Financial cybercrime avoidance behavior among employees of financial sector companies in Indonesia

Hanifah Zahra*, Dekar Urumsah

Universitas Islam Indonesia, Sleman Regency, Special Region of Yogyakarta, Indonesia

ARTICLE INFO

Article history
Received June 18, 2024
Revised October 17, 2024
Accepted November 6, 2024

JEL Classification:
M41

Key words:
Avoidance behavior,
Avoidance motivation,
Financial cybercrime.

DOI:
10.14414/tiar.v14i2.4596

ABSTRACT

This study aims to examine the factors that influence the behavior of avoiding financial cybercrime among employees of financial sector companies in Indonesia. This studyuses Technology Threat Avoidance Theory (TTAT) and Regret Theory as theoretical frameworks. Data are collected through a survey conducted onemployees of financial sector companies in Indonesia, both in paper-based and online formats, resulting in a total of 180 questionnaires for analyses. Data analysis is conducted using Structural Equation Modeling-Partial Least Squares (SEM-PLS) in SmartPLS 4.0. The results of this study show thatperceived susceptibility and perceived severity have a significant positive influence on perceived threat. However, the interaction between perceived susceptibility and perceived severity has no effect on perceived threat. Perceived threat, safeguard effectiveness, and anticipated regret have a significant influence on financial cybercrime avoidance motivation. Conversely, self-efficacy and safeguard cost do not have an effect onfinancial cybercrime avoidance motivation. Furthermore, financial cybercrime avoidance motivation has a significant and positive influence on financial cybercrime avoidance behavior. These findings offer insights for policymakers, financial sector companies, and antivirus software developers to enhance cybersecurity policies, responses to cybercrime, and software features.

ABSTRAK

Penelitian ini bertujuan untuk menguji faktor-faktor yang mempengaruhi perilaku penghindaran kejahatan siber keuangan oleh pekerja sektor keuangan di Indonesia. Penelitian ini menggunakan Teori Penghindaran Ancaman Teknologi (TTAT) dan Teori Penyesalan sebagai kerangka teorinya. Data dikumpulkan melalui survei, baik secara langsung (berbasis kertas) maupun tidak langsung (berbasis online menggunakan formulir google), terhadap pegawai sektor keuangan di Indonesia, sehingga menghasilkan total 180 kuesioner untuk dianalisis. Structural Equation Modeling-Partial Least Squares (SEM-PLS) di SmartPLS 4.0 digunakan untuk analisis data. Hasil penelitian menunjukkan bahwa Perceived Susceptibility dan Perceived Severity mempunyai pengaruh positif signifikan terhadap Perceived Threat. Namun tidak terdapat pengaruh interaksi antara Perceived Susceptibility dan Perceived Severity terhadap Perceived Threat. Persepsi Ancaman, Efektivitas Perlindungan, dan Penyesalan yang Diantisipasi berpengaruh signifikan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Sebaliknya Self-Efficacy dan Safeguard Cost tidak berpengaruh terhadap motivasi tersebut. Selanjutnya, Motivasi Penghindaran Kejahatan Siber Keuangan berpengaruh secara signifikan dan positif terhadap Perilaku Penghindaran Kejahatan Siber Keuangan. Temuan ini memberikan wawasan bagi para pembuat kebijakan, perusahaan sektor keuangan, dan pengembang perangkat lunak anti-virus untuk meningkatkan kebijakan keamanan siber, respons terhadap kejahatan siber, dan fitur-fitur perangkat lunak keamanan siber.

* Corresponding author, email address: hanifah.zahra@uii.ac.id

1. INTRODUCTION

The increasing prevalence of cybercrime in Indonesia lately has raised concerns among many parties. The National Cyber and Crypto Agency (BSSN) of the Republic of Indonesia stated that more than 700 million cyberattacks occurred in the country in 2022. The most common types of cyberattacks are ransomware and malware because these attacks usually involve ransom demands. Meanwhile, phishing and exploitation are in second and third place. This spike in cybercrime is in line with the increasing use of the internet among the Indonesian people. Based on a digital 2022 report presented by *We Are Social* Hootsuite, Indonesia has 204.7 million internet users, or 73.7% of the total population. Most users access the internet via mobile phones and computers and spend an average of approximately 8 hours and 36 minutes online. Given the very widespread adoption of the internet, Indonesia's cybersecurity needs to be improved. According to the 2022 NCSI report, Indonesia is ranked 84th out of 161 countries in cybersecurity, with a score of 38.96 out of 100, highlighting significant challenges in this domain.

This inadequate level of cybersecurity poses difficulties for businesses that have adopted digital transformation. One of the efforts made to overcome the obstacles they face is the need for more effective data security improvements to protect stakeholder and company information (Gupta et al., 2020). According to PWC's 2022 Global Economic Crime and Fraud Survey, cybercrime is the top threat to organizations of all sizes, followed by customer fraud and asset misappropriation. The survey also shows a shift in fraud patterns, with the top threats coming from external sources outside of a company's control. Globally, 43% of fraud perpetrators are external entities, 31% are internal actors, and 26% are the result of collusion between the two. External entity-based fraud accounts for about 33% of hacking incidents, with 28% of cybercrime being orchestrated (PwC, 2022).

In 2022, the largest share of cyberattacks targeted the manufacturing sector (23.2%), followed by the financial sector (22.4%), business services (12.7%), energy (8.2%), trade (7.3%), healthcare (5.1%), transportation (4%), government (2.8%), education (2.8%), and media (2.5%) (IBM, 2022). IBM also indicated that 95% of successful cyberattacks stemmed from human error, with 19 out of 20 online breaches due to human negligence. Common human errors encompass downloading infected software, using weak passwords, and neglecting software updates. As people's reliance on the internet continues to swell, the potential for hacking and other security breaches also rises consistently (Liang & Xue, 2010). This underscores the importance of researching cybersecurity avoidance behavior, particularly in the financial sector.

Previous studies on cybercrime avoidance behavior have predominantly adopted the Technology Threat Avoidance Theory (TTAT) and Protection Motivation Theory (PMT), often concentrating on evading phishing attacks. The Technology Threat Avoidance Theory has been utilized by Gillam and Foster, (2020); Mark et al., (2021); Saidi and Prayudi, (2021); Sylvester, (2022); and Verkijika, (2019). Meanwhile, the Protection Motivation Theory has been employed by Bax et al. (2021) and Tang et al. (2021).

This study uses the TTAT framework with the constructs of perceived susceptibility, perceived severity, threat perception, self-efficacy, safeguard cost, and motivation to avoid financial cybercrime as factors influencing cybercrime avoidance behavior. This study places more emphasis on using Technology Threat Avoidance Theory (TTAT) than Protection Motivation Theory (PMT), because this study emphasizes the technical aspects of cybersecurity, especially how individuals avoid and address financial cybercrime. In addition to using TTAT, this study also expands the research model by incorporating the construct of anticipated regret, which was formulated from the regret theory by Loomes and Sugden (1982), into the framework. The addition of this construct is based on the regret theory which states that in every decision made by an individual there is an element of regret. In terms of avoiding financial cybercrime, anticipated regret can influence financial sector employees to be more cautious when facing threats. Anticipated regret will make individuals consider how they will feel if they fail to take proper precautions and then become victims of crime (Shih & Schau, 2011). Anticipated regret can strengthen a person's intention to seriously avoid a threat because everyone wants to avoid feelings of regret in the future. This emotional response can increase motivation to take proactive steps in preventing a threat. Understanding and utilizing psychological factors, such as anticipated regret, is essential to creating effective risk management strategies. It helps in designing interventions that resonate with people, leading to better adoption of protective behaviors, such as using antivirus software or engaging in cybersecurity education. This approach not only strengthens the intention to avoid threats, but also ensures a more comprehensive and behaviorally based strategy to protect the financial system from cyber threats. This study is very interesting, especially in Indonesia, because it is relatively rare.

Previous studies conducted by Bax et al. (2021); Mark et al. (2021); Saidi and Prayudi (2021); Sylvester (2022); and Verkijika (2019) have shown inconsistent results for each of their respective variables. This inconsistency suggests the need for further investigation and validation.

2. THEORETICAL FRAMEWORK AND HYPOTHESES

Technology Threat Avoidance Theory

The Technology Threat Avoidance Theory (TTAT) developed by Liang & Xue (2009) elucidates how individuals respond to network protection by avoiding potential threats to their networks or computers. It integrates several existing theoretical frameworks, including cybernetics theory (Wiener, 1948), coping theory (Lazarus, 1966), protection motivation theory (Rogers, 1975), health belief model (Janz & Becker, 1984), and risk analysis research model (Baskerville, 1991).

Specifically, TTAT states that people's perception of cyber threats stems from their assessment of a particular threat's severity and susceptibility to cybercrime. Given this perceived threat, individuals will evaluate their ability to ward off threats by considering their confidence in the effectiveness of cybercrime protection, the overall effort required to implement protective measures, and their capacity to implement protective measures. This assessment will increase motivation to avoid cybercrime and encourage individuals to choose to engage in behaviors aimed at avoiding cyber threats.

Regret Theory

Regret theory is an economic model developed by Bell (1982); Fishburn (1982); and Loomes & Sugden (1982). This theory explains regret under uncertainty by considering the effects of anticipated regret. Regret theory is built on two assumptions. First, individuals tend to compare the outcomes of their chosen decisions with the outcomes they will receive if they make different choices (Bell, 1982; Loomes & Sugden, 1982). Second, individuals tend to anticipate regret before making decisions, often altering their choices to avoid potential regret. Anticipated regret can also be understood as regret of action or regret of inaction. Regret of action involves the regret resulting from engaging in specific behaviors, while regret of inaction arises from an individual's failure to engage in specific behaviors (Brewer et al., 2016). According to Sukamulja et al. (2019), anticipated regret emerges when the outcome of a process that has undergone planning does not align with expectations.

Financial Cybercrime

Cybercrime refers to criminal activities carried out through the internet network. It can also be defined as the deliberate exploitation of computer systems, technology-dependent companies, and networks (Jenab & Moslehpour, 2016). Some literature defines cybercrime as actions synonymous with computer crime. According to the U.S. Department of Justice, computer crime is an illegal act requiring computer technology knowledge for its commission, investigation, and prosecution. Meanwhile, according to the Organization for Economic Cooperation and Development (OECD), computer crime encompasses illegal, unethical, or unauthorized actions related to automated data processing and/or data transmission.

Financial cybercrime, as referred to in this study, involves criminal activities within computer-based systems or internet networks aimed at manipulating financial information or targeting victims' money as the primary objective, resulting in financial losses. Cyberattacks on the financial services and banking sector in Indonesia take various forms or modes of crime (Suwiknyo et al., 2021). These forms of cybercrime are carding, cyber extortion, adware, one-time password (OTP) scams, fake link fraud, and android application kit (APK) message scams.

Avoidance Behavior

Avoidance behavior is a widespread reaction to situations infused with strong emotions, typically linked with anxiety or fear. It can also be characterized as any effort to elude or distance oneself from particular thoughts or emotions (Baker et al., 2016). Given these interpretations, avoidance behavior refers to actions frequently adopted by individuals to evade certain circumstances. Therefore, financial cybercrime avoidance behavior can be understood as actions routinely undertaken by individuals to safeguard themselves from becoming victims of financial cybercrime.

The Influence of Perceived Susceptibility on Perceived Threat

Perceived susceptibility refers to an individual's belief about his or her vulnerability to becoming a victim of cyberattack. This belief will motivate to adopt more proactive behaviors to safeguard his or her cyber security (Liang & Xue, 2010). When technology users are aware of their vulnerabilities, they are more likely to view cybercrime as a significant threat. The results of research conducted by Arachchilage et al. (2016) and Gillam & Foster (2020) show that perceived susceptibility positively impacts perceived threat. Therefore, the first hypothesis proposed is as follows:

H_1: Perceived susceptibility has a positive influence on perceived threat.

The Influence of Perceived Severity on Perceived Threat

Perceived severity refers to an individual's belief about the seriousness of a potential threat. This can motivate the individual to take certain precautions. When an individual perceives a higher level of severity towards a threat, he or she is more likely to engage in behaviors aimed at avoiding the threat (Kasmaei et al., 2014). In terms of financial cybercrime avoidance, if technology users perceive financial cybercrime as a serious crime, they will view it as a significant threat. The results of studies conducted by Mark et al. (2021) and Sylvester (2022) show that perceived severity has a positive effect on perceived threat. Therefore, the second hypothesis proposed is as follows:

H_2: Perceived severity has a positive influence on perceived threat.

The Influence of the Interaction between Perceived Susceptibility and Perceived Severity on Perceived Threat

Perceived threat is also influenced by the interaction between perceived susceptibility and perceived severity (Liang & Xue, 2009). When individuals feel vulnerable to being a victim of financial cybercrime, they are more likely to perceive the consequences as serious. Conversely, when they perceive the potential consequences as serious, they may also feel more susceptible to the threat. These simultaneous beliefs about susceptibility and severity contribute to the increased perceived threat associated with financial cybercrime. The results of studies conducted by Mark et al. (2021) and Sylvester (2022) show that both perceived susceptibility and perceived severity have a significant influence on perceived threat. Therefore, the third hypothesis is as follows:

H_3: The interaction between perceived susceptibility and perceived severity has a positive influence on perceived threat.

The Influence of Perceived Threat on Financial Cybercrime Avoidance Motivation

Perceived threat is defined as a difficult or distressing situation for an individual (Bennett & Galpert, 1992). In the context of financial cybercrime, when individuals perceive themselves to be at risk of being victimized, they are more likely to be motivated to take action to avoid the threat. The results of a study conducted by Mark et al. (2021) show that perceived threat has a positive effect on the motivation to avoid phishing threats. Therefore, the fourth hypothesis proposed is as follows:

H_4: Perceived threat has a positive influence on financial cybercrime avoidance motivation.

The Influence of Self-Efficacy on Financial Cybercrime Avoidance Motivation

Self-efficacy refers to an individual's belief in his or her ability to take security-related actions (Liang & Xue, 2010). This belief can serve as a key motivator for an individual to take action and avoid undesirable outcomes, such as cybercrime. The higher a person's self-efficacy, the more motivated the person is to engage in cybercrime prevention behavior. The results of research conducted by Butler (2020); Gillam and Foster (2020); and Mark et al. (2021) show that self-efficacy has a positive effect on the motivation to avoid information technology crimes. Therefore, the fifth hypothesis proposed is as follows:

H_5: Self-efficacy has a positive influence on financial cybercrime avoidance motivation.

The Influence of Safeguard Effectiveness on Financial Cybercrime Avoidance Motivation

Safeguard effectiveness is defined as an individual's assessment of security measures regarding how effectively they can be implemented to avoid malicious IT threats (Liang & Xue, 2010). In this study, safeguard effectiveness is considered to be running well if it can minimize vulnerability to financial cybercrime attacks. Protection measures that can be used to prevent financial cybercrime include the use of security software such as antivirus, anti-malware, anti-ransomware, and anti-spyware. The results of research conducted by Arachchilage et al. (2016) and Butler (2020) show that protection effectiveness influences motivation to avoid cybercrimes. Therefore, the sixth hypothesis proposed is as follows:

H_6: Safeguard effectiveness has a positive influence on financial cybercrime avoidance motivation.

The Influence of Safeguard Cost on Financial Cybercrime Avoidance Motivation

Safeguard costs are defined as the physical and cognitive efforts required, such as time, money, discomfort, and understanding, when implementing security measures (Liang & Xue, 2009). In this study, safeguard costs specifically relate to the efforts needed to install and maintain security software, such as antivirus, for protection against financial cybercrime. The greater the effort or resources required to use these security tools, the lower the motivation to engage in cybercrime avoidance. The results of research conducted by Butler (2020) show that cost considerations influence avoidance behavior. However, the results of a study conducted by Arachchilage et al. (2016) show that safeguard cost has no effect on motivation to avoid financial cybercrime. Therefore, the seventh hypothesis proposed is as follows:

H_7: Safeguard cost has a negative influence on financial cybercrime avoidance motivation.

The Influence of Anticipated Regret on Financial Cybercrime Avoidance Motivation

Anticipated regret is defined as the negative emotional response individuals experience when they compare the expected outcomes of not taking action with the potential consequences of taking action (Xiling et al., 2018). In terms of motivation to avoid financial cybercrime, when someone is faced with the threat of financial cybercrime, he will regret it if he does not take the decision to protect himself from the threat. The results of research conducted by Verkijika (2019) show that anticipated regret positively influences motivation to avoid financial cybercrime. Therefore, the seventh hypothesis proposed is as follows:

H_8: Anticipated regret has a positive influence on financial cybercrime avoidance motivation.

The Influence of Financial Cybercrime Avoidance Motivation on Financial Cybercrime Avoidance Behavior

Financial cybercrime avoidance motivation is the motivation that drives IT users to protect against IT threats through security measures (Liang & Xue, 2010). Those who are highly motivated to avoid cybercrime in the financial sector will take action to protect themselves from these threats. The results of studies conducted by Butler (2020); Gillam and Foster (2020); Mark et al. (2021); and Verkijika (2019) consistently show that motivation for avoidance has a positive influence on cybercrime avoidance behavior. Therefore, the eighth hypothesis proposed is as follows:

H_9: Financial cybercrime avoidance motivation has a positive influence on financial cybercrime avoidance behavior.

3. RESEARCH METHOD

This quantitative study uses primary data. The population of this study is employees of financial sector companies in Indonesia. The sample used in the study includes 180 employees of financial sector companies in Indonesia who use electronic devices in their work. The sample size is determined using the Hair formula since the exact population size is unknown. Sampling is conducted using convenience sampling technique. Data for this study is distributed through both offline questionnaires (paper-based) and online questionnaires (via Google Forms). Using both offline and online questionnaires allows for a broader reach of potential respondents. Some individuals prefer or have easier access to paper-based questionnaires (offline), while others may find it more convenient to respond online. The data used in this study are measured using a Likert scale ranging from 1 (strongly disagree) to 6 (strongly agree).

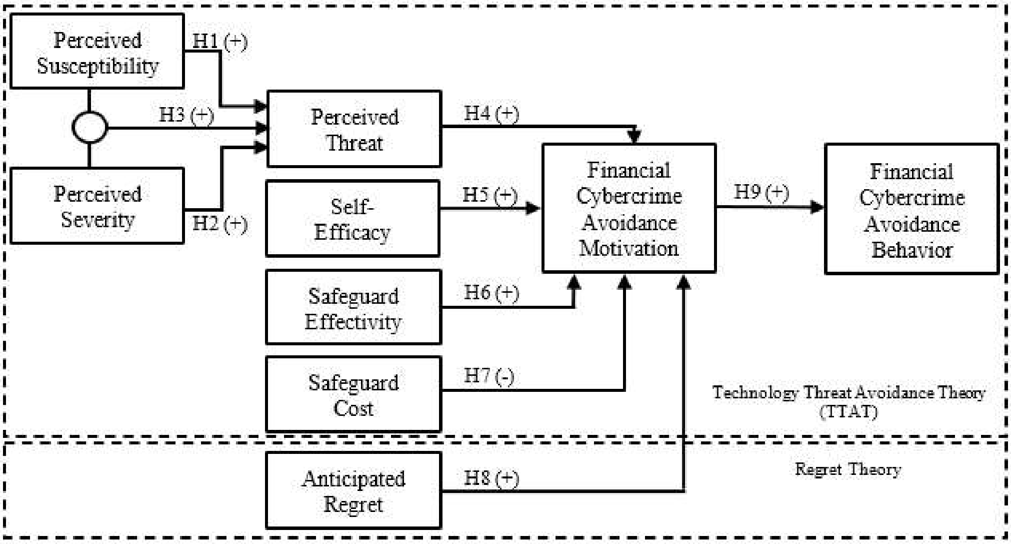

Figure 1
Research Model

Data analysis is carried out using the Structural Equation Modeling (SEM) - Partial Least Squares (PLS) method with SmartPLS software. The analysis includes measurement model analysis and path analysis. The variables examined are perceived susceptibility using 3 question items from Liang and Xue (2009); perceived severity using 3 question items from Liang and Xue (2009); perceived threat using 4 question items from Liang and Xue (2009); self-efficacy using 4 question items from Liang and Xue (2009) and Verkijika (2019); safeguard effectivity using 3 question items from Liang and Xue (2009); safeguard cost using 4 question items from Liang and Xue (2009); anticipated regret using 3 question items from Verkijika (2019); financial cybercrime avoidance motivation using 4 question items from Liang and Xue (2009); and financial cybercrime avoidance behavior using 6 question items from Liang and Xue (2009) & Verkijika (2019).

4. DATA ANALYSIS AND DISCUSSION

Respondents Demographics

Data collection is conducted through both offline and online questionnaires. This study involves 180 respondents consisting of 37 respondents with offline questionnaires and 143 respondents with online questionnaires which are eligible for analysis. The gender distribution among respondents consists of 52% male and 48% female. All participants work in the financial sector, with the following breakdown: 48% in banking companies, 14% in insurance companies, 12% in financing companies, 8% in securities companies, 2% in savings and loan cooperatives, 1% in pawnshops, and 15% in other financial sector companies. Most respondents (42%) work in Jakarta area, 31% work in Yogyakarta area, and 27% work in other regions. Furthermore, all participants use electronic devices for their work, with a note that 38% of respondents (68 people) reported having been victims of financial cybercrime.

Validity Test

Table 1 shows that all indicator variables have outer loading values greater than 0.6, and each variable has an AVE value greater than 0.5. Therefore, all variables are considered valid. The discriminant validity test in this study is conducted using the Heterotrait-Monotrait (HTMT) method. Discriminant validity is confirmed to meet conservative criteria when the HTMT value is below 0.90 (Henseler et al., 2015). The highest HTMT value in the Table 2 is 0.864. Therefore, all variables are considered valid because they have values < 0.90. This strong validation increases the credibility of the research findings and provides a reliable basis for developing effective strategies against financial cybercrime.

Reliability Test

Good composite reliability value should be above 0.7, and the recommended Cronbach's alpha value should be higher than 0.7 (Hair et al., 2019). Table 2 shows that all variables have composite reliability values higher than 0.7 and less than 0.95, indicating that all variables are considered reliable. This suggests that the instruments used in this study have good internal consistency, meaning that all items within each variable consistently measure the same concept.

R-Squared Test

The R-Square test is used to measure the model's ability to explain the variance in the dependent variable. The R-Square value ranges from 0 to 1, where higher values indicate higher accuracy in predictions (Hair et al., 2019). In Table 2 below, the R-Square values for the constructs are as follows: Perceived Threat (PT) is 0.537, Financial Cybercrime Avoidance Motivation (AM) is 0.374, and Financial Cybercrime Avoidance Behavior (AB) is 0.290. Therefore, these values can be categorized as meeting moderate criteria. This indicates that although the model can explain most of the variance, there are still other factors that are not captured in this model.

PLS-Predict Test

PLS-Predict is used to assess the predictive power of the model under study. Referring to Table 3, the outcomes of the PLS-SEM model are juxtaposed with those of the naive linear regression (LM) benchmark model. Given that all Q2 predicted values exceed zero, the comparison of both models can proceed. The evaluation of predictive performance (PLS-SEM – LM) uses root mean squared error (RMSE) values, which exhibit a symmetrical distribution of prediction errors (Shmueli et al., 2019). When comparing the RMSE statistical values of the PLS-SEM model to the naive LM benchmark model, the majority of the indicators indicate that the PLS-SEM RMSE values are lower than those of the naive LM benchmark. This indicates that the PLS-SEM model has better predictive ability than the benchmark model, although its predictive power is moderate.

Goodness of Fit (GoF) Test

The Goodness of Fit (GoF) test is conducted by taking the square root of the product of the average AVE value and the average R-Square value.

$$\textbf{GoF} \quad = \sqrt{\overline{\text{AVE}} \times \overline{\text{R}^2}} = \sqrt{0{,}653 \times 0{,}410} = \mathbf{0{,}517}$$

A GoF value of 0.517 falls under the category of "large" GoF. Therefore, it can be concluded that this research has a robust research model. With a larger GoF value, this model shows a good fit to the data, and indicates a strong and accurate relationship between the variables in the research model.

Table 1
Convergent Validity Test Results

Variable	Code	Loading	AVE	Variable	Code	Loading	AVE
Perceived Susceptibility (PSC)	PSC1	0.872	0.760	Safeguard Cost (SC)	SC1	0.906	0.879
	PSC2	0.894			SC2	0.968	
	PSC3	0.849		Anticipated Regret (AR)	AR1	0.816	0.685
Perceived Severity (PSV)	PSV1	0.889	0.713		AR2	0.798	
	PSV2	0.897			AR3	0.868	
	PSV3	0.737		Financial Cybercrime Avoidance Motivation (AM)	AM1	0.775	0.655
Perceived Threat (PT)	PT1	0.877	0.654		AM2	0.863	
	PT2	0.899			AM3	0.759	
	PT3	0.772			AM4	0.853	
	PT4	0.664		Financial Cybercrime Avoidance Behavior (AB)	AB1	0.837	0.618
Self -Efficacy (SLE)	SLE1	0.817			AB2	0.859	
	SLE2	0.916	0.775		AB3	0.772	
	SLE3	0.909			AB4	0.760	
	SLE4	0.875			AB5	0.790	
Safeguard Effectiveness (SFE)	SFE1	0.912	0.858		AB6	0.685	
	SFE2	0.957					
	SFE3	0.910					

Source: Data Processed

Table 2
Heterotrait-Monotrait Ratio (HTMT), Composite Reliability (CR), Cronbach's Alpha (CA), and R-Squared

Construct	AR	SFE	SLE	AM	AB	PT	PSV	PSC	SC	PSC X PSV
AR										
SFE	0.395									
SLE	0.093	0.285								
AM	0.707	0.381	0.162							
AB	0.418	0.460	0.390	0.621						
PT	0.506	0.309	0.060	0.528	0.480					
PSV	0.540	0.352	0.067	0.506	0.397	0.862				
PSC	0.430	0.166	0.125	0.362	0.189	0.708	0.864			
SC	0.123	0.121	0.069	0.135	0.177	0.331	0.252	0.303		
PSC X PSV	0.112	0.110	0.029	0.090	0.116	0.454	0.521	0.477	0.040	
CR	0.867	0.948	0.932	0.883	0.906	0.882	0.881	0.905	0.936	
CA	0.772	0.918	0.902	0.824	0.876	0.823	0.794	0.842	0.871	
R-Squared				0.374	0.290	0.507				

Source: Data Processed

Table 3
PLS Predict Test Results

Construct	Q^2 Predict	PLS-SEM	LM	Interpretation
		RMSE	RMSE	
AM1	0.254	0.674	0.707	Medium Predictive Power
AM2	0.218	0.758	0.792	
AM3	0.159	0.790	0.847	
AM4	0.172	0.924	0.989	
AB1	0.107	0.924	0.960	
AB2	0.141	**0.907**	0.873	
AB3	0.179	0.842	0.876	
AB4	0.098	0.951	0.979	
AB5	0.080	1.043	1.052	
AB6	0.062	1.159	1.202	
PT1	0.460	0.687	0.693	
PT2	0.403	0.674	0.677	
PT3	0.241	0.911	0.916	
PT4	0.075	1.114	1.121	

Source: Data Processed

Hypothesis Test

The hypotheses test results are illustrated in Table 4.

Discussions

This study aims to examine the factors influencing financial cybercrime avoidance behavior among employees in financial sector companies in Indonesia. Previous studies have encouraged further studies due to inconsistent results. This study is conducted in Indonesia because the country experiences a high level of cybercrime, yet there has been limited research on preventing cybercrime in this region. This study contributes to both theoretical discourse and the practical realm. From a practical perspective, this study is useful for regulators, cybersecurity system developers, and information technology users.

Table 4
Hypothesis Test Results

Hypotheses		Relations	Coefficient Value	T-Stat.	P Values	Results
H1:	Perceived Susceptibility	PSC → PT	0.192	2.079	0.038***	Supported
H2:	Perceived Severity	PSV → PT	0.548	6.476	0.000***	Supported
H3:	Perceived Susceptibility X Perceived Severity	PSC X PSV → PT	-0.050	0.671	0.503	Not Supported
H4:	Perceived Threat	PT → AM	0.224	2.930	0.003***	Supported
H5:	Self-Efficacy	SLE → AM	0.092	1.461	0.144	Not Supported
H6:	Safeguard Effectivity	SFE → AM	0.117	1.685	0.092*	Supported
H7:	Safeguard Cost	SC → AM	-0.008	0.115	0.908	Not Supported
H8:	Anticipated Regret	AR → AM	0.426	4.563	0.000***	Supported
H9:	Avoidance Motivation	AM → AB	0.542	8.524	0.000***	Supported

Significance level *p < 0,10; **p < 0,05; ***p < 0,01
Source: Data Processed

The results of this study show that six hypotheses are supported, while others are not supported. The first hypothesis (H_1) is supported. Individuals who feel susceptible to financial cybercrime attacks tend to be more sensitive to potential risks and dangers. When people believe that numerous risks could occur in the future, they tend to heighten their perception of the threats they might face. Their increased perception of these threats is a natural response to their belief that a wide range of risks may materialize, leading them to be more vigilant and concerned about potential dangers. This finding aligns with the results of research conducted by Sylvester (2022) that susceptibility perception affects the perception of threats related to phishing attacks. Additionally, the results of research conducted by Mark et al. (2021) on 170 US citizens who are computer users also show that perceived susceptibility has a significant and positive influence on the perception of phishing attack threats. When the perceived susceptibility to financial cybercrime is high, the government should pay attention to and consider the factors that influence perceived susceptibility when formulating policies and actions related to cybersecurity. If someone feels vulnerable to cybercrime threats, he or she will pay more attention to and follow the security measures recommended by the government or relevant organizations.

The second hypothesis (H_2) is supported. When individuals perceive financial cybercrime as a serious threat, they will feel threatened. This underlines the critical connection between the perceived severity of cybercrimes and the psychological response of potential victims. When people perceive financial cybercrime as a significant and imminent danger, it triggers a higher sense of worry. If this perceived severity is indeed high, it becomes imperative for the government to develop more comprehensive policies and mitigation measures to address financial cybercrime effectively. This may involve increasing the effectiveness of law enforcement agencies dedicated to tackling cybercrime, developing stricter regulations, and undertaking greater international cooperation in combating the threat of financial cybercrime. Furthermore, it highlights the need for public awareness campaigns to educate individuals about the risks of financial cybercrime and encourage responsible online behavior. In addition to government action, financial sector companies must also enhance employees' electronic device protection facilities, investing in cybersecurity training, and implementing robust security measures. These findings align with the results of research conducted by Carpenter et al. (2019) that the perceived severity of cybercrimes has a positive influence on the perceived threat of phishing attacks.

Interestingly, this study finds that there is no interaction between perceived susceptibility and perceived severity in shaping perceived threat. The interaction between perceived susceptibility and perceived severity has no effect on perceived threat. So, the third hypothesis (H_3) is not supported. The lack of interaction between perceived susceptibility and perceived severity in influencing perceived threat is due to the fact that when individuals believe they are at risk of financial cybercrime, they may, at the same time, perceive that this susceptibility will not lead to severe consequences. Moreover, perceived threat is highly subjective, which is influenced by individual's interpretation and judgment of specific situations or threats. Some may perceive themselves as vulnerable to financial cybercrime but still feel that they can control their response to prevent it from causing something severe. The results of this study differ from the results of the research conducted by Sylvester (2022) that the interaction between perceived susceptibility and perceived severity positively influences perceived threats. While both factors play crucial roles in shaping perceived threat, the results of this study suggest that they operate independently rather than interactively. This indicates that perceived susceptibility and perceived severity each exert their own influence on how individuals assess threats without directly influencing each other.

The fourth hypothesis (H_4) is supported. Perceived threat has a significant positive influence on the motivation to avoid financial cybercrime. A high level of perceived threat increases vigilance among financial sector workers regarding potential financial cybercrime. This heightened awareness motivates them to take preventive actions. These findings are consistent with the results of research conducted by Carpenter et al. (2019) that perceived threat significantly influences motivation to avoid technological threats. When individuals perceive a higher threat, they are more likely to take proactive steps, such as learning about cybercrime prevention strategies, using protective software, such as antivirus, and engaging in activities to avoid financial cybercrime. Additionally, heightened perceived threat can drive greater support for financial cybersecurity policies. This includes backing governmental or institutional efforts to reduce financial cybercrime risks by strengthening cybersecurity measures, formulating stricter cybercrime legislation, enforcing more rigorous law enforcement, and increasing penalties for offenders.

The fifth hypothesis (H_5) is not supported. Self-Efficacy does not significantly influence the motivation to avoid financial cybercrime because respondents tend to have low confidence in their ability to protect themselves from a cybercrime. They feel uncertain when faced with risky situations or taking necessary preventive measures. This results in reduced motivation to engage in efforts to prevent financial cybercrime. The results of this study align with the results of research conducted by Carpenter et al. (2019) that self-efficacy does not affect the financial cybercrime avoidance motivation. It implies that individuals are less motivated to use protection software (antivirus), as they lack confidence in their ability to operate it to see its value or benefit.

To address this situation, efforts are needed to increase awareness, knowledge, skills, and support related to software protection against financial cybercrime. Training, raising awareness of the importance of a secure cyberspace, and creating an environment that supports cyber safety are crucial for increasing an individual's motivation to avoid financial cybercrime and implement better security practices. Furthermore, software protection (antivirus) developers also need to provide effective and reliable security solutions. This includes developing robust protection software, user-friendly cybercrime detection tools, and additional security features that can assist users in implementing necessary preventive measures efficiently.

The sixth hypothesis (H_6) is supported. Safeguard effectiveness has a positive influence on the financial cybercrime avoidance motivation. When electronic users realize that the antivirus effectively protects their devices, it can impact their motivation to adopt proactive prevention measures. The results of this study are in line with the results of research conducted by Carpenter et al. (2019) that safeguard effectiveness significantly affects motivation to avoid technological threats. High safeguard effectiveness also enhances users' perception of cybersecurity control. If users believe their antivirus provides adequate protection, they feel a greater sense of control over the security of their systems. Effective antivirus software reinforces the perceived value and benefits of engaging in financial cybercrime prevention. This suggests that users tend to view self-protection as a worthwhile investment when they understand the protection that antivirus offers. In addition, this precaution can help them minimize future risks, such as financial loss, identity theft, or reputational damage. Knowing these benefits motivates users to adopt cybercrime prevention strategies and maintain cybersecurity.

The seventh hypothesis (H_7) is not supported. Safeguard cost does not significantly affect financial cybercrime avoidance motivation among financial sector workers. They often do not consider the effort required to obtain protective software (antivirus) because they use devices provided by their companies. The results of this study align with the results of research by Arachchilage et al. (2016), that safeguard cost does not affect motivation to avoid phishing attacks among computer science students in the UK. It is important to note that individuals have different priorities and values regarding their resource allocation. If they perceive safeguard cost as not worth the benefits or other value they consider more important, they are not motivated to take preventive actions involving high safeguard costs. In addition, the availability of resources can significantly affect motivation. If users do not have the resources to access or implement protective measures that require higher effort and costs, the cost of protection will not affect their motivation. In such cases, they may seek more affordable prevention alternatives or rely on other factors like knowledge and skills to reduce the risk of cybercrime. This can result in ineffective prevention efforts, such as installing protective software. A lack of motivation to engage in protective actions with safeguard costs can increase the risk of cybercrime. Vulnerability to threats may rise because individuals do not adopt adequate or effective protective measures. For software protection developers, the implications are clear: if safeguard cost does not impact motivation to avoid cybercrime, it may hinder innovation in developing more effective and affordable protective solutions. Without economic incentives to create large-scale protection measures, the development of innovative and efficient solutions is likely to be hampered.

The eighth hypothesis (H_8) is supported. The results of this study show that anticipated regret positively influences motivation to avoid financial cybercrime. It makes individuals more aware of the negative consequences that may occur if they become victims of financial cybercrime. The results of this study align with the results of research conducted by Verkijika (2019) that anticipated regret has a positive effect on motivation to avoid phishing attacks. Anticipated regret can also increase individuals' perception of the risks associated with crime. They may be more inclined to consider the potential risks and dangers associated with cybercrime and seriously weigh the negative impact that may occur. This can increase their motivation to take preventive measures to avoid these risks.

The implication of this research is that a high level of anticipated regret tends to lead individuals to adopt proactive avoidance strategies such as installing protective software, using strong passwords, regularly updating software, and/or agreeing to recommended security policies. They realize that these preventive actions can help reduce risks and avoid regret in the future. This understanding can drive the development of targeted cybersecurity interventions and educational campaigns that harness the power of anticipated regret to encourage responsible online behavior and create a safer digital environment for everyone.

The ninth hypothesis (H_9) is supported. Motivation to avoid financial cybercrime significantly shapes financial cybercrime avoidance behavior. When individuals possess strong desire to steer clear of cybercrime, they proactively embrace preventive measures to shield themselves from potential risks. The results of this study are consistent with the results of research conducted by Butler (2020); Gillam and Foster (2020); and Verkijika (2019) that motivation to avoid cybercrime has an effect on behavior to avoid cybercrime. High motivation to avoid crime can also increase individuals' awareness of potential cybercrime threats. They may be more sensitive to suspicious signs or potentially dangerous situations, allowing them to avoid or reduce interaction with cybercrime risks. Moreover, motivation to avoid crime can encourage individuals to enhance their knowledge and awareness of the types of financial cybercrime and how to avoid them. They may be more proactive in keeping up with the latest security practices, participating in financial cybercrime education programs, or seeking references to help them learn, identify, and avoid financial cybercrime threats. A great motivation to avoid financial cybercrime can lead individuals to develop safe behaviors as a habit. Individuals who have a great motivation to avoid financial cybercrime are more likely to consistently adopt cybercrime avoidance measures in their daily lives, thus enhancing overall cybersecurity.

5. CONCLUSION, IMPLICATION, SUGGESTION, AND LIMITATIONS

The results of this study show that perceived susceptibility and perceived severity partially have a significant positive influence on perceived threat. However, perceived susceptibility and perceived severity simultaneously do not have a significant effect on perceived threat. This highlights the need to treat perceived susceptibility and perceived severity as independent factors when evaluating their impact on perceived threat.

The results of this study also show that perceived threat, safeguard effectiveness, and anticipated regret have a significant influence on financial cybercrime avoidance motivation. This suggests that individuals who perceive a high risk and anticipate regret from financial losses are more motivated to take preventive actions. Conversely, self-efficacy and safeguard cost do not have a significant effect on financial cybercrime avoidance motivation, indicating that individuals' confidence in their ability to avoid cybercrime or concerns about the cost of protective measures may not play as large a role as anticipated regret. Finally, financial cybercrime avoidance motivation has a significant positive influence on financial cybercrime avoidance behavior, confirming that motivation is a key in driving protective actions.

These findings offer practical implications for various stakeholders. For governments and cybersecurity regulators, the results of the study can inform the development and implementation of policies aimed at reducing financial cybercrime. Specifically, policies should focus on increasing awareness of perceived threats and the potential regret from financial losses to enhance avoidance behavior. For system developers and antivirus software creators, this study emphasizes the importance of protection effectiveness in motivating users to adopt preventive measures. Users who perceive their antivirus as effective are more likely to feel confident and take protective actions. For IT users, both individuals and organizations, these findings provide practical insights to guide decision-making in responding to financial cybercrime threats and helping to reduce their risk of falling victim. Additionally, financial sector companies can use these findings to develop cybersecurity strategies and data governance policies that protect confidential information and safeguard their reputation.

The limitations of the current study lie in the absence of assistance when respondents filled out the questionnaire, which could lead to misunderstandings regarding certain questions. In addition, in the safeguard cost variable, only two of the four measurement indicators could be used. This has the potential to affect the test results for this variable.

It is recommended that future research consider exploring other variables that may influence financial cybercrime avoidance behavior, such as trust in technology, fear of cybercrime, or organizational support. Future research should also involve other industry sectors that are highly vulnerable to financial cybercrime, such as healthcare or retail, so as to deepen the understanding of the specific risks of these sectors. Finally, it is recommended that future research refine invalid indicators to make the research instrument more relevant and accurate.

REFERENCES

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing Threat Avoidance Behaviour: An Empirical Investigation. *Computers in Human Behavior, 60,* 185–197. https://doi.org/https://doi.org/10.1016/j.chb.2016.02.065.

Baker, A. W., Keshaviah, A., Horenstein, A., Goetter, E. M., Mauro, C., Reynolds, C. F., Zisook, S., Katherine Shear, M., & Simon, N. M. (2016). The Role of Avoidance in Complicated Grief: A Detailed Examination of the Grief-Related Avoidance Questionnaire (GRAQ) in a Large Sample of Individuals with Complicated Grief. *Journal of Loss and Trauma, 21*(6), 533–547. https://doi.org/10.1080/15325024.2016.1157412.

Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive Behavior in Response to Email Phishing Threats: The Roles of Rewards and Response Costs. *Computers and Security, 106,* 1–15. https://doi.org/10.1016/j.cose.2021.102278.

Bell, D. E. (1982). Regret in Decision Making Under Uncertainty. *Operations Research, 30*(5), 961–981. https://doi.org/doi:10.1287/opre.30.5.961.

Bennett, M., & Galpert, L. (1992). Complex Belief-Desire Reasoning in Children. *Social Development*, *1*(3), 201–210. https://doi.org/https://doi.org/10.1111/j.1467-9507.1992.tb00124.x.

Brewer, N. T., DeFrank, J. T., & Gilkey, M. B. (2016). Anticipated regret and health behavior: A meta-analysis. *Health Psychology*, *35*(11), 1264–1275. https://doi.org/10.1037/hea0000294.

Butler, R. (2020). A Systematic Literature Review of The Factors Affecting Smartphone User Threat Avoidance Behaviour. *Information and Computer Security*, *28*(4), 555–574). https://doi.org/10.1108/ICS-01-2020-0016.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*(1), 380–407. https://doi.org/10.17705/1CAIS.04422.

Fishburn, P. C. (1982). *The Foundations of Expected Utility*. D. Reidel. Springer.

Gillam, A. R., & Foster, W. T. (2020). Factors Affecting Risky Cybersecurity Behaviors by U.S. Workers: An Exploratory Study. *Computers in Human Behavior*, *108*, 1–12. https://doi.org/10.1016/j.chb.2020.106319.

Gupta, B. B., Perez, G. M., Agrawal, D. P., & Gupta, D. (2020). *Handbook of Computer Networks and Cyber Security* (1st ed.). Springer International Publishing.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203.

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. https://doi.org/10.1007/s11747-014-0403-8.

IBM. (2022). *X-Force Threat Intelligence Index 2022 Full Report*. IBM Security.

Jenab, K., & Moslehpour, S. (2016). Cyber Security Management: A Review. *Business Management Dynamics*, *5*(11), 16–39.

Kasmaei, P., Shokravi, F. A., Hidarnia, A., Hajizadeh, E., Atrkar-Roushan, Z., Shirazi, K. K., & Montazeri, A. (2014). Brushing Behavior Among Young Adolescents: Does Perceived Severity Matter. *BMC Public Health*, *14*(8), 1-6. https://doi.org/10.1186/1471-2458-14-8.

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly: Management Information Systems*, *33*(1), 71–90. https://doi.org/10.2307/20650279.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Loomes, G., & Sugden, R. (1982). Regret Theory: An Alternative Theory of Rational Choice Under Uncertainty. *The Economic Journal*, *92*(368), 805–824. https://doi.org/https://doi.org/10.2307/2232669.

Mark, M. S., Borda, O., Stroman, J., Member, C., & Wilson, T. C. (2021). An Analysis of Factors Influencing Phishing Threat Avoidance Behavior: A Quantitative Study. *Computers in Human Behavior, 60*, 185–197.

NCSI. (2022). *National Cyber Security Index - Indonesia*. National Cyber Security Index.

PwC. (2022). *PwC's Global Economic Crime and Fraud Survey 2022*. PwC.

Saidi, K., & Prayudi, Y. (2021). Analisis Indikator Utama Dalam Information Security-Personality Threat Terhadap Phishing Attack Menggunakan Metode Technology Threat Avoidance Theory (TTAT). *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia), 6*(1), 21-30

Shih, E., & Schau, H. J. (2011). To Justify or Not to Justify: The Role of Anticipated Regret on Consumers' Decisions to Upgrade Technological Innovations. *Journal of Retailing*, *87*(2), 242–251. https://doi.org/https://doi.org/10.1016/j.jretai.2011.01.006.

Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J. H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: guidelines for using PLSpredict. *European Journal of Marketing*, *53*(11), 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189.

Sukamulja, S., Meilita, A. Y. N., & Senoputri, D. (2019). Regret Aversion Bias, Mental Accounting, Overconfidence, and Risk Perception in Investment Decision Making on Generation Y Workers in Yogyakarta. *International Journal of Economics and Management Studies*, *6*(7), 102–110. https://doi.org/10.14445/23939125/ijems-v6i7p116.

Sylvester, F. L. (2022). Mobile Device Users' Susceptibility to Phishing Attacks. *International Journal of Computer Science and Information Technology*, *14*(1), 1–18. https://doi.org/10.5121/ijcsit.2022.14101.

Tang, Z., Miller, A. S., Zhou, Z., & Warkentin, M. (2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly*, *38*(2), 1-11. https://doi.org/10.1016/j.giq.2021.101572.

Verkijika, S. F. (2019). If You Know What to Do, Will You Take Action to Avoid Mobile Phishing Attacks: Self-Efficacy, Anticipated Regret, and Gender. *Computers in Human Behavior*, *101*, 286–296. https://doi.org/https://doi.org/10.1016/j.chb.2019.07.034.

Xiling, H., Yuli, Z., Yiran, L., & Yan-ping, P. (2018). A Theoretical Framework for Counterfactual Thinking in The Context of Entrepreneurial Failure. *Foreign Economics and Management*, *40*, 3–15. https://doi.org/10.16538/j.cnki.fem.2018.04.001.

Appendix 1. Research Instrument

Variable	Question Items	Reference
Perceived Susceptibility	It is very likely that my devices will become targets of financial cybercrime in the future. The chance of me becoming a victim of financial cybercrime through electronic devices is quite high. There is a strong possibility that my electronic devices contain or are infected with malware (viruses) that can steal my personal data.	(Liang & Xue, 2009), with modification.
Perceived Severity	Perpetrators of financial cybercrime can collect personal data from my electronic devices without my knowledge. The personal data collected by financial cybercriminals from my electronic devices can be misused. Financial cybercrime attacks can slow down the performance of my electronic devices and internet connection.	(Liang & Xue, 2009), with modification.
Perceived Threat	Financial cybercrime attacks on electronic devices can pose a threat to me. Issues caused by financial cybercrime attacks on electronic devices are harmful to me. Financial cybercrime is harmful to my electronic devices and internet network. I cannot imagine the consequences if I were to become a victim of financial cybercrime targeting my electronic devices.	(Liang & Xue, 2009), with modification.
Self-Efficacy	I am confident that, without assistance from others, I can acquire knowledge about financial cybercrime threats that could target my electronic devices. I am confident in my ability to detect financial cybercrime attacks on my electronic devices. I am confident in my ability to detect applications/software on my electronic devices that do not come from trusted sources. I am confident that I have the ability to identify SMS/emails containing malicious links on my electronic devices.	(Liang & Xue, 2009) and (Verkijika, 2019), with modification.
Safeguard Effectivity	Protective software (antivirus) will be useful in detecting and removing financial cybercrime attacks on my electronic devices. Protective software (antivirus) can enhance my ability to protect my electronic devices from financial cybercrime attacks. Protective software (antivirus) can improve my effectiveness in identifying and eliminating financial cybercrime attacks on my electronic devices.	(Liang & Xue, 2009), with modification.
Safeguard Cost	The process of acquiring protective software (antivirus) for electronic devices will require a significant amount of time and effort, as it is not an easy task. The installation process of protective software (antivirus) on electronic devices will require a substantial amount of time and effort, as the installation is not straight forward. Having protective software (antivirus) on my electronic devices will disrupt my comfort, as the software may cause issues with my devices. Subscribing to protective software (antivirus) for electronic devices is a form of wastefulness, as the subscription costs are not cheap.	(Liang & Xue, 2009), with modification.
Anticipated Regret	I would regret it if I failed to take the necessary steps to protect my electronic devices from financial cybercrime attacks. I would regret it if I installed software from untrusted sources on my electronic devices. I would regret it if I opened a link from an SMS/email containing a virus on my electronic devices.	(Verkijika, 2019) , with modification

Variable	Question Items	Reference
Financial Cybercrime Avoidance Motivation	I am motivated to acquire knowledge about financial cybercrime to avoid cyber-attacks targeting my electronic devices. I am motivated to use protective software (antivirus) to prevent financial cybercrime attacks on my electronic devices. I am motivated to share knowledge about financial cybercrime with others so they do not fall victim to cyber-attacks. I am motivated to encourage others to use protective software (antivirus) on their electronic devices to avoid financial cybercrime attacks.	(Liang & Xue, 2009), with modification.
Financial Cybercrime Avoidance Behavior	I always verify that all emails come from trusted sources before opening any attachments or links on my electronic devices. I always verify the authenticity of messages before opening links from SMS or messaging platforms on my electronic devices (e.g., WhatsApp, Line, Facebook Messenger). I only allow notifications from trusted websites or software on my electronic devices. All software installed on my electronic devices always comes from trusted sources. I regularly update the operating system and all installed software on my electronic devices as soon as updates become available. I regularly run protective software (antivirus) on my electronic devices to prevent financial cybercrime attacks.	(Liang & Xue, 2009) and (Verkijika, 2019), with modification.