Journal of Human Security | 2025 | Volume 21 | Issue 1 | Pages 81-89
DOI: https://doi.org/10.12924/johs2025.21114
ISSN: 1835–3800

Journal of Human Security

Research Article

More than Fear: A Path Analysis of Cybercrime among Thai Internet Users with Organizational and Institutional Trust as a Mediator

Samanan Rattanasirivilai[1], Trynh Phoraksa[2*]

[1]Graduate School, Suan Sunandha Rajabhat University, Thailand. Email: samanan.ra@ssru.ac.th
[2]Assistant Faculty of Social Sciences and Humanities, Mahidol University, Thailand. Email: trynh.pho@mahidol.ac.th

***Correspondence:** trynh.pho@mahidol.ac.th

Submitted: 20 April 2025 | Revised: 30 May 2025| Accepted: 22 June 2025 | Published: 30 June 2025

Abstract: In today's borderless digital world, cybercrime follows individuals like a shadow. What matters most is not merely fear but rather understanding and preparedness. Fear of cybercrime has emerged as a critical issue that directly affects both the quality of life and the behavior of internet users. This study emphasizes the role of organizational and institutional trust in mitigating such fears and aims to examine the causal relationships underlying fear of cybercrime, with institutional trust serving as a mediating variable. The sample comprised 400 Thai internet users. Data was collected using a five-point Likert scale questionnaire and analyzed through descriptive statistics, Pearson's correlation, path analysis, and mediation analysis with statistical software. The findings revealed that the proposed path model demonstrated a good fit with the empirical data (= 6.404, df = 5, p = .26(, = 1.281, GFI = 0.995, AGFI = 0.974, NFI = 0.992, NNFI = 0.992, CFI=0.998, RMR = 0.006, SRMR = 0.019, RMSEA=0.027). Overall, the model explained 61.50% of the variance in fear of cybercrime. Two sets of mediating factors were identified: (1) factors that reduced fear of cybercrime through organizational and institutional trust, including perceived knowledge of cybercrime (= –0.170, p < .001), digital literacy (= –0.116, p < .001), and awareness of cybercrime (= –0.034, p = .022); and (2) factors that amplified fear of cybercrime through organizational and institutional trust, including social media intensity (= 0.097, p < .001) and cybercrime victimization (= 0.063, p < .001). These findings indicated that fear of cybercrime is not merely an individual perception but rather the outcome of an evaluative process that integrates cognition, lived experience, and behavior. The results have important implications for development administration. They call for integrated strategies that strengthen organizational and institutional trust, enhance digital literacy, and expand perceived knowledge of cybercrime, alongside systemic risk management. Such measures not only help reduce fear of cybercrime but also contribute to building social resilience and establishing a solid foundation for sustainable development.

Keywords: Fear of Cybercrime, Organizational and Institutional Trust, Perceived Knowledge of Cybercrime, Digital Literacy, and Awareness of Cybercrime.

1. Background and Significance of Problem

Amidst the current digital era, the volume of internet and online platform use has rapidly risen. Consequently, the occurring cybercrime becomes a widespread problem that affects both individuals and organizations. Cybercrime includes personal data theft, financial fraud, phishing, and online harassment. All of these have an impact on the digital security of individuals and organizations [1]. The impact does not only on financial loss and breaches of personal data, but it also inevitably undermines individuals' psychological well-being. This is considered the fear of cybercrime which is a critical psychological condition. The fear of cybercrime refers to the anxiety and apprehension stemming from the perceived risk of becoming a victim of online crime. It is also a psychological phenomenon reflecting individuals' emotional, cognitive, and behavioral responses to the perception of online threats [2; 3]. This kind of fear does not only impact individuals' mental health but can also lead to behavioral changes aiming at restricting or reducing the risk of encountering cybercrime in the online environment. One form of behavior influenced by fear of cybercrime is "constrained behavior." It refers to individuals choosing to reduce, refrain from, or avoid certain online activities such as reducing online shopping through electronic platforms, avoiding the disclosure of personal data, or adopting stricter self-protective measures [4]. These behaviors serve as adaptive mechanisms that reflect self-regulation to diminish vulnerability to risks. However, in some cases, they may result in the reduction of efficiency in technology adoption or the deterioration of the entire confidence in digital systems.

Although the academicians across various fields have been attracted by fear of cybercrime Brands and Van Doorn [4], studies on fear of cybercrime remain relatively limited, both in terms of quantity and diversity of measurement approaches. For instance, distinctions between emotions such as fear, anxiety, or worry are often not clearly measured. Likewise, the types of cybercrimes under study vary, ranging from general cybercrime to more specific forms. This causes the research findings remain inconclusive [4]. Furthermore, previous studies focusing on factors influencing fear of cybercrime have also been relatively limited. For example, gender has been found to be associated with fear of cybercrime, with women typically reporting higher levels of fear compared to men [5; 6]. Victimization is also consistently connected with continuous fear [7]. In addition, perceived risk has been identified as a key variable affecting levels of fear [8; 9]. Other factors such as "social media intensity" have also been found to influence the level of such fear [4].

However, several studies have focused solely on the direct relationship between fear and behavior. An explanation of the internal mechanisms of individuals that function as mediators between causal factors and the fear of cybercrime is still overlooked. Understanding these mechanisms requires consideration of the role of society and, more specifically, the role of government agencies responsible for law enforcement and the suppression of cybercrime. This is the role of "Organizational and Institutional Trust" serving as a mediator between causes and the fear of cybercrime [2; 10; 11]. As the mediator, Organizational and Institutional Trust influences individuals' decisions regarding whether to restrict or maintain their online behavior when facing with threats. Therefore, investigating the mechanisms and role of institutional trust is of critical importance in shaping the attitudes and behaviors of internet users, particularly in terms of the acceptance of preventive measures or responses to cyber threats. Nonetheless, research on the role of institutional trust as a mediator remains limited, especially within the context of internet users in Thailand, where unique cultural and social contexts possibly influence both trust and fear in different ways from other countries. From these reasons, the researcher is interested in studying the fear of cybercrime among internet users in the context of Thailand through the development and testing of a Structural Equation Model (SEM) using Path Analysis. The study focuses on examining the role of Organizational and Institutional Trust as the mediator to deepen the understanding of the mechanisms linking cognition, experiences, and behavior with the reduction of fear of

cybercrime. The findings are expected to provide valuable guidance for relevant agencies in reducing public fear of cybercrime by strengthening institutional trust, as well as contributing knowledge for the development of preventive policies and cybersecurity measures for internet users.

2. Research Questions

1. What is the level of fear of cybercrime among internet users?
2. Does the path model of fear of cybercrime among internet users, developed by the researcher, fit the empirical data and how?
3. Do Organizational and Institutional Trust serve as mediators in the path model of fear of cybercrime among internet users and how?

3. Research Objectives

1. To develop and examine the goodness-of-fit of the path model of fear of cybercrime among internet users developed by the researcher with empirical data.
2. To analyze the mediator's role of Organizational and Institutional Trust between various factors and the fear of cybercrime among internet users.

4. Literature Review

The literature review for this research emphasizes the investigation of fear of cybercrime within the context of Thailand, particularly the factors influencing such fear. The rapid expansion of internet access in thailand has heightened public awareness of risks associated with online activities, especially in terms of recurring incidents of cyber-attacks and data breaches [12; 13]. In Thailand's rapidly advancing technological context, this research focuses on fear of cybercrime by examining the role of Organizational and Institutional Trust as the mediator. Specifically, the study examines how victimization from cybercrime, knowledge and awareness of cybercrime, social media usage, and digital literacy skills are associated with fear of cybercrime [14; 15; 16].

5. Theoretical Framework

The study of fear of cybercrime requires a theoretical framework capable of explaining the complex human phenomena that encompass cognition, experience, and behavior. This research considers three principal theories including Risk Perception Theory, Trust Theory, and Cybersecurity Perception Theory. Each of these theories plays a specific role in explaining the mechanisms that generate and mitigate fear.

5.1 Risk Perception Theory

Risk Perception Theory highlights that individuals perceived risks influence their decisions and behaviors, particularly in the context of cybercrime. Perceptions of risk directly affect fear and shape individuals' preventive behaviors [17]. In cybercrime cases, individuals who perceive higher risks of being targeted such as identity theft or personal data breaches are more likely to avoid online transactions or limit their engagement with digital platforms.

5.2 Trust Theory

Trust Theory emphasizes the role of trust in reducing uncertainty and perceived risks in situations that require reliance on others or institutions [18]. This research focuses on studying organizational trust such as government agencies, technology companies, and law enforcement bodies. All of these play a critical role in cybercrime prevention. Higher levels of institutional trust enhance individuals' confidence in digital technology use and help alleviate fears associated with cyber threats.

5.3 Cybersecurity Perception Theory

Cybersecurity perception refers to individuals' awareness of the security of the online systems or platforms they use. Users are more confident in engaging with digital platforms when they perceive that these systems have adequate safeguards against cyber-attacks [19]. When individuals believe that the systems they use are sufficiently secure, they experience greater confidence and reduced anxiety towards potential cyber threats. By integrating the three theories, this research links them to three key dimensions that explain the dynamics of fear of cybercrime as follows:

5.4 Cognition

This refers to the mental processes used by individuals to perceive, evaluate, and interpret cyber threats. It encompasses prior knowledge, awareness, and perceptions of system security, which serve as cognitive mechanisms guiding decisions about whether to perceive digital systems as risky or safe. The cognition expands to Risk Perception, Cybersecurity perception, and cyber threat knowledge. The variables involved are Perceived Knowledge of Cybercrime (PKC), Digital Literacy (DGL), and Awareness of Cybercrime (AWC)

5.5 Experience

This refers to the cumulative effects of direct or proximate encounters with real-life events such as being victimized by cybercrime or being exposed to experiences faced by close acquaintances. This dimension represents lived evidence that strengthens the perception of risk and amplifies fear with greater emotional intensity, beyond mere theoretical awareness. Experience encompasses both direct Cybercrime Victimization (CCV) and proximate exposure. This reinforces risk assessment and heightens the intensity of fear.

5.6 Behavior

This refers to patterns of digital system use, and expressions of online engagement shaped by risk assessments and past experiences. Examples include frequent use of social media or avoidance of online transactions. This dimension reflects cognition and experience. Simultaneously, it also exerts influence on future levels of fear. Behavior encompasses patterns of usage that reflect both risk assessment and prior experiences. For instance, Social Media Intensity (SMI) possibly increases exposure to cyber threats which in turn can intensify fear. The three dimensions operate in a dynamic manner. Organizational and Institutional Trust (OIT) serves as the mediator to mitigate negative effects of risk perception and adverse experiences, while reinforcing the positive effects derived from heightened security awareness and appropriate behavioral practices.

5.7 Conclusion

From the theoretical framework outlined above, it can be synthesized that fear of cybercrime does not stem from a single factor. It rather emerges as the outcome of an integrated evaluative process encompassing cognition, experience, and behavior. Institutional and organizational trust functions as a balancing mechanism within this process. Therefore, the research framework should reflect the dynamic interplay between the independent variables including cognition, experience, and behavior. The dependent variables are, namely fear of cybercrime, with organizational and institutional trust serving as the mediator. This approach enables a comprehensive and systematic explanation and understanding of the phenomenon.

6. Research Conceptual Framework

Based on a review of related concepts, theories, and previous studies, it can be concluded that prior cybercrime victimization, social media intensity, perceived knowledge of cybercrime, and awareness of cybercrime exert direct influences on fear of cybercrime. It also exerts indirect influences through institutional and organizational trust. This can be illustrated in Figure 1.

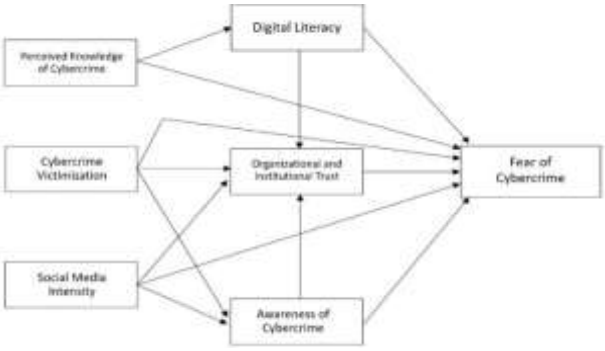


Figure 1: Research Conceptual Framework

7. Research Methodology

7.1 Population and Sample

The population for this study consisted of Thai nationals aged 18 years and older who use the Internet. The sample comprised 400 Thai Internet users aged 18 years and older. The sample size was determined based on Structural Equation Model (SEM) using the LISREL program, with estimation conducted through the Maximum Likelihood (ML) method. Hair ,Black [20] recommend an appropriate sample size of 200–300. Meanwhile, Kline [21] suggests calculating sample size by considering the number of parameters, using a ratio of 10–20:1. For this study, with 23 parameters, the researcher selected a ratio of 17:1, resulting in a required sample size of 391 participants. To ensure data distribution approximated normality, the sample size was adjusted to 400 participants.

Regarding sampling methods**,** Purposive Sampling was employed to obtain the study sample. The inclusion and exclusion criteria were as follows. In terms of Inclusion Criteria, the research participants must be Thai nationals aged 18 years or older who are able to read and understand Thai accurately, must be regular Internet users at least one hour per day, and must voluntarily consent to participate in the study. In terms of Exclusion Criteria, they are non-internet users who are non-Thai nationals or individuals under 18 years of age, are unable to read or comprehend Thai, use the internet less than one hour per day, decline to provide informed consent. Moreover, participants who began but did not complete the study such as those who failed to complete the questionnaire or withdrew during data collection were excluded from the research analysis.

8. Data Collection

The research instrument used in this study was a questionnaire consisting of eight parts as detailed below:

Part 1: Personal Data. This part included both multiple-choice and open-ended questions, comprising 5 items; gender, age, education level, average monthly income, and average daily hours of internet use.

Part 2: Fear of Cybercrime (FOC). This refers to the anxiety or fear stemming from the perception of threats associated with cybercrime, which may include identity theft, online fraud, or becoming a victim of cyberattacks that could affect privacy, financial security, and personal safety. It was measured using 9 items on a five-point Likert scale, adapted from the frameworks of [22; 23; 24; 25].

Part 3: Organizational and Institutional Trust (OIT). This refers to the level of confidence individuals have in the competence, credibility, and integrity of government or private organizations responsible for cybersecurity management and oversight. Examples include cybersecurity agencies, banks, financial institutions, and online platform providers. It was measured using 9 items on a five-point Likert scale, adapted from [26; 27; 28].

Part 4: Cybercrime Victimization (CCV). This refers to an individual's prior experience of being subjected to or affected by cybercrime. Such incidents may involve privacy violations, fraud, online attacks, or other harmful activities occurring on digital platforms. It was measured using 9 items with Yes or No answers, adapted from [29; 30; 31].

Part 5: Perceived Knowledge of Cybercrime (PKC). This refers to the extent to which individuals believe they possess knowledge about the nature, forms, methods, or techniques of cybercrime, as well as strategies for prevention and response. It was measured using 9 items on a five-point Likert scale, with a Cronbach's alpha reliability coefficient of 0.813. The items were adapted from [22; 23; 24].

Part 6: Awareness of Cybercrime (AWC). This refers to the degree to which individuals recognize and understand cyber threats, risks, and behaviors that may lead to cybercrime, including the potential consequences of careless digital technology adoption. It was measured using 9 items on a five-point Likert scale, adapted from [32; 33; 34].

Part 7: Social Media Intensity (SMI). This refers to the extent of individuals' engagement with and use of social media in their daily lives. It encompasses the frequency of use, time spent, emotional attachment, and the role of social media in day-to-day activities. It was measured using 9 items on a five-point Likert scale, adapted from [35; 36; 37].

Part 8: Digital Literacy (DGL). This refers to individuals' ability to use digital technologies for learning, communication, and daily work. It includes knowledge of information retrieval, online content analysis, problem-solving with digital tools, and critical decision-making in technology use. It was measured using 9 items on a five-point Likert scale, adapted from [38; 39; 40].

The research instrument was examined for both content validity and reliability. The details are as follows:

Content Validity: The Index of Item-Objective Congruence (IOC) was employed to assess the alignment between the questionnaire items and the research objectives/operational definitions. Three experts evaluated each item for congruence with the research objectives/definitions. Only items with an IOC score of 0.50 or higher were retained.

Reliability: The items that had passed the content validity examination were pilot tested with 30 respondents who were not part of the main study sample in order to evaluate the quality of the research instrument. The collected data were analyzed to determine internal consistency using Cronbach's α coefficient. In addition, the Corrected Item-Total Correlation (CITC) was calculated to assess the degree of alignment between each individual item and the overall construct. The results of the reliability analysis are presented in Table 1.

Table 1: Results of the Reliability Analysis of the Questionnaire

Variables	Number of items (questions)	Corrected-Item Total Correlation: CITC	Cronbach's α coefficient
FOC	9	0.870 – 0.890	0.974
OIT	9	0.898 – 0.916	0.979
CCV	9	0.701 - 0.765	0.925
PKC	9	0.240 – 0.759	0.874
AWC	9	0.250 – 0.776	0.854
SMI	9	0.874 – 0.895	0.964
DGL	9	0.867 – 0.896	0.954

According to Table 1, the results of the reliability test of the questionnaire indicated that all variables had Corrected Item-Total Correlation (CITC) values within the acceptable range, ranging from 0.240 to 0.916. The Cronbach's alpha coefficients between 0.854 and 0.979 are higher than the standard threshold of 0.70. This demonstrates that the questionnaire employed in this study possessed a high level of reliability and was suitable for effectively measuring the intended variables.

Regarding the data collection, the researcher obtained ethical approval from the Human Research Ethics Committee, Association of Law and Political Science (Committee Set 1: Humanities and Social Sciences). Once approval was granted, the researcher contacted social media service providers to distribute the online questionnaire in the form of a Google Form. After data collection was completed, all questionnaires were screened for completeness, yielding a 100% response rate.

9. Data Analysis

The data were analyzed using statistical software, with significance levels set at .05 and .01 (α = .05, .01). The analytical procedures were as follows:

1. Personal data were analyzed to describe the characteristics of the sample and the distribution of variables using frequency, percentage, mean, standard deviation, minimum, maximum, skewness, and kurtosis.
2. The correlation coefficients among observed variables were examined using Pearson's correlation coefficient to generate a correlation matrix, which served as the basis for the subsequent path analysis.
3. The Path Analysis was conducted using the parameter estimation with the Maximum Likelihood (ML) method.
4. The Mediation Analysis was conducted using the bootstrapping method with 5,000 resamples. The significance of indirect effects was assessed through a bias-corrected 95% confidence interval (95% BC CI).

10. Research Findings

The sample in this study consisted of 400 Thai internet users. Among these, 46 participants (11.50%) identified as male, 329 participants (82.30%) as female, and 18 participants (4.50%) as LGBTQIA+, respectively. In terms of age, the largest group was those aged 41–50 years (152 participants; 38.00%)**,** followed by participants aged 51–60 years (98 participants; 24.50%)**,** 31–40 years (91 participants; 22.80%)**,** 20–30 years (35 participants; 8.80%)**,** over 60 years (21 participants; 5.30%)**,** and those under 20 years (3 participants; 0.80%), respectively. Regarding the educational attainment, the majority held a bachelor's degree (233 participants; 58.30%)**,** followed by those with a master's degree or higher (110 participants; 27.50%)**,** upper secondary/vocational certificate (33 participants; 8.30%)**,** and diploma/high vocational certificate (24 participants; 6.00%)**.**

Regarding average monthly income, most participants earned 30,001–50,000 THB (88 participants; 22.00%)**,** followed by those earning 10,001–20,000 THB (81 participants; 20.30%)**,** and 20,001–30,000 THB (75 participants; 18.80%)**,** respectively. The average daily internet usage was 7.89 hours per day**.**

Table 2: Descriptive Statistics of Independent and Dependent Variables

Variables	Mean	SD	Min	Max	Skewness	Kurtosis
FOC	3.64	0.63	1.27	5.00	-0.15	-0.03
OIT	2.66	0.71	0.84	4.94	0.14	-0.01
CCV	0.80	0.68	0.00	1.00	0.06	-0.00
PKC	4.84	0.23	4.08	5.00	-0.15	-0.09
AWC	4.78	0.31	4.04	5.00	0.02	-0.30
SMI	3.84	0.65	1.95	5.00	-0.01	-0.14
DGL	3.89	0.66	2.30	500	0.14	-0.36

According to Table 2, the results of the descriptive statistical analysis of the independent and dependent variables are presented. It was found that the variable fear of cybercrime, which is the dependent variable, had a mean score at a high level ($\overline{X}$ = 3.64, SD = 0.63). Among the independent variables, the highest mean was PKC, at the highest level ($\overline{X}$ = 4.84, SD = 0.23), followed by AWC with the mean at the highest level ($\overline{X}$ = 4.78, SD = 0.31). DGL had a mean at a high level ($\overline{X}$ = 3.89, SD = 0.66). SMI had a mean at a high level ($\overline{X}$ = 3.84, SD = 0.65) while OIT had a mean at a moderate level ($\overline{X}$ = 2.66, SD = 0.71), respectively.

The skewness values of all variables ranged between -0.15 and 0.14, and the kurtosis values ranged from -0.36 to -0.01. Since these values are close to zero, the data distribution is approximately symmetrical, resembling a normal curve. In addition, the researcher examined outliers using Mahalanobis distance and found that the maximum value in this dataset was 19.97, which did not exceed the threshold (24.32, p < .001). This indicates that the dataset contains no outliers and is reliable for conducting Path Analysis.

Table 3: presents the Pearson correlation coefficients of the observed variables.

Variables	FOC	OIT	CCV	PKC	AWC	SMI	DGL
FOC	1.000						
OIT	-.479**	1.000					
CCV	.490**	-.075	1.000				
PKC	-.487**	.199**	-.180**	1.000			
AWC	.307**	-.020	.221**	-.079	1.000		
SMI	.396**	-.213**	.180**	-.234**	.455**	1.000	
DGL	-.571**	.412**	-.250**	.565**	-.126**	-.207**	1.000

** p < .01

According to Table 3, it was found that the Pearson correlation coefficients between all 21 pairs of observed variables (7 variables) showed that 18 pairs had statistically significant correlations at the .01 level, with values ranging from –.571 to .565. Since these values do not exceed the threshold of .80, it indicates that there is no problem of multicollinearity. Therefore, this dataset is suitable for further Path Analysis.

10.1 Examination on the Assumption of Path Analysis

The Path Analysis is a statistical technique developed from multiple regression analysis and falls within the framework of Structural Equation Modeling (SEM). Hence, the researcher must examine the assumptions to ensure that the data used in the analysis are accurate and reliable, thereby preventing biased parameter estimates. The assumptions to be considered include 1) Linearity, 2) Normality, 3) Independence of Errors, 4) Homoscedasticity, 5) No Multicollinearity, and 6) Sample Size Adequacy. Verifying these assumptions is a crucial step to ensure that the Path Analysis accurately and reliably reflects the relationships among the variables. The results are presented in Table 4.

According to Table 4, the results of testing the assumptions of Path Analysis show that the data used in the analysis are appropriate and consistent with the assumptions. Specifically, the data exhibit linearity, an approximately normal distribution, independence of errors, and homoscedasticity (constant variance of errors).

Table 4: Results of Assumption Testing for Path Analysis

Assumptions	Testing Method	Test Results	Conclusion
1. Linearity	Partial regression plots	Relationship approximates linearity No curvature detected	Consistent with the assumption
2. Normality	Skewness (SK) and Kurtosis (KU)	SK = –1.328 to 0.144 KU = –0.743 to 1.324	Consistent with the assumption
3. Independence of Errors	Durbin–Watson values range between 1.500-2.500	Durbin–Watson value = 2.059	Consistent with the assumption
4. Homoscedasticity	Residual Plot	The variance of the error terms is similarly distributed, indicating homoscedasticity.	Consistent with the assumption
5. No Multicollinearity	Tolerance higher than 0.200 and VIF not exceeding 5	Tolerance range between 0.565–0.896 and VIF value range between 1.116–1.771	Consistent with the assumption
6. Sample Size Adequacy	10-20: 1 parameter	17: 23 parameter equaling to 391 ≈ 400 persons	Consistent with the assumption

In addition, no problem of multicollinearity was found and there was sample size adequacy according to the calculation criteria. Therefore, this dataset is suitable for conducting Path Analysis.

10.2 Results of Model Fit Analysis for the Path Model with Empirical Data

The results of the analysis revealed that the path model of fear of cybercrime demonstrated a good fit with the empirical data (χ^2 =6.404, df = 5, p = .269, χ^2 / df = 1.281, GFI = 0.995, AGFI = 0.974, NFI = 0.992, NNFI = 0.992, CFI = 0.998, RMR = 0.006, SRMR = 0.019, RMSEA = 0.027).

Table 5: Results of Path Analysis of the Path Model of Fear of Cybercrime

Path			b	SE	β	t	p-value	R^2
OIT	→	FCC	– 0.267	0.031	– 0.298**	– 8.632	< .001	0.615
CCV	→	FCC	0.428	0.043	0.326**	9.938	< .001	
SMI	→	FCC	0.120	0.036	0.121**	3.329	.001	
PKC	→	FCC	– 0.717	0.128	– 0.215**	– 5.616	< .001	
DGL	→	FCC	– 0.201	0.041	– 0.201**	– 4.951	< .001	
AWC	→	FCC	0.329	0.089	0.131**	3.686	< .001	
SMI	→	OIT	– 0.206	0.057	– 0.185**	– 3.633	< .001	0.193
DGL	→	OIT	0.436	0.051	0.389**	8.545	< .001	
AWC	→	OIT	0.317	0.142	0.113*	2.238	.025	
CCV	→	DGL	– 0.201	0.054	– 0.153**	– 3.718	< .001	0.342
PKC	→	DGL	1.787	0.137	0.538**	13.025	< .001	
SMI	→	AWC	0.171	0.018	0.429**	9.597	< .001	0.227
CCV	→	AWC	0.075	0.023	0.143**	3.198	.001	

*** p < .01, * p < .05*

All variables together were able to explain 61.50% of the variance in fear of cybercrime. Details are shown in Table 5 and Figure 2.

According to Table 5, the results of the Path Analysis of the path model of fear of cybercrime revealed that the variables that most effectively reduce fear of cybercrime were trust in Organizational and Institutional Trust **(OIT)** (β = – 0.298, p < .001), followed by perceived knowledge of cybercrime (PKC) (β = –0.215, p < .001), and digital literacy (DGL) (β = –0.201, p < .001). This indicates that when individuals have higher levels of trust in organizations and government agencies, greater perceived knowledge of cybercrime, and higher levels of digital literacy, their fear of cybercrime tends to decrease, after controlling for other variables in the model. Conversely, if these variables decrease, fear of cybercrime is likely to increase.

On the other hand, the variables that most strongly increase fear of cybercrime were cybercrime victimization experience (CCV) (β = 0.326, p < .001), followed by awareness of cybercrime (AWC) (β = 0.131, p < .001) and social media intensity (SMI) (β = 0.121, p = .001),

respectively. This suggests that when individuals have direct experiences as victims, exhibit excessively high levels of awareness of cybercrime, or engage intensively in social media use including frequency, level of participation, and emotional attachment to usage, they are more likely to experience greater fear of cybercrime. Under the condition that other variables in the model are controlled, if the levels of these variables decrease, fear of cybercrime tends to decline accordingly. Details are illustrated in Figure 2.

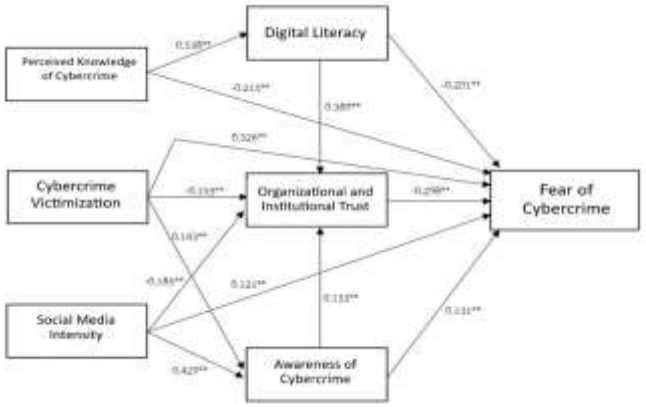


Figure 2: Path model of fear of cybercrime consistent with empirical data

10.3 Testing the Mediator's Role of Confidence in Organizational and Institutional Trusts

The researcher examined the role of Organizational and Institutional Trusts (OIT) as the Mediator using mediation analysis. The bootstrapping method was employed with 5,000 resamples and the significance of indirect effects was assessed through bias-corrected 95% confidence intervals (95% BC CI).

The results revealed that the confidence intervals of the indirect effects did not include zero across several pathways, thereby confirming that OIT plays a statistically significant role of mediator. The mediation was identified as partial mediation since the direct effects remained present. Details of the indirect effects and statistical estimates are presented in Table 6.

Table 6: Indirect effects of independent variables on fear of cybercrime through OIT

Independent variables	Indirect Effect through OIT (β)	95% CI (Bias-corrected)	p-value	Mediation status
CCV	0.063	[0.032, 0.097]	< .001	Partial mediation
SMI	0.097	[0.056, 0.141]	< .001	Partial mediation
PKC	–0.170	[–0.220, –0.125]	< .001	Partial mediation
DGL	–0.116	[–0.153, –0.082]	< .001	Partial mediation
AWC	–0.034	[–0.067, –0.005]	.022	Partial mediation

According to Table 6, the variables can be categorized into two groups; those that reduce fear of cybercrime and those that increase it. The variables that reduce fear of cybercrime with Organizational and Institutional Trusts functioning as the mediator were perceived cybercrime knowledge (β = – 0.170, p < .001), followed by digital literacy (β = – 0.116, p < .001) and awareness of cybercrime (β = – 0.034, p < .022), respectively. Although the three variables of perceived cybercrime knowledge, digital literacy, and awareness of cybercrime exert a direct positive influence on fear of cybercrime, when mediated by Organizational and Institutional Trusts, they contribute to a reduction in fear of cybercrime. This underscores the crucial role of Organizational and Institutional Trusts in mitigating individuals' fear of cybercrime.

For the group that increases fear of cybercrime, the variables were social media intensity (β = 0.097, p < .001) and cybercrime victimization (β = 0.063, p < .001), respectively. These findings indicate that as individuals' social media intensity increases or if they have previously experienced cybercrime victimization, their Organizational and Institutional Trusts decrease. This decline in Organizational and Institutional Trusts consequently leads to heightened fear of cybercrime.

11. Conclusion and Discussion

The examination on the consistency of the fear of cybercrime path model revealed that the model demonstrated an excellent fit with the empirical data and explained a high proportion of the variance in fear of cybercrime, amounting to 61.50%. Importantly, Organizational and Institutional Trusts functioned as a statistically significant mediator. The researcher divided the discussion of research findings into five key issues.

11.1 Factors reducing the fear of cybercrime

Organizational and Institutional Trusts emerged as the most effective factor in reducing fear of cybercrime. The findings of this study revealed that Organizational and Institutional Trusts exerted a direct negative influence on fear of cybercrime. This is consistent with international evidence, which highlights institutional trust as a key determinant in reducing fear of crime both in the physical world and in cyberspace [41; 42]. In particular, given the complexity of cyber threats being difficult to detect and highly technical beyond what individuals can evaluate themselves, Organizational and Institutional Trusts play a vital role in reducing uncertainty that individuals cannot manage alone. Individuals thus place their expectations on protective systems, response mechanisms, and credible remediation measures, which are embodied in these organizations and government agencies.

The negative relationship between Organizational and Institutional Trusts and fear of cybercrime reflects that when individuals perceive such institutions as reliable, they feel more secure in cyberspace. Conversely, when individuals lack trust Organizational and Institutional Trusts, fear of crime intensifies. This agrees with the findings of Gupta ,Hooda [43], who demonstrated that Organizational and Institutional Trusts significantly reduces digital fear and enhances individuals' willingness to continue using online services.

Perceived Knowledge of Cybercrime (PKC) and Digital Literacy (DGL) were found to have a direct negative influence on fear of cybercrime. This finding indicates that individuals with higher levels of knowledge and digital skills are more confident in assessing and coping with cyber threats, thereby experiencing a significant reduction in fear. This result is correspondent with Wang and Wu [44], who studied 1,200 internet users in China by measuring both perceived and objective knowledge of cyber threats. They found that individuals with higher perceived knowledge were better able to evaluate risks in a balanced manner and reported lower levels of fear of cybercrime. Therefore, perceived knowledge of cybercrime acts as a crucial mechanism for calibrating fear within an appropriate range. Similarly, Cho ,Lee [45] reported that digital literacy is directly associated with self-efficacy and indirectly associated with reduced cyber anxiety. Hence, digital literacy does not only mitigate emotional responses but it also enables individuals to adopt a more rational and evaluative approach. These findings support the notion that enhancing knowledge and digital skills functions as a form of "individual capital" that strengthens self-control, reduces fear, and increases confidence in navigating a risk-laden digital world.

11.2 Factors increasing the fear of cybercrime

The findings also reveal that certain factors do not mitigate fear but instead exacerbate it, intensifying individuals' sense of vulnerability. Key factors include cybercrime victimization (CCV), awareness of cybercrime (AWC), and social media intensity (SMI). Among these, cybercrime victimization (CCV) emerged as the strongest contributor to heightened fear. This agrees with Ngo and Paternoster [46]; [47], who confirmed that cybercrime victimization directly increases fear of cybercrime, particularly when users suffer tangible losses of data or assets rather than merely virtual harm. Similarly, Lee and Rho [48] demonstrated that victims of phishing and identity theft in South Korea reported significantly greater digital anxiety compared to non-victims. These insights highlight the necessity of designing preventive measures with an emphasis on victim support systems such as easily accessible reporting mechanisms, psychological counseling services, and compensation schemes. Such measures do not only aid recovery for victims but also contribute to rebuilding trust in the overall system.

Although intended to enhance understanding of cyber threats, without proper regulation, Awareness of Cybercrime (AWC) can

inadvertently lead to risk amplification, causing individuals to become excessively fearful. Solmaz and Tekin [49] found that risk communication focusing solely on "threats" without offering solutions tends to heighten anxiety rather than promote prevention. Boerman ,Kruikemeier [50] also confirmed that excessive use of fear appeals in campaigns fails to translate into positive behavioral change. Therefore, relevant agencies should emphasize constructive risk communication, striking a balance between providing information on cybercrime and presenting concrete solutions or coping strategies such as creating secure passwords, using two-factor authentication, or reporting incidents through digital platforms.

The social media intensity is another factor that can exacerbate fear of cybercrime. Individuals who are heavily connected to multiple platforms are more likely to encounter exaggerated threat narratives, misinformation, or continuous amplification of cybercrime news. Studies by Marwick and Boyd [51] and Choi ,Lim [52] highlight that consuming negative content on social media is directly associated with heightened risk perception and increased fear. Consistent with these findings, Jansen and Vonk [53] reported that individuals with high levels of social media engagement tend to exhibit stronger fear of cybercrime. Thus, effective preventive measures should focus on enhancing media literacy and collaborating with online platforms to develop fact-checking mechanisms in order to reduce the spread of misinformation and exaggerated negative narratives.

Overall, these findings suggest that managing fear of cybercrime requires more than simply increasing knowledge or awareness. It must also involve systemic measures operating at both individual and institutional levels. Such measures should focus on three parallel dimensions: 1) victim recovery and trust restoration, 2) efficacy-based communication, and 3) social media governance & literacy. These strategies must be designed in a comprehensive and well-considered manner.

11.3 The Role of Organizational and Institutional Trusts as the Mediator in Reducing Fear of Cybercrime

Organizational and Institutional Trusts also function as the mediator that plays a significant role in alleviating fear of cybercrime. This research extends the boundaries of knowledge on fear of crime and risk perception into the cyber context, affirming the Institutional Trust Theory, which posits that individuals' perceptions of institutional competence and legitimacy can mitigate fear [54]. The findings indicate that merely possessing cybercrime-related knowledge, digital literacy, or awareness of cybercrime is not sufficient to directly reduce fear of cybercrime. Rather, such effects must operate through Organizational and Institutional Trusts before fear can be alleviated. This finding is correspondent with Jackson ,Stafford [55], who demonstrated that trust in institutions can serve as a buffer against anxiety caused by online threats. It also resonates with research in the Southeast Asian context by Tan [56], which showed that internet users in Singapore with high levels of trust in government were less likely to fear online fraud. This highlights that Organizational and Institutional Trusts are crucial determinants in reducing fear of crime, both in the physical and online worlds.

Digital literacy exerts an indirect influence on fear of cybercrime through Organizational and Institutional Trusts. Virtanen [6] found that digital skills and confidence help reduce fear of cybercrime, but only under the condition that individuals hold Organizational and Institutional Trusts. This suggests that without such trust, digital literacy alone may be insufficient to alleviate fear of cybercrime. Moreover, Mushtaq and Shah [57] found that the effectiveness of public digital literacy depends on the presence of institutional cybercrime safeguards, including legal frameworks, preventive measures, response protocols, reporting mechanisms, reliable communication, and credible infrastructure. Therefore, it can be concluded that while individuals with higher digital literacy may believe they can cope with cybercrime to some extent, the extent to which this literacy reduces fear depends on their trust in organizations and government agencies responsible for handling cybercrime. When individuals are confident in the institutional system's ability to effectively manage cybercrime, they are more likely to perceive such threats as manageable and controllable leading to a reduction in fear of cybercrime.

Awareness of Cybercrime affects the reduction of fear of cybercrime when Organizational and Institutional Trusts act as the mediator. This finding is consistent with the study of Brands and Van Doorn [4], which revealed that when individuals become more aware of cyber risks, their fear tends to increase. However, this relationship is not always linear. If individuals have confidence that governmental agencies or relevant organizations can effectively manage cybercrime, awareness of cybercrime does not necessarily escalate into fear of cybercrime. This also agrees with the study of Konstantinidou [58], which confirmed that the role of institutional trust can provide people with a sense of security, even in the face of cyber threats. Thus, it shows that individuals with high levels of cybercrime awareness are able to interpret or perceive cybercrime in a proportionate and realistic manner, which in turn reduces fear, compared to those with low or no trust in organizations and governmental agencies.

11.4 Integrating the Path Model of Fear of Cybercrime

The research findings reflected through the path model of fear of cybercrime demonstrate that Organizational and Institutional Trusts (OIT) function as a structural mechanism, while Perceived Knowledge of Cybercrime (PKC) and Digital Literacy (DGL) as well as cybercrime victimization, awareness of cybercrime, and social media intensity function as individual capacities. When these two levels operate together, they can explain up to 61.50% of the variance in fear of cybercrime. This suggests that fear is not caused by a single factor but is instead the outcome of an integrative evaluative process that links structural mechanisms and individual capacities with triggers and amplifiers that interact at the structural level. Organizational and Institutional Trusts (OIT) serve as an important structural buffer, mitigating fear by creating confidence that the state and institutions are capable of effectively preventing and managing cyber threats [48; 57]. At the individual level, Perceived Knowledge of Cybercrime (PKC) and Digital Literacy (DGL) enhance individual control, enabling people to distinguish real threats from exaggerated ones and to respond with rational protective behaviors rather than emotional panic [19; 44; 45].

However, a comprehensive understanding of fear of cybercrime requires consideration of supportive triggers, including Cybercrime Victimization (CCV), Awareness of Cybercrime (AWC), and Social Media Intensity (SMI). Although these are not primary mechanisms, they play a critical role in "amplifying" fear if not properly managed. Previous research confirms that prior victimization is the most direct and severe predictor of fear [47; 48]. Meanwhile, excessive cybercrime awareness without proper governance may lead to risk amplification or the escalation of fear [50]. High social media intensity often exposes users repeatedly to cybercrime-related information and exaggerated misinformation, resulting in fear contagion across networks [52; 53].

In summary, the path model of fear of cybercrime indicates that fear of cybercrime is a systemic dynamic requiring the interaction of structural mechanisms (Organizational and Institutional Trusts) and individual capacities (perceived knowledge of cybercrime and digital literacy), alongside measures to manage impacts from direct experiences (victimization, excessive awareness, and overuse of social media). Therefore, policies and practical interventions must integrate both levels. This includes top-down institutional trust building through public policy, protection mechanisms, and transparent, reliable governance systems, together with bottom-up individual capacity development by enhancing cybercrime knowledge and digital literacy to empower self-regulation against cyber threats. Coordinated action across both levels will enable society to manage fear of cybercrime effectively and sustainably.

12. Recommendations from This Research

1. The findings reflect that Organizational and Institutional Trusts (OIT) plays the most significant role in reducing fear of cybercrime. Therefore, fostering and maintaining this trust is a critical condition for effectively managing fear of cybercrime.
2. Perceived Knowledge of Cybercrime (PKC) and Digital Literacy (DGL) serve as factors that enhance individual control, enabling people to distinguish between real threats and overestimated risks. It is recommended to develop training programs or curricula that focus on building individuals' self-efficacy. Such initiatives can strengthen confidence in facing risks, reduce emotional responses caused by fear, and promote rational preventive decision-making in the digital environment.
3. The variables in this study collectively explain up to 61.50% of the variance in fear of cybercrime, which is a high level, demonstrating that integration of both institutional and individual factors is crucial and cannot be considered in isolation. Therefore, the government should focus on building institutional trust through transparent and reliable governance and preventive measures. Meanwhile, the educational sector and private organizations should develop programs and activities to enhance public knowledge of cybercrime and digital literacy. Citizens themselves must take a proactive role in learning and adjusting their digital behaviors responsibly. Integrating these three sectors will help reduce fear of cybercrime and build sustainable societal resilience.

13. Recommendations for Future Research

1. A longitudinal study should be conducted to better understand the dynamics of institutional trust and risk perception, which may change over time depending on events such as major cyberattacks.
2. A cross-cultural study should be undertaken to examine whether the relationships among Organizational and Institutional Trusts (OIT), Perceived Knowledge of Cybercrime (PKC), and Digital Literacy (DGL) share similar or different patterns across countries with varying levels of institutional trust. Such research would help in understanding the global dynamics of fear of cybercrime and in developing policy recommendations that are tailored to the contexts of different societies, whether they are characterized by high or low institutional trust.
3. A multi-group SEM (Structural Equation Modeling) should be conducted to compare the structural differences in the model across groups categorized by age, gender, educational attainment, or socioeconomic status, as these factors may influence levels of fear of cybercrime differently.

14. Policy Recommendations

14.1 Institutional trust building

1. Enhance transparency in government communication regarding cyber risks, establish standardized incident response systems, and provide accessible redress mechanisms to strengthen public trust and reduce citizens' sense of vulnerability.
2. Promote the implementation of cybersecurity certification measures to serve as confidence signals, create clear decision-making criteria, and build public trust in choosing digital services.

14.2 Individual capacity development

1. Develop cybercrime knowledge and digital literacy programs tailored to different target groups such as students, working-age adults, and the elderly, in order to enhance cyber protection skills across all age groups and reduce the digital divide.
2. Launch public awareness campaigns enabling internet users to recognize, differentiate, and effectively protect themselves against cyber threats. These campaigns should aim to reduce biases created by fear-based communication, which can lead to exaggerated threat perceptions, while promoting mindful and confident use of technology.

14.3 Systemic integration

1. Foster collaboration between government agencies, the private sector particularly social media platforms and educational institutions to design integrated measures that combine structural trust and individual knowledge, thereby building comprehensive and sustainable social resilience.
2. Develop risk communication policies that do not only provide warnings but also include clear solutions. This approach helps avoid unnecessarily fear-inducing messages and ensures that citizens have concrete guidance on how to respond to cyber threats.

References

[1] Gordon S, & Ford R. On the definition and classification of cybercrime. Journal in computer virology. 2006;2(1):13-20 https://doi.org/10.1007/s11416-006-0015-z

[2] Lee H, & Kim S. Social media use, digital literacy, and public trust: Evidence from South Korea. Journal of Computer-Mediated Communication. 2021;26(4):215–232. Doi: https://doi.org/10.1093/jcmc/zmab007

[3] Rader NE, May DC, & Goodrum S. An empirical assessment of the "threat of victimization:" Considering fear of crime, perceived risk, avoidance, and defensive behaviors. Sociological Spectrum. 2007;27(5):475-505 https://doi.org/10.1080/02732170701434591

[4] Brands J, & Van Doorn J. The measurement, intensity and determinants of fear of cybercrime: A systematic review. Computers in Human Behavior. 2022;127:107082

[5] Ferraro KF. Women's fear of victimization: Shadow of sexual assault? Social forces. 1996;75(2):667-690 https://doi.org/10.1093/sf/75.2.667

[6] Virtanen SM. Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. Psychiatry, Psychology and Law. 2017;24(3):323-338 https://doi.org/10.1080/13218719.2017.1315785

[7] Henson B, Reyns BW, & Fisher BS. Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. Journal of Contemporary Criminal Justice. 2013;29(4):475-497 https://doi.org/10.1177/1043986213507403

[8] Ferraro KF. Fear of crime : interpreting victimization risk: State University of New York Press; 1995. https://cir.nii.ac.jp/crid/1970304959852682153

[9] Hicks S, & Brown S. Perceptions of risk: A review of the effects of individual and community-level variables on perceptions of risk. International Review of Victimology. 2013;19(3):249-267 https://doi.org/10.1177/0269758013492753

[10] Wendt DC, Huson K, Albatnuni M, & Gone JP. What are the best practices for psychotherapy with indigenous peoples in the United States and Canada? A thorny question. Journal of Consulting and Clinical Psychology. 2022;90(10):802 http://doi.org/10.1037/ccp0000757

[11] Park S, Oh Y, Moon J, & Chung H. Recent trends in continuum modeling of liquid crystal networks: a mini-review. Polymers. 2023;15(8):1904 https://doi.org/10.3390/polym15081904

[12] Gerdruang A. Monitoring to Evaluate Operations: A Case Study at the National Broadcasting and Telecommunication Commission (NBTC). University of the Thai Chamber of Commerce Journal Humanities and Social Sciences. 2016;36(1):178-195 https://so06.tci-thaijo.org/index.php/utccjournalhs/article/view/185216

[13] Smith MY, Frise S, Feron J, & Marshall R. Improving the safety of medicines via digital technology: an assessment of the scope and quality of risk minimization websites in the United States and United Kingdom. Drug Safety. 2022;45(3):259-274 https://doi.org/10.1007/s40264-022-01165-4

[14] Dinev T, & Hart P. Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use. E-service. 2006;4(3):25-60 https://doi.org/10.2979/esj.2006.4.3.25

[15] Lee MK, & Turban E. A trust model for consumer internet shopping. International Journal of electronic commerce. 2001;6(1):75-91 https://doi.org/10.1080/10864415.2001.11044227

[16] Räsänen K, Pietarinen J, Pyhältö K, Soini T, & Väisänen P. Why leave the teaching profession? A longitudinal approach to the prevalence and persistence of teacher turnover intentions. Social Psychology of Education. 2020;23(4):837-859 https://doi.org/10.1007/s11218-020-09567-x

[17] Slovic P, Fischhoff B, & Lichtenstein S. Behavioral decision theory perspectives on risk and safety. Acta psychologica. 1984;56(1-3):183-203 https://doi.org/10.1016/0001-6918(84)90018-0

[18] Mayer RC, Davis JH, & Schoorman FD. An integrative model of organizational trust. Academy of management review. 1995;20(3):709-734 https://doi.org/10.5465/amr.1995.9508080335

[19] Vance A, Siponen M, & Pahnila S. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management. 2012;49(3-4):190-198. Doi: https://doi.org/10.1016/j.im.2012.04.002

[20] Hair JF, Black WC, Babin BJ, & Anderson RE. Multivariate data analysis: Pearson new international edition PDF eBook: Pearson Higher Ed; 2013. https://www.scirp.org/reference/ReferencesPapers?ReferenceID=1841396

[21] Kline P. A handbook of test construction (psychology revivals): introduction to psychometric design: Routledge; 2015. https://doi.org/10.4324/9781315695990

[22] Holt T, & Bossler A. Cybercrime in progress: Theory and prevention of technology-enabled offenses: Routledge; 2015. doi: https://doi.org/10.4324/9781315775944

[23] Morgan DL, & Drury J. Emotional responses to cybercrime: Fear and anxiety. . Journal of Interpersonal Violence. 2015;30(4):657–677. Doi: https://doi.org/10.1177/0886260514536254

[24] Randa R, Reyns BW, & Nobles MR. Measuring the effects of limited and persistent school bullying victimization: Repeat victimization, fear, and adaptive behaviors. Journal of interpersonal violence. 2019;34(2):392-415 https://doi.org/10.1177/0886260516641279

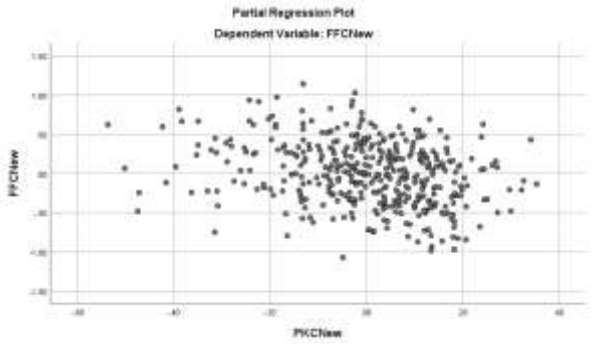
[25] Randa RS, & Reyns BW. Fear of cybercrime: A multidimensional examination. . Cyberpsychology, Behavior, and Social Networking. 2019;22(1):29-36. Doi: https://doi.org/10.1089/cyber.2018.0291

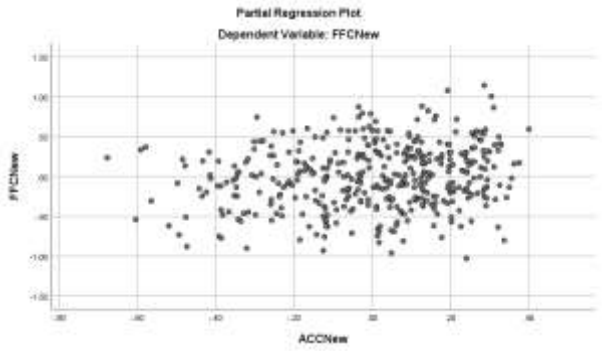
[26] Grimmelikhuijsen S. Trust in government and trust in performance: The role of political trust. International Review of Administrative

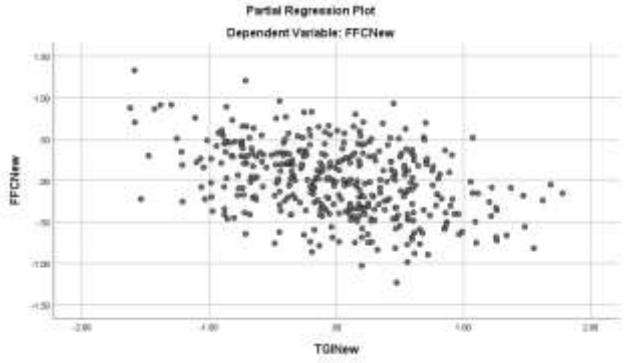
Sciences. 2017;83(3):583–601. Doi: https://doi.org/10.1177/0020852316681248
[27] Holzer M. Restoring trust in government: The potential of digital citizen participaton. Frontiers of Public Administration. 2004;6(6):6-23 https://www.researchgate.net/publication/237227870
[28] Janssen M, & van der Voort H. Adaptive governance: Towards a stable, accountable and responsive government. Government Information Quarterly. 2020;37(1). Doi: https://doi.org/10.1016/j.giq.2019.101397
[29] Bossler A, & Holt T. On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. International Journal of Cyber Criminology (IJCC) ISSN. 2009;3(1):974-2891 https://www.researchgate.net/publication/228929213
[30] Reyns BW, & Henson B. Cybercrime victimization: A longitudinal test of lifestyle-routine activities theory. . Journal of Quantitative Criminology. 2020;36(3):553–575. Doi: https://doi.org/10.1007/s10940-019-09420-0
[31] Wall DS. Cybercrime victimization and its prevention. Journal of Criminal Justice. 2017;51:123-130. Doi: https://doi.org/10.1016/j.jcrimjus.2017.03.005
[32] Aggarwal N, & Mittal A. Cyber security awareness among college students. Journal of Cybersecurity Education, Research and Practice. 2022;2(1):15-26. Doi: https://doi.org/10.1007/978-3-319-94782-2_8
[33] Alqaralleh B, Mueen A, & Kim HC. Cybercrime awareness and prevention behaviors: Evidence from university students. Computers & Security. 2021:102. Doi: https://doi.org/10.1016/j.cose.2020.102153
[34] Hadlington L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon. 2017;3(7) https://doi.org/10.1016/j.heliyon.2017.e00346
[35] Bright LF, Kleiser SB, & Grau SL. Too much Facebook? An exploratory examination of social media fatigue. Computers in human behavior. 2015;44:148-155 https://doi.org/10.1016/j.chb.2014.11.048
[36] Tandoc EC, Ferrucci P, & Duffy M. Facebook use, envy, and depression among college students: Is facebooking depressing? . Computers in Human Behavior. 2015(43):139–146. Doi: https://doi.org/10.1016/j.chb.2014.10.053
[37] Verduyn P, Ybarra O, Résibois M, Jonides J, & Kross E. Do social network sites enhance or undermine subjective well-being? A critical review. Social Issues and Policy Review. 2017;11(1):274-302. Doi: https://doi.org/10.1111/sipr.12033
[38] Eshet-Alkalai Y, & Chajut E. Digital literacy. Theory and Research in Education. 2016;14(1):28-38. Doi: https://doi.org/10.1177/1477878515623999
[39] Ng W. Can we teach digital natives digital literacy? . Computers & Education. 2018(59):1065–1078. Doi: https://doi.org/10.1016/j.compedu.2012.04.016
[40] Van Deursen AJ, Helsper, E. J., & Eynon, R. Development and validation of the Internet Skills Scale (ISS). Information, Communication & Society, 20(6), 804–823. . 2017;20(6):804-823. Doi: https://doi.org/10.1080/1369118X.2016.1207142
[41] Räsänen P, Lappalainen P, Muotka J, Tolvanen A, & Lappalainen R. An online guided ACT intervention for enhancing the psychological wellbeing of university students: A randomized controlled clinical trial. Behaviour research and therapy. 2016;78:30-42 https://doi.org/10.1016/j.brat.2016.01.001
[42] Villarejo-Carballido B, Pulido CM, de Botton L, & Serradell O. Dialogic model of prevention and resolution of conflicts: Evidence of the success of cyberbullying prevention in a primary school in Catalonia. International Journal of Environmental Research and Public Health. 2019;16(6):918 https://doi.org/10.3390/ijerph16060918
[43] Gupta P, Hooda A, Jeyaraj A, Seddon JJ, & Dwivedi YK. Trust, risk, privacy and security in e-Government use: Insights from a MASEM analysis. Information Systems Frontiers. 2025;27(3):1089-1105 https://doi.org/10.1007/s10796-024-10497-8
[44] Wang C-H, & Wu C-L. Bridging the digital divide: the smart TV as a platform for digital literacy among the elderly. Behaviour & Information Technology. 2022;41(12):2546-2559 https://doi.org/10.1080/0144929X.2021.1934732
[45] Cho H, Lee J, & Chung S. Digital literacy and self-efficacy in managing cyber risks: Evidence from South Korea. Cyberpsychology, Behavior, and Social Networking. 2020;23(8):551-558. Doi: https://doi.org/10.1089/cyber.2019.0482
[46] Ngo FT, & Paternoster R. Cybercrime victimization and fear of online fraud. Crime & Delinquency. 2019;65(8):1025–1048. Doi: https://doi.org/10.1177/0011128718813077
[47] Pratt TC, Holtfreter K, & Reisig MD. Routine activity theory and fear of cybercrime: Testing an integrated model. . Journal of Criminal Justice. 2017(53):1-9. Doi: https://doi.org/10.1016/j.jcrimjus.2017.09.001
[48] Lee H, & Rho J. Public trust and fear of cybercrime in South Korea: A path analysis. . Asian Journal of Criminology. 2022;17(3):221-240. Doi: https://doi.org/10.1007/s11417-021-09364-2
[49] Solmaz S, & Tekin H. Cyber awareness and risk amplification: A Turkish case study. . Information & Security: An International Journal. 2021;49(2):203-220. Doi: https://doi.org/10.11610/isij.4920
[50] Boerman SC, Kruikemeier S, & Zuiderveen Borgesius FJ. Online privacy and the role of awareness campaigns: A European perspective. , 46(3), 102292. . Telecommunications Policy. 2022;46(3). Doi: https://doi.org/10.1016/j.telpol.2021.102292
[51] Marwick AE, & Boyd D. Networked privacy: How teenagers manage context in social media. New Media & Society. 2019;21(1):55-72. Doi: https://doi.org/10.1177/1461444819856619
[52] Choi J, Lim S, & Kim Y. Social media use, cyber risk perception, and fear of cybercrime. Journal of Computer-Mediated Communication. 2021;26(4):173–189. Doi: https://doi.org/10.1093/jcmc/zmab008
[53] Jansen M, & Vonk G. Social media intensity and cyber fear: Evidence from the Netherlands. Cyberpsychology. Journal of Psychosocial Research on Cyberspace. 2022;16(2):4. Doi: https://doi.org/10.5817/CP2022-2-4
[54] Tyler TR. Why people obey the law. 2nd ed: Princeton University Press.; 2006. doi: https://doi.org/https://www.researchgate.net/publication/220011500
[55] Jackson JA, Stafford R, Cvitanovic M, & Cantarello E. Interactions of a Farming System Using a Whole-Farm-Approach. Available at SSRN 4820708. 2024 https://dx.doi.org/10.2139/ssrn.4820708
[56] Tan SS. The responsibility to provide in Southeast Asia : towards an ethical explanation: Bristol University Press; 2019. https://cir.nii.ac.jp/crid/1971993809788602397
[57] Mushtaq S, & Shah M. Threats to the Digital Ecosystem: Can Information Security Management Frameworks, Guided by Criminological Literature, Effectively Prevent Cybercrime and Protect Public Data? Computers. 2025;14(6):219 https://doi.org/10.3390/computers14060219
[58] Konstantinidou K. Institutional trust and fear of crime: a study of criminology and social work students at malmö university. 2025.https://www.diva-portal.org/smash/record.jsf?pid=diva2:1960866

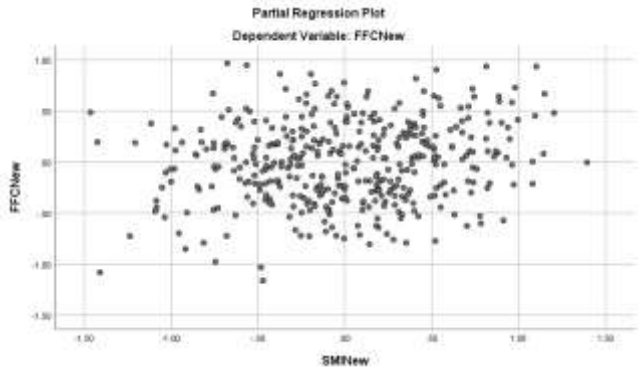
Appendix A

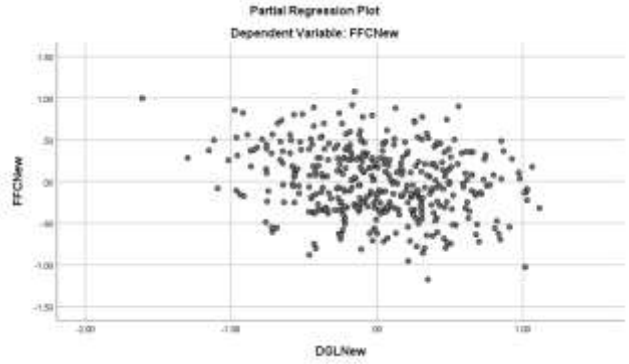
Partial Regression Plot

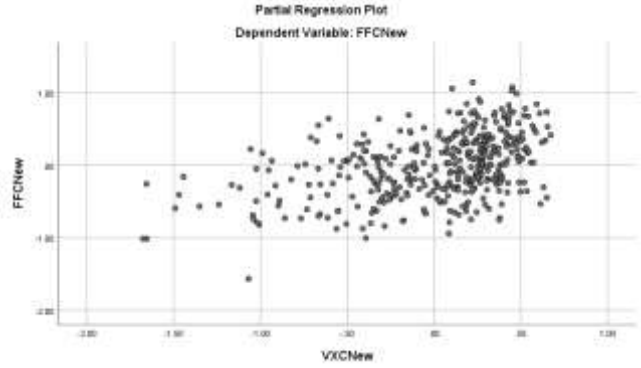












Appendix B

Residual Plot