Attack Experience on Banking Technology Acceptance is rejected. Perceived benefits as moderation between the fear of cyber attacks on the acceptance of banking technology, the original sample value (O) is positive by 0.051 and p-values = 0.245 > 0.05, so H5: Perceived Benefits can moderate the influence between Fear of Cyber Attacks on Acceptance of Banking Technology is rejected. Perceived benefits as moderation between cyberattack awareness and banking technology acceptance, the original sample value (O) is positive at 0.100 and p-values = 0.083 > 0.05, so H6: Perceived Benefits can moderate the influence between Cyber Attack Awareness on Banking Technology Acceptance is rejected.

Of the three direct effect test results, there is one hypothesis that has a significant effect. Namely on the variable Cyber Attack Awareness > Acceptance of Banking Technology. Where when the research was conducted, there were still many general public who had knowledge about cyber attacks including how to prevent cyber attacks, this caused the community to still accept banking technology in Indonesia today. From the results of the moderation test, it can be seen that perceived benefits cannot significantly moderate cyber attacks on the acceptance of banking technology. It is stated that perceived benefits do not have a sufficiently active role in the acceptance of banking technology in the midst of cyber attacks. At present, many people still accept banking technology, so there is no need for perceived benefits to strengthen the acceptance of banking technology amid cyber attacks. Which is where the acceptance of banking technology will arise if there is an understanding of cyber attacks and their current prevention.

This study has six hypotheses, and each hypothesis will be discussed separately based

on research data processed using SEM-Smart PLS, as mentioned in chapter II.

The Effect of Cyber Attack Experience on Acceptance of Banking Technology

The cyber attack experience on the acceptance of banking technology obtained a negative original sample value (O) of -0.011 and p-values = 0.414> 0.05, then H1: Cyber Attack Experience negatively affects Banking Technology Acceptance is rejected. Thus, it can be said that the cyber attack experience cannot have a significant effect on the acceptance of banking technology in the development of digital-based banking services in Indonesia.

This result is certainly in accordance with the model used in this study, namely TAM 3, namely direct experience with cyber attacks makes a person reluctant to accept digital-based banking services or vice versa. These experiences include hacking, malicious links, and so on. This proves that the acceptance of banking technology is significantly negatively affected by the experience of cyber attacks. This is because many customers and other public audiences understand cyber-attacks and their prevention nowadays. Thus, it is easy to avoid and prevent common cyber attacks. Therefore, the experience of cyber attacks rarely occurs and does not have a significant effect on the acceptance of banking technology.

Based on current facts, many general public can easily obtain information about cyber attacks from various media such as social media and so on, even in digital-based banking applications are currently equipped with information about cyber attacks and their prevention. This is what makes the community able to understand and avoid cyber attacks easily. Thus, the experience of cyber attacks does not have any impact on the acceptance of current banking technology.

This research is also in line with the research of Lestari et al (2024) which identifies that the experience of cyber attacks negatively affects customer trust in using banking technology.

The Effect of Fear of Cyber Attacks on Acceptance of Banking Technology

The fear of cyber attacks on the acceptance of banking technology obtained a negative original sample value (O) of -0.054 and p-values = 0.199> 0.05, so H2: Fear of Cyber Attacks has a negative effect on Acceptance of Banking Technology is rejected. So, it can be said that the fear of cyber attacks cannot have a significant effect on the acceptance of banking technology in the development of digital-based banking services in Indonesia.

This result is certainly in accordance with the model used in this study, namely TAM 3, namely the fear of cyber attacks makes a person reluctant to accept digital- based banking services or vice versa. These fears include worrying if sensitive data is stolen, losing money, and so on. This proves that the acceptance of banking technology is significantly negatively affected by the fear of cyber attacks. This happens because many customers and other public audiences easily find information spread about cyber attacks in various media and places and are easy to understand. Thus, the fear of cyber attacks will disappear. Therefore, the fear of cyber attacks does not have a significant effect on the acceptance of banking technology.

Based on current facts, many general public can easily obtain information about cyber attacks from various media such as social media and so on, even in digital-based banking applications are currently equipped with information about cyber attacks and their prevention. This is what makes the community able to eliminate the fear of cyber attacks today. Thus, even

the fear of cyber attacks does not have any impact on the acceptance of current banking technology.

This research is also in line with Murthy & Gopalkrishnan's research (2024) which identifies that the fear of cyber attacks negatively affects customer confidence in using banking technology.

The Effect of Cyber Attack Awareness on Banking Technology Acceptance

Cyber attack awareness on the acceptance of banking technology obtained a positive original sample value (O) of 0.100 and p-values = 0.039 <0.05, so H3: Cyber Attack Awareness has a positive effect on Banking Technology Acceptance is accepted. So, it can be said that cyber attack awareness can have a significant effect on the acceptance of banking technology in the development of digital-based banking services in Indonesia.

This result is certainly in accordance with the model used in this study, namely TAM 3, namely awareness of cyber attacks makes someone still accept digital-based banking services. This awareness is in the form of knowledge about the types of cyber attacks, prevention of these attacks, and so on. This proves that the acceptance of banking technology is influenced by cyber attack awareness. This happens because many customers and other public audiences easily find information spread about cyber attacks in various media and places and are easy to understand. Thus, awareness of cyber attacks is getting stronger and higher. Therefore, cyber attack awareness has a significant effect on the acceptance of banking technology.

Based on current facts, many general public can easily obtain information about cyber attacks from various media such as social media and so on, even in digital-based banking applications are currently equipped with information about cyber attacks and their prevention. This is what makes the community able to easily understand and realize about current cyber attacks. Thus, even this cyber attack awareness has any impact on the acceptance of current banking technology.

This research is also in line with the research of Khan et al (2023) which identified that cyberattack awareness positively affects customer confidence in using banking technology.

1. Moderation of Perceived Benefits on the Effect of Cyber Attack Experience on Banking Technology Acceptance

   Perceived benefits as moderation between cyber attack experience on banking technology acceptance, the original sample value (O) is positive value of 0.027 and p-values = 0.375> 0.05, so H4: Perceived Benefits can moderate the influence between Cyber Attack Experience on Banking Technology Acceptance is rejected. So, it can be said that perceived benefits cannot have a significant effect on the effect of cyber attack experience on banking technology acceptance on the development of digital-based banking services in Indonesia.

   This result certainly does not contradict the model used in this study, namely TAM 3, namely perceived benefits moderate direct experience with cyber attacks on decisions to accept current banking technology. The perceived benefits are in the form of easy, fast, practical and value-added services. This proves that perceived benefits have no significant effect. This happens because many customers and other public audiences still accept this technology so there is no need for the perception of benefits in using these technology services. The current acceptance of this technology is due to the large number of people who understand and get information about cyber attacks from anywhere. Thus,

perceived benefits do not have an active role in moderating this influence.

Based on current facts, many general public still accept banking technology as a result of easily obtaining information about cyber attacks from various media such as social media and so on, even in digital-based banking applications are currently equipped with information about cyber attacks and their prevention. This is what makes the perception of benefits unnecessary in strengthening the acceptance of banking technology. Thus, even this perceived benefit does not have any impact on the effect of cyber attack experience on the acceptance of current banking technology.

This research is also in line with the research of Lestari et al (2024) and Abdul Sathar et al (2023) which identified that perceived benefits significantly affect the influence of cyber attacks in using banking technology.

2. Moderation of Perceived Benefits on the Effect of Fear of Cyberattacks on Acceptance of Banking Technology

Perceived benefits as moderation between the fear of cyber attacks on the acceptance of banking technology obtained the original sample value (O) is positive value of 0.051 and p-values = 0.245> 0.05, so H5: Perceived Benefits can moderate the influence between Fear of Cyber Attacks on Acceptance of Banking Technology is rejected. So, this can be said that the perception of benefits cannot have a significant effect on the effect of fear of cyber attacks on the acceptance of banking technology on the development of digital-based banking services in Indonesia.

This result certainly does not contradict the model used in this study, namely TAM 3, namely perceived benefits moderate the fear of cyber attacks on decisions to accept current banking technology. The perceived benefits are in the form of easy, fast, practical and value-added services. This proves that perceived benefits have no significant effect. This happens because many customers and other public audiences still accept this technology so there is no need for the perception of benefits in using these technology services. The current acceptance of this technology is due to the large number of people who understand and get information about cyber attacks from anywhere. Thus, perceived benefits do not have an active role in moderating this influence.

Based on current facts, many general public still accept banking technology as a result of easily obtaining information about cyber attacks from various media such as social media and so on, even in digital-based banking applications are currently equipped with information about cyber attacks and their prevention. This is what makes the perception of benefits unnecessary in strengthening the acceptance of banking technology. Thus, even this perceived benefit does not have any impact on the effect of fear of cyber attacks on the acceptance of current banking technology.

This research is also in line with the research of Abdul Sathar et al (2023) which identified that perceived benefits significantly influence the influence of cyber attacks in using banking technology.

3. Moderation of Perceived Benefits on the Effect of Cyber Attack Awareness on Banking Technology Acceptance

Perceived benefits as moderation between cyber attack awareness on banking technology acceptance, the original sample value (O) is positive at 0.100 and p-values = 0.083> 0.05, so H6: Perceived Benefits can moderate the influence between Cyber Attack Awareness on Banking Technology Acceptance is rejected. So, it can be said that perceived benefits cannot have a significant effect on the effect of cyber attack awareness on banking technology acceptance on the development of digital-based banking services in Indonesia.

This result certainly does not contradict the model used in this study, namely TAM 3, namely perceived benefits moderate awareness of cyber attacks on decisions to accept current banking technology. The perceived benefits are in the form of easy, fast, practical and value-added services. This proves that perceived benefits have no significant effect. This happens because many customers and other public audiences still accept this technology so there is no need for the perception of benefits in using these technology services. The current acceptance of this technology is due to the large number of people who understand and get information about cyber attacks from anywhere. Thus, perceived benefits do not have an active role in moderating this influence.

Based on current facts, many general public still accept banking technology as a result of easily obtaining information about cyber attacks from various media such as social media and so on, even in digital-based banking applications are currently equipped with information about cyber attacks and their prevention. This is what makes the perception of benefits unnecessary in strengthening the acceptance of banking technology. Thus, even this perceived benefit does not have any impact on the effect of cyber attack awareness on the acceptance of current banking technology.

This research is also in line with the research of Abdul Sathar et al (2023) which identified that perceived benefits significantly influence the influence of cyber attacks in using banking technology.

CONCLUSION

The research concluded that while the experience of cyberattacks and fear of cyberattacks did not significantly influence the acceptance of banking technology in Indonesia, awareness of cyberattacks had a positive and significant impact on acceptance. Perceived usefulness was not found to significantly moderate the relationships between experience, fear, or awareness of cyberattacks and technology acceptance. These findings suggest that greater access to and understanding of cyberattack information enhances users' comfort and trust in digital banking. To improve adoption, banks and fintechs should prioritize cybersecurity education and transparency, while the government can support with national digital literacy programs and strengthened regulations, especially targeting vulnerable groups. Future research is recommended to investigate how perceptions of cybersecurity vary across demographic or regional segments and to explore other potential moderators like institutional trust or social influences, fostering more inclusive and sustained growth in Indonesia's digital banking sector.

REFERENCES

Abdul Sathar, M. B., Rajagopalan, M., Naina, S. M., & Parayitam, S. (2023). A moderated-mediation model of perceived enjoyment, security and trust on customer satisfaction: evidence from banking industry in India. Journal of Asia Business Studies, 17(3), 656-

679. https://doi.org/10.1108/JABS-03-2022-0089

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. Information and Computer Security, 31(5), 635-654. https://doi.org/10.1108/ICS-11-2022-0179

Bank Indonesia. (2021). Digital Banking Transaction Chart.

Diener, F., & Špaček, M. (2021). Digital transformation in banking: A managerial perspective on barriers to change. *Sustainability*, *13*(4), 2032.

Fadilla, Z., Ketut Ngurah Ardiawan, M., Eka Sari Karimuddin Abdullah, M., Jannah Ummul Aiman, M., & Hasda, S. (2021). Quantitative research methodology.

http://penerbitzaini.com

Hill, -Napoleon. (2021). Blueprint for digital banking transformation. Financial Services Authority. https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Cetak-Biru-Transformasi-Digital-Perbankan/CETAK%20BIRU%20TRANSFORMASI%20DIGITAL%20PERBANKAN%20(SHORT%20VERSION).pdf

ISACA. (2022). Cybersecurity and Technology Risk in Virtual Banking. https://engage.isaca.org/

Kaur, S., & Arora, S. (2021). Role of perceived risk in online banking and its impact on behavioral intention: trust as a moderator. Journal of Asia Business Studies, 15(1), 1-30. https://doi.org/10.1108/JABS-08-2019-0252

Khan, H. U. A., Khalil, S. F. A., Kazmi, S. J. H., Umar, M., Shahzad, A., & Farhan, S. Bin. (2017). Identification Of River Bank Erosion And Inundation Hazard Zones Using Geospatial Techniques - A Case Study Of Indus River Near Layyah District, Punjab, Pakistan. Geoplanning:

Journal of Geomatics and Planning, 4(2), 121. https://doi.org/10.14710/geoplanning.4.2.121-130

Khan, N. F., Ikram, N., Murtaza, H., & Asadi, M. A. (2023). Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach. Kybernetes, 52(1), 401-421. https://doi.org/10.1108/K-05-2021-0377

Krishna, B., Krishnan, S., & Sebastian, M. P. (2023). Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective. Information Technology and People. https://doi.org/10.1108/ITP-05-2023-0434

Lestari, S., Adawiyah, W. R., Alhamidi, A. L., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. Safer Communities. https://doi.org/10.1108/SC-04-2024-0018

Murthy, N., & Gopalkrishnan, S. (2024). Exploiting fear and vulnerabilities of senior citizens: are regulatory changes required to prevent digital frauds? Working with Older People, 28(1), 84-95. https://doi.org/10.1108/WWOP-06-2023-0021

Nain Sharma, K., & Kala, A. (2022). ENVISION-International Journal of Commerce and Management Online Banking Frauds and Necessary Preventive Measures. https://journalsacfa.apeejay.edu/

OJK (2021). Consultative Paper on Cybersecurity Risk Management of Commercial Banks.

OJK. (2023). Financial services authority of the republic of Indonesia.

Saif-Alyousfi, A. Y. H., & Alshammari, T. R. (2025). Environmental sustainability and climate change: an emerging concern in banking sectors. *Sustainability*, *17*(3), 1040.

Statista. (2021). Digital Banking Transaction Chart.

Swinburn, B. A., Kraak, V. I., Allender, S., Atkins, V. J., Baker, P. I., Bogard, J. R., Brinsden, H., Calvillo, A., De Schutter, O., & Devarajan, R. (2019). The global syndemic of obesity, undernutrition, and climate change: the Lancet Commission report. *The lancet*, *393*(10173), 791–846.