# Preventing Cyber Crime Through Awareness, Use of Technology and Facilitating Conditions: Theory of Planned Behavior Perspective

Hendi Prihanto
*Universitas Prof.Dr.Moestopo (Beragama); Jakarta, Indonesia*
E-Mail: hendiprihanto@dsn.moestopo.ac.id

Usmar
*Universitas Prof.Dr.Moestopo (Beragama); Jakarta, Indonesia*
E-Mail: usmarismail1504@dsn.moestopo.ac.id

Prisila Damayanti
*Institut Bisnis & Informatika (IBI) Kosgoro 1957; Jakarta, Indonesia*
E-Mail: prisild@rocketmail.com

**Submitted:**
**AUGUST 2025**

**Accepted:**
**OCTOBER 2025**

***ABSTRACT***

*The increasing reliance on digital technology has simultaneously escalated the frequency and sophistication of cybercrime, posing serious risks to financial stability, data security, and organizational performance. This condition underscores the urgent need for effective prevention strategies that combine user awareness, technological adoption, and supportive facilitating conditions. The study aims to analyze factors that influence cybercrime prevention, including user awareness of the dangers of cybercrime and its prevention, the use of information technology, and facilitating conditions towards cybercrime prevention in Indonesia. The study was conducted using quantitative methods through a series of primary data tests obtained using questionnaires, with respondents being users of cloud-based information technology systems, such as private companies and banks, in 2025. Data processing was carried out using SEM-PLS media with a series of inner and outer model feasibility tests before regression and hypothesis testing were carried out. The results of the study stated that all observed variables that were predicted to influence the effectiveness of cybercrime prevention, namely awareness, use of information technology, and facilitating conditions, had a positive and significant effect on cybercrime prevention.*

***Keywords****: Awareness, Cybercrime Prevention, Facilitating Conditions, Information Technology, SEM-PLS.*

***ABSTRAK***

*Meningkatnya ketergantungan pada teknologi digital secara bersamaan telah meningkatkan frekuensi dan kecanggihan kejahatan dunia maya, menimbulkan risiko serius terhadap stabilitas keuangan, keamanan data, dan kinerja organisasi. Kondisi ini menggarisbawahi kebutuhan mendesak akan strategi pencegahan yang efektif yang menggabungkan kesadaran pengguna, adopsi teknologi, dan kondisi fasilitasi yang mendukung. Penelitian bertujuan untuk menganalisis factor-faktor yang mempengaruhi pencegahan kejahatan siber diantaranya kesadaran pengguna atas bahaya kejahatan siber dan pencegahannya, penggunaan informasi teknologi, dan kondisi yang memfasilitasi terhadap pencegahan kejahatan siber di Indonesia. Penelitian dilakukan dengan mengunakan metode kuantitatif melalui serangkaian pengujian data primer yang diperoleh dengan mengunakan kuesioner, dengan responden para pengguna sistem informasi teknologi berbasis cloud seperti perusahaan swasta dan perbankan pada tahun 2025. Pengolahan data dilakukan dengan*

**JIAKES**
Jurnal Ilmiah Akuntansi Kesatuan
Vol. 13 No. 5, 2025
pp. 1079-1092
IBI Kesatuan
ISSN 2337 – 7852
E-ISSN 2721 – 3048
DOI: 10.37641/jiakes.v13i5.3985

*mengunakan media SEM PLS dengan serangkaian uji kelayakan inner dan outer model sebelum uji regresi dan hipotesis dilakukan. Hasil penelitian menyatakan bahwa seluruh variabel yang dilakukan observasi yang diprediksi mempengaruhi efektivitas pencegahan kejahatan siber yaitu kesadaran, pengunaan teknologi informasi dan kondisi yang memfasilitasi berpengaruh positif dan signfikan terhadap pencegahan kejahatan siber tersebut.*

***Kata kunci**: Kesadaran, Pencegahan Kejahatan Siber, Kondisi yang Memfasilitasi, Teknologi Informasi, SEM-PLS.*

## INTRODUCTION

The rapid development of digital technology and the internet has brought significant changes in life, business, work, and communication. in line and at the same time, cybercrime, which is a threat to all parties, is also increasing, especially to business and financial operations that are related to the public (Symons & Blannin, 2020; Akinbowale et al., 2020; Kaur et al., 2023; Prihanto & Usmar, 2024). Cybercrime refers to criminal activities carried out by perpetrators using digital technology, such as computers, smartphones, applications, and the internet, and can usually occur simultaneously and are carried out in various forms such as hacking, identity theft, online fraud, cyberbullying, and cyberstalking (Siregar & Tenoyo, 2015; Rahim et al., 2017; Al-Khater et al., 2020; Althibyani & Al-Zahrani, 2023). Furthermore, Wati et al. (2024) stated that other forms of cybercrime include: Illegal contents, illegal or unauthorized access to computer systems and services, cyber espionage, data falsification, cyber sabotage and extortion, Infringements of privacy, and violations of Intellectual Property Rights.

The first cybercrime case occurred in Indonesia in the 1990s, with the emergence of a case of use of the domain name www.mustikaratu.com, which was tried in the South Jakarta District Court (Wati et al., 2024). Ministry of Communication and Information Technology (MCIT) of the Republic of Indonesia in 2024 explained that Indonesia currently ranks 48th out of 176 countries with a cybersecurity index of 63.64, and ranks 5th in Southeast Asia. Information through Press Release Number 243/HM/KOMINFO/03/2024 stated that globally, there has been an increase in cybersecurity cases from 2019 by 40% and more than 77% in 2023. Cybercrime occurs with various typologies. Association of Indonesian Internet Service Providers (*Asosiasi Penyelenggara Jasa Internet Indonesia*/APJII) stated that motives for online fraud are the highest problem in cybercrime, with a figure reaching 32.5%, and increasing 22.2% from 2023, which was only 10.3%. Currently, the trending mode of cybercrime is theft of personal data, and it is a very serious threat. This crime is ranked 2nd with a number of 20.97% which continues to increase significantly from 2023. Previously, this case was only 7.96% (Popham et al., 2020).

The impact of cybercrime is certain to damage a company or organization's financial infrastructure, e-commerce, and overall business processes. Cybercrime can trigger fear, distrust, and increased risk perception (Rogers, 1975; Slovic, 1987). Prevention is necessary because it not only impacts financial aspects, data, confidentiality, and other losses (Tariq, 2018; Furnell & Dowling, 2019). Examples of conscious cybercrime prevention in several countries, such as Nigeria, are taking preventative measures that harm internet users in that country (Adomi & Igun, 2008; Zia et al., 2024). The behavior of being aware of the dangers and losses caused, and then taking preventative measures significantly influences the success of cybercrime prevention (Drew & Farrell, 2018; Kaur et al., 2023; Tim et al., 2024; Ismaeel, 2025).

User awareness alone is not sufficient to prevent cybercrime; effective efforts also require the use of up-to-date technology such as AI and analytics, which have proven to enhance efficiency and business performance (Halbouni et al., 2016; Nwankpa & Roumani, 2016; Biswas et al., 2020; Zhan et al., 2024). However, the rise of the digital economy has also increased risks such as data exploitation and leaks (Wati et al., 2024).

To address these challenges, facilitating conditions play a critical role, particularly through the use of frameworks like the Cybercrime Mitigation Framework (CCMF) to detect, assess, and respond to evolving threats (Yeboah-Ofori & Opoku-Boateng, 2023). Modern infrastructure further supports timely fraud detection and prevention across dispersed organizational networks, including branches in different regions and countries (Fedyk et al., 2022; Roy & Prabhakaran, 2022; Tim et al., 2024; Pham et al., 2025).

In the Indonesian context, cybercrime has become a growing national concern due to the increasing integration of digital services in public administration, banking, and MSMEs. The lack of awareness, limited technological infrastructure, and uneven digital literacy make Indonesia particularly vulnerable to such threats. Therefore, understanding the determinants of cybercrime prevention is not only academically relevant but also essential for formulating effective national policies and corporate strategies

The study aims to analyze factors that influence cybercrime prevention, including user awareness of the dangers of cybercrime and its prevention (CCP), the use of information technology (UIT) and facilitating conditions (FC) towards cybercrime prevention in Indonesia. This research is very important to carry out, considering the many institutions and individuals who become victims of cybercrime, so it is necessary to carry out effective prevention through identified factors that are able to prevent cybercrime through user awareness of the dangers and losses due to cybercrime, the use of actual information technology, and conditions that facilitate the state of prevention.

## LITERATURE REVIEW & HYPOTHESIS DEVELOPMENT

### Prevention Awareness and Cybercrime Prevention

The use of the Theory of Planned Behavior (TPB) in this study is related to how individuals and organizations behave to carry out planning related to the prevention of cybercrime committed by companies or individuals (Fishbein & Ajzen, 1975; Ajzen, 1991). TPB as a basis that can be used as a guide in research because it helps in understanding the factors that influence a person's or organization's intention to carry out certain behaviors in an effort to prevent cybercrime in the organization, such as planning to improve the information system infrastructure (Robertson & Sribar, 2001). Awareness or concern from individuals and organizations as a whole who realize the importance of protecting the security of their systems and information, and planning for conditions that allow and limit an organization to act (Endsley, 1995; Chatterjee, 2019; Tim et al., 2024). The discussion of TPB is then always related to human behavior, which can be influenced by at least three kinds of belief considerations which are categorized as follows: 1) Beliefs regarding the possible consequences or other attributes of behavior (behavioral beliefs), 2) Beliefs regarding the normative expectations of others (normative beliefs), and 3) Beliefs regarding the existence of factors that can advance or hinder behavioral performance (control beliefs) (Ajzen, 2002).

TPB is essentially a psychological theory developed by Icek Ajzen in the late 1980s that explains how attitudes, subjective norms, and perceived control over behavior influence an individual's intention to perform an action. This theory then becomes a bridge to develop and combine links to other theories, then ultimately determine the behavior of the individual itself, as occurred in this study, namely the effects of cybercrime that can trigger fear, distrust, and increased risk perception and motivation to take protective measures (Rogers, 1975; Slovic, 1987). Ultimately, individuals and organizations will maintain their assets by trying everything to protect them from harm and loss.Literature on cybercrime prevention increasingly highlights the crucial role of digital literacy, public education, and community engagement in reducing risks in the digital era. Kont (2025) emphasizes the need for systematic measurement of information security awareness as a foundation for building resilience against cyber threats. Aborisade (2025) connects crime prevention to sustainable development, noting that community awareness and engagement not only mitigate risks but also promote social stability. Imani and Prastyanti (2025) introduce the concept of the "human firewall," where individuals' literacy and awareness act as essential defenses complementing technological safeguards.

Similarly, Eshra et al. (2025) demonstrate that combining awareness with threat intelligence can effectively reduce financially motivated cyberattacks. Collectively, these studies show that effective cybercrime prevention depends on both technological tools and human knowledge, positioning individuals and communities as key agents in fostering digital resilience through education and proactive information sharing.

The Knowledge, Education, and Security (KES) framework reinforces this view by linking cybercrime prevention to individuals' understanding of how cyber systems work, how to conduct safe online activities, and how to access legal mechanisms against cybercrime (Aggarwal, 2015; Chatterjee et al., 2019). Evidence from India provides practical support for this approach, where awareness campaigns have significantly reduced cybercrime risks. Research by Aparna and Chauhan (2012), Mehta and Singh (2013), Singaravelu and Pillai (2014), and Parmar and Patel (2016) shows that education initiatives empower citizens to recognize, avoid, and report online threats more effectively. These findings indicate that sustainable cybercrime prevention must extend beyond technical defenses, integrating continuous public education, awareness initiatives, and community-based participation to establish a comprehensive, adaptive, and human-centered approach to digital security.

H1: Awareness of cybercrime has a positive effect on cybercrime prevention.

**Current Use of Information Technology and Cybercrime Prevention**

In addition to the Theory of Planned Behavior (TPB), this research applies the Technology Acceptance Model (TAM) proposed by Davis (1989), which examines technology use by stakeholders in financial-based companies. TAM, derived from psychological theory, explains users' computer-related behaviors based on belief, attitude, intention, and behavioral relationships. The development of information technology significantly influences individual behavior (Lindell, 2020). Comprehensive national digitalization efforts also extend to educational curricula aligned with societal progress, as shown by Chen et al. (2018), Hsu et al. (2018), and Scherer et al. (2019). However, many schools, particularly in Indonesia, face technological limitations due to inadequate infrastructure and lagging implementation.

Technology adoption aims to provide ease of use, build stakeholder trust, and enhance user experience in utilizing information systems (Bashir & Madhavaiah, 2015). The ongoing transformation in information technology has produced financial services that align with evolving consumer needs and preferences. In the financial sector, technology enhances customer service, increases efficiency, and strengthens competitive advantage (Mann & Sahni, 2012). TAM itself is an extension of the Theory of Reasoned Action (TRA) by Fishbein and Ajzen (1975), which studies how various factors shape attitudes and behavioral intentions toward adopting technology (Chang & Cheung, 2001; Wang & Ahmed, 2003; Guriting & Ndubisi, 2006; Kesharwani & Bisht, 2012; Abbad, 2013).

To complement TAM, this study also employs the Unified Theory of Acceptance and Use of Technology (UTAUT-2) developed by Venkatesh et al. (2012), which integrates constructs such as hedonic motivation, price value, and habit, moderated by demographic variables including age, gender, and experience. Further expansion into UTAUT-3 incorporates personal innovation as a moderating factor influencing intention, behavior, and technology usage among fintech consumers (Farooq et al., 2017).

The use of information technology (UIT) is increasingly central to cybercrime prevention, with innovations such as artificial intelligence (AI), financial technology (fintech), and blockchain providing new tools to combat evolving threats. Dilek et al. (2015) highlight the role of computational intelligence in monitoring online crimes, particularly against women, where advanced analytics help identify abuse patterns and support preventive legal measures. Fintech innovations that apply AI-driven fraud detection and data privacy technologies to secure financial systems against real-time cyber risks. Similarly, Li et al. (2025) propose a blockchain-based collaborative intrusion

detection framework that strengthens resilience in control systems by enabling early detection and mitigation of cyberattacks. Collectively, these studies show that integrating IT innovations with legal and institutional frameworks is critical to building proactive, technology-driven defenses against cyber threats.

At the same time, IT adoption is closely related to how organizations and societies understand and apply technological tools. The rapid pace of technological development compels organizations to expand and modernize their infrastructure, a trend evidenced by accounting service firms that increasingly invest in technology to improve operational resilience (Sorebo et al., 2007; Pham et al., 2025). When prevention technologies are adopted and utilized effectively, coupled with greater public awareness, communities can play an active role in minimizing cyber risks (Longstaff & Schultz, 1993; Zaied, 2012). This alignment between technological innovation, organizational investment, and user awareness underscores that cybercrime prevention is most effective when technology is embedded not only in technical systems but also in social practices and institutional strategies. Based on this perspective, the second research hypothesis (H2) is formulated to test the relationship between IT adoption and its effectiveness in reducing and preventing cybercrime.

H2: The use of actual technology has a positive effect on cybercrime prevention.

**Conditions that Facilitate and Prevent Cybercrime**

Research by Tim et al. (2024) defines facilitating conditions as environmental factors that help individuals perform certain behaviors more easily, a perspective also supported by Pee et al. (2008). In behavioral theory, intention alone does not guarantee action; an individual may intend to engage in a preventive behavior, but without an enabling environment, that intention may not translate into practice. Robinson (2010) strengthens this argument by noting that environmental barriers can directly obstruct individuals from carrying out desired actions, even when motivation and intention are present. In the context of cybercrime prevention, these facilitating conditions become particularly relevant as technology use and digital threats continue to expand.

Betts et al. (2014) identified several practical examples of facilitating conditions, including cybercrime awareness campaigns, implementation of clear information security policies, and the encouragement of preventive behaviors in remote work environments. These measures create a supportive structure that enables individuals and organizations to engage in cyber-safe practices. Thus, facilitating conditions not only bridge the gap between intention and action but also enhance the effectiveness of broader prevention strategies. Based on this reasoning, the third research hypothesis (H3) is proposed: facilitating conditions have a positive and significant influence on cybercrime prevention.

H3: Facilitating conditions have a positive influence on cybercrime prevention.

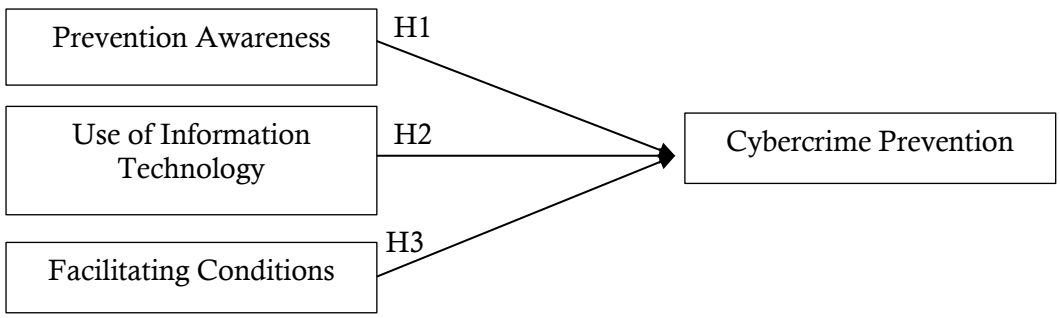


**Figure 1.** Research Methods

Based on Figure 1, this study develops a research framework that examines three key factors influencing cybercrime prevention. First, user awareness of cybercrime (H1) is expected to positively affect prevention efforts, as individuals who understand risks and threats are more likely to adopt secure behaviors. Second, the use of actual and up-to-date technology (H2) is hypothesized to strengthen prevention by enabling effective detection and mitigation of cyberattacks. Third, facilitating conditions (H3), such as supportive infrastructure and organizational resources, are assumed to enhance prevention by providing the necessary environment for timely and efficient responses. Together, these factors form an integrated framework that explains how awareness, technology utilization, and facilitating conditions collectively contribute to strengthening cybercrime prevention.

## RESEARCH METHODS

The quantitative method used in this study involved statistical testing assumptions through a series of data quality tests, research models, and hypotheses with SEM PLS tools (Hair et al. 2014). Data collection was carried out using questionnaires (physical and virtual) and obtained data from 208 questionnaires filled out by respondents from companies that manage finances, such as online loans, leasing, and banking, conducted between June and August 2025, using incidental sampling (Sugiyono, 2017). Researchers gave questionnaires to objects who happened to be met while conducting observations on a number of research objects in the Greater Jakarta area (Jakarta, Bogor, Tangerang, and Depok).

The data obtained from 208 questionnaires were then processed through several stages using SEM-PLS. The first stage is a data quality test, including convergent validity (seen from the value of loading factor, AVE, and communality) and discriminant validity to ensure that each construct is measured appropriately. The second stage is a reliability test using Composite Reliability and Cronbach's Alpha values to ensure that the instrument is consistent. Furthermore, an evaluation of the measurement model (outer model) was carried out to assess the relationship between the indicator and the construct, then an evaluation of the structural model (inner model) was carried out to see the strength of the relationship between latent variables through the values of $R^2$, $Q^2$, and to test the significance of the path by bootstrapping. The final stage is the hypothesis test, which is done by looking at the path coefficient and t-statistic values of the bootstrapping results to determine whether the hypothesis is accepted or rejected.

The dependent variable, cybercrime prevention, is measured through dimensions of user awareness, technological awareness, and the role of authorities, expanded with additional indicators reflecting novelty learning avoidance techniques from non-victims, regularly checking bank accounts, telecommunications vigilance, and reporting incidents to the police (Chatterjee et al., 2019; Wilson et al., 2023). The independent variable, perceived awareness of cybercrime, includes dimensions of understanding various forms of cybercrime, recognizing the importance of such knowledge, and overall awareness, further developed with elements of continuous knowledge updating and security consciousness. The variable of perceived technology use is assessed through technology training, training adequacy, and the extent of technology utilization, enhanced by the inclusion of updated technology adoption. Meanwhile, the facilitating conditions variable is measured through aspects such as remote campaigns, cybersecurity policies for remote work, supervision of remote human resources, and sufficient access provision (Tim et al., 2024).

## RESULTS

The results of data collection through questionnaires show that 208 respondents filled out the questionnaire for this study, originating from various institutions or companies engaged in financial services or whose fields of work are related to financial transactions. The number of questionnaires is less than the planned target of 448. However, if referring to the opinion of Hair et al. (2019) regarding the adequacy of research data using primary

data, at least having a sample quantity 10 times (240) or at least 5 times (120) of the number of indicators in the study can also be accepted. The largest number of indicators in this crime prevention variable is 24, so if using the minimum assumption, it certainly has enough to be used in its processing. Based on the results of the research data identification, the following demographic description of the research sample was obtained in Table 1.

**Table 1.** Sampling Demographic

| Demographic | Type | Value |
|---|---|---|
| Gender | Male | 49% |
| | Female | 51% |
| Age | 20-30 | 49% |
| | 31-40 | 19% |
| | >41 | 32% |
| Education | Highschool | 29% |
| | Bachelor | 41% |
| | Master | 20% |
| | Doctoral | 10% |
| Work Experience | 3-10 | 59% |
| | 11-20 | 24% |
| | 21-30 | 14% |
| | >41 | 2% |

Gender demographics indicate that the majority of those filling out this questionnaire are female, while the age of the majority of questionnaire respondents is 20-30 years old. The majority of educational levels are at the undergraduate level, with the majority of work experience being 3-10 years. Based on the demographic data of questionnaire respondents, it can be concluded that the workers in the financial sector in this study sample are female, with the productive age of workers being 20-30 years old, the highest level of education is undergraduate, at this level it proves that in the sector of operational and control systems related to finance are carried out by undergraduate graduates.

**Table 2.** Data Quality Test Results and Research Model

| Variable | Min | Max | Mean | Std Dev. |
|---|---|---|---|---|
| Cybercrime Prevention (CP) | 1 | 6 | 4.54 – 5.58 | 0.73 – 1.32 |
| Cybercrime Awareness (CA) | 1 | 6 | 4.93 – 5.31 | 0.85 -0.99 |
| Use of Information Technology (UIT) | 1 | 6 | 4.50 – 5.18 | 0.84 – 1.35 |
| Facilitating Conditions (FC) | 1 | 6 | 4.77 – 5.13 | 0.85 – 1.03 |

Table 2 shows descriptive results of four research variables related to cybercrime prevention. The mean values for all variables range between 4.5 and 5.5, indicating relatively high levels. Cybercrime Awareness (CA) shows the highest mean (4.93–5.31), suggesting strong awareness of cybercrime among respondents. In contrast, the Use of Information Technology (UIT) records the lowest mean range (4.50–5.18), though still within a moderately high level. The standard deviations range from 0.73 to 1.35, reflecting moderate variation in responses. The findings indicate that respondents demonstrate good levels of awareness, technology use, and facilitating conditions in supporting cybercrime prevention.

Table 3 shows validity test using SPSS using the assumption of the guide value of the r product moment table where in a sample of around 200 it has a product moment value of 0.138, it can be concluded that all variables have a decent validity value because they have a validity value (r count) of at least 0.456 greater than 0.138, and the Cronbach Alpha reliability value of all variables shows above 0.70 namely 0.923 to 0.944, then with this range of values it is concluded that it is very strong (reliable) which can be continued in further testing (Nunnally & Bernstein, 1994).

**Table 3.** Validity and Reliability Test

| Variable | Cronbach Alpha | Validity | AVE | Composite Reliability | Rho_A | Note |
|---|---|---|---|---|---|---|
| Cybercrime Prevention (CP) | 0.933 | 0.456 – 0.691 | 0.727 | 0.899 | 0.812 | Goodfit |
| Cybercrime Awareness (CA) | 0.944 | 0.701 – 0.803 | 0.786 | 0.917 | 0.917 | Goodfit |
| Use of Information Technology (UIT) (36-46) | 0.923 | 0.499 – 0.801 | 0.749 | 0.899 | 0.814 | Goodfit |
| Facilitating Conditions (FC) | 0.943 | 0.691 – 0.829 | 0.825 | 0.950 | 0.932 | Goodfit |

In addition, the results of other model feasibility tests using SEM PLS provisions on several values , such as AVE, Composite Reliability, and Rho_A, indicate a very feasible value in the model to be continued in the next test (Ghozali & Latan, 2016; Hair et al., 2017). The interpretation of Table 2 presents the results of data processing that reflect the ability of variables in predicting their values. In the overall feasibility test on the instrument, it can be concluded that all questions/statements in the questionnaire are concluded to have strong values, with a total sample of 208.

**Table 4.** Hypothesis Testing

| Variable Relationship | Prediction | Coef. | P-Value | Sign. | Decision |
|---|---|---|---|---|---|
| Initial model multiple regression: | CCAo = 0.245CCP + 0.281FC + 0.248UIT | | | | |
| Cyber Crime Awareness (CCA) → Cyber Crime Prevention (CCP) | H1 + | 0.245 | 0.006 | Sig. 0.00 | Accepted |
| Facilitating Conditions (FC) → Cyber Crime Prevention (CCP) | H2 + | 0.281 | 0.006 | Sig. 0.00 | Accepted |
| Use of Information Technology (UIT) →Cyber Crime Prevention (CCP) | H3 + | 0.248 | 0.005 | Sig. 0.00 | Accepted |
| Multiple regression model developed: | CCA1 = 0.273CCP + 0.177FC + 0.420UIT | | | | |
| Cyber Crime Awareness (CCA) → Cyber Crime Prevention (CCP) | H1 + | 0.273 | 0.001 | Sig. 0.00 | Accepted |
| Facilitating Conditions (FC) → Cyber Crime Prevention (CCP) | H2 + | 0.177 | 0.032 | Sig. 0.00 | Accepted |
| Use of Information Technology (UIT) →Cyber Crime Prevention (CCP) | H3 + | 0.420 | 0.000 | Sig. 0.00 | Accepted |
| $R^2$ (1) | | 0.495 | | | Goodfit |
| $R^2$ (2) | | 0.655 | | | |

Based on Table 4, the results of the hypothesis test prove that all hypotheses proposed with positive assumptions can be accepted with a significance value range between 0.000 and 0.035, where this assumption is less than 0.05. All hypotheses proposed in this study are accepted based on the statistical hypothesis acceptance decision value, which serves as a guideline value in research in general.

Furthermore, a sensitivity test was conducted to determine the ability of the new measurements developed in this study to predict the variables developed. Based on the

sensitivity test of this study, it can be concluded that the development of measurements from the dependent variable of Cybercrime Prevention (CP), which includes the development of dimensions: Learning avoidance techniques from non-victims of crime, Always check bank accounts, Telecommunications, and Reporting to the authorities, stated that the novelty test on the variable was successful and acceptable. Then the development of other measurements on the Crime Prevention Awareness variable which includes: Awareness of updating knowledge and Awareness of security, was also stated to be acceptable, the predictive ability of the modified dimensions can be proven by the regression coefficient value on Prevention Awareness (PA) → CP is 0.245 where the value is smaller than 0.275, and is proven by the significance value of 0.001 which is smaller than 0.006.

The next variable developed is the Use of Information Technology (UIT), which was also modified in its measurement. The development of the measurement provided maximum results, as evidenced by the results of data processing showing that the new UIT measurement has a coefficient value and its significance has increased and strengthened. Statistical data processing is proven by the previous coefficient value being smaller than after the development of 0.248, which is smaller than 0.420, with a significance value that is also greater than 0.005, which is greater than 0.000. The test results are based on the output of statistical test results using SEM PLS. In addition to using regression and hypothesis tests, proof of the success of the development of new measurements can also be proven by the value of the coefficient of determination ($R^2$), where the initial measurement model before developing the variable measurement is smaller than after the variable has been modified by adding a number of dimensions.

## DISCUSSION

The study finds that awareness of cybercrime prevention has a positive and significant effect on reducing cybercrime, aligning with previous research emphasizing the importance of user and organizational awareness (Burns et al., 2004; Kim & Eastin, 2011; Singh, 2013; Hung & Lai, 2015; Chanuvai et al., 2016; Chatterjee et al., 2019; Ismaeel, 2025). Drawing on the Theory of Planned Behavior (TPB), awareness reflects beliefs, attitudes, intentions, and behaviors shaped by perceived cyber risks. Cybercrimes disrupt business stability and damage reputation, while weak employee awareness reduces organizational resilience (Anita & Tanujaya, 2023). In an increasingly digital society, user awareness of cyber risks determines the success of prevention efforts (Davis, 1989; Hikmany, 2024).

Phishing remains one of the most critical threats in the banking sector, exploiting psychological manipulation to access confidential data (Putri & Sugiyono, 2023; Aljaradat & Shukla, 2025). Limited awareness of phishing, smishing, and vishing, especially among users with low digital literacy, amplifies these risks (Prihanto & Usmar, 2024; Fitrian et al., 2025). Awareness-building initiatives, including government programs, organizational training, and law enforcement actions, have proven effective in mitigating threats (Aggarwal, 2015; Chatterjee et al., 2019; Tibi et al., 2019). In Indonesia, 8,831 cybercrime cases were recorded in 2023, highlighting incidents such as the Tokopedia and BRI Life data breaches, which caused severe economic and reputational losses (Rahakbauw, 2024).

The study also confirms that technological adequacy significantly enhances prevention, particularly in fraud detection within the banking sector (Roy & Prabhakaran, 2022). This finding supports prior evidence that technological advancement improves prevention effectiveness, with artificial intelligence adding predictive and analytical value (Biswas et al., 2020; Mandal & Amilan, 2023). Theories of Risk Perception and Protection Motivation explain that responses to cyber threats are influenced not only by technical skills but also by psychological and emotional perceptions. Technological progress and awareness have evolved concurrently, leading organizations to invest in preventive tools that improve operational efficiency (Halbouni et al., 2016; Nwankpa & Roumani, 2016; Prihatini, 2022; Zhan et al., 2024).

Technology plays a central role through the use of antivirus systems, encryption, multifactor authentication, and intrusion detection, supported by user vigilance (Chatterjee, 2019). The Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) demonstrate that perceived usefulness, ease of use, and social influence determine adoption. In emerging economies such as Indonesia, these factors shape users' engagement with preventive technology (Aljaradat & Shukla, 2025). Since cyber threats like phishing and identity theft continue to evolve, awareness-based interventions must complement technological safeguards (Hikmany, 2024).

Facilitating conditions also significantly influence cybercrime prevention by providing the necessary environment for effective implementation (Pee et al., 2008; Tim et al., 2024). Although Indonesia is not among the top 20 victim countries, it ranks as a major origin point for cybercrime, reflecting broader challenges in digital trust and governance across developing regions (Wati et al., 2024; Aljaradat & Shukla, 2025). Frameworks such as the Cybercrime Mitigation Framework (CCMF) underscore the role of modern infrastructure in threat detection and response (Yeboah-Ofori & Opoku-Boateng, 2023). Adequate facilitating conditions, ranging from digital policies to AI integration to motivate preventive action and reinforce resilience, particularly amid global digital transitions such as remote work during the COVID-19 pandemic (Rogers, 1975; Ajzen, 1991; Mugarura & Ssali, 2020; Fedyk et al., 2022; Pham et al., 2025).

The findings have significant implications for cybersecurity policy and practice in Indonesia. At the policy level, they highlight the need to strengthen national cybersecurity frameworks, promote public awareness, and foster collaboration among government, private, and educational sectors. At the organizational level, continuous training, an ethical digital culture, and effective monitoring systems are crucial to minimizing risks. Furthermore, enhancing digital literacy can reinforce national cyber resilience. Overall, this study contributes to both theoretical understanding and practical strategies for improving cybercrime prevention.

## CONCLUSION

The research has been conducted based on a good research methodology mechanism by conducting a series of statistical tests through assumptions established in the rule of thumb properly, through a number of uses of previous theories and research as support that produces an influence on all variables (CP, CA, UIT, FC), namely a positive and significant influence. The novelty of this research, which was previously planned, has been tested with a series of statistical procedures using SEM PLS, in a scenario, in the sensitivity test, showing that the development of research variables through dimensions produces a stronger value compared to the previous value.

To obtain better results in the future in measuring and predicting more comprehensive cybercrime prevention, it is necessary to modify the variables in this research model in the future, such as adding moderating variables that are able to control the strengths and weaknesses of the observed variables, more varied samples, and new variables that are observed with a practical and literature approach. As with the risks associated with using research data, research based primarily on questionnaires carries the potential for high levels of subjectivity among respondents when completing the questionnaire, coupled with potential conflicts of interest. Furthermore, the homogeneity of the initial research sample, which was limited to financial institutions, may prevent the results from being generalizable to other cases, and the relatively limited research timeframe. Future research should explore the moderating and mediating roles of organizational culture, digital literacy, and regulatory enforcement in strengthening the relationship between awareness, technological adequacy, and cybercrime prevention across different sectors and levels of digital maturity.

## REFERENCES

[1] Abbad, M. M. (2013). E-banking in Jordan. *Behavior and Information Technology*, *32*(7), 618–694.

[2] Aborisade, R. A. (2025). Nigerian criminology and the united nations sustainable development goals: Challenges, opportunities and directions. *International Annals of Criminology, 1*(2), 1-20.

[3] Adomi, E. E., & Igun, S. E. (2008). Combating cybercrime in Nigeria. *Electronic Library*, *26*(5), 716–725.

[4] Aggarwal, G. (2015). General awareness on cyber crime. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(8), 204–206.

[5] Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Process*. *50*, 179–211.

[6] Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683.

[7] Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime*, *27*(3), 945–958.

[8] Aljaradat, A., & Shukla, S. K. (2025). Trust and cybersecurity in digital payment adoption: socioeconomic insights from India. *Journal of Business and Socio-Economic Development*, *8(1), 1-12.*

[9] Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8(1)*, 137293–137311.

[10] Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. *Sustainability (Switzerland)*, *15*(15), 1-10.

[11] Anita, F. & Tanujaya, K. (2023). Pengaruh kejahatan siber terhadap kinerja organisasi dengan moderasi kesadaran keamanan informasi. *Jurnal Ekuilnomi*, *5*(2), 266–275.

[12] Aparna, M., & Chauhan, M. (2012). Preventing cyber crime: A study regarding awareness of cyber crime in tricity. *International Journal of Enterprise Computing and Business Systems*, *2*(1), 1–10.

[13] Bashir, I., & Madhavaiah, C. (2015). Consumer attitude and behavioural intention towards Internet banking adoption in India. *Journal of Indian Business Research*, *7*(1), 67–102.

[14] Betts, T. K., Setterstrom, A. J., Pearson, J. M., & Totty, S. (2014). Explaining cyberloafing through a theoretical integration of theory of interpersonal behavior and theory of organizational justice. *Journal of Organizational and End User Computing*, *26*(4), 23–42.

[15] Biswas, S., Carson, B., Chung, V., Singh, S., & Thomas, R. (2020). *AI-bank of the future: Can banks meet the AI challenge*. New York: McKinsey & Company.

[16] Burns, R., Whitworth, K., & Thompson, C. (2004). Assessing law enforcement preparedness to address internet fraud. *Journal of Criminal Justice*, *32*(5), 477–493.

[17] Chang, M. K., & Cheung, W. (2001). Determinants of the intention to use Internet/www at work:a confirmatory study. *Information & Management*, *39*(1), 1–14.

[18] Chanuvai N., A., & Shah, V. (2016). Cyber crime and security – a study on awareness among young netizens of Anand (Gujarat State, India). *Ijariie*, *6(1)*, 2395–4396.

[19] Chatterjee, S. (2019). Is data privacy a fundamental right in India?: An analysis and recommendations from policy and legal perspective. *International Journal of Law and Management*, *61*(1), 170–190.

[20] Chatterjee, S., Kar, A. K., Dwivedi, Y. K., & Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. *Information Technology and People*, *32*(5), 1153–1183.

[21] Chen, D. T., Lin, T. B., Li, J. Y., & Lee, L. (2018). Establishing the norm of new media literacy of Singaporean students: implications to policy and pedagogy. *Computers and Education, 124(1)*, 1–13.

[22] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Research Center, University of Minnesota*, *13*(3), 319–340.

[23] Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. Retreieved on May 1 2025 from *arXiv preprint arXiv:1502.03552.*

[24] Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs. *Police Practice and Research*, *19*(6), 537–549.

[25] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(1), 32–64.

[26] Eshra, S. A., Zohora, F. T., Akter, S., Rasul, I., & Hossain, A. (2025). The role of threat intelligence in preventing financially motivated cyberattacks. *Journal of Engineering and Computational Intelligence Review*, *3*(2), 20-37.

[27] Farooq, M. S., Salam, M., Jaafar, N., Fayolle, A., Ayupp, K., Radovic-Markovic, M., & Sajid, A. (2017). IAcceptance and use of lecture capture system (LCS) in executive business studies: extending UTAUT2. *Interactive Technology and Smart Education,* 14(4), 329-348.

[28] Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies*, *27*(3), 938–985.

[29] Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Reading, MA: Addison-Wesley.

[30] Fitrian, H. P., Abidah, L., Zahra, K. W., & Hafidudin, W. H. (2025). Pengaruh kesadaran pengguna

terhadap keberhasilan serangan phishing di jaringan perbankan. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 1888–1892.

[31] Furnell, S., & Dowling, S. (2019). Cyber crime: a portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, *5*(1), 13–26.

[32] Ghozali, I., & Latan, H. (2016). *Partial Least Squares : Konsep, Teknik dan Aplikasi Menggunakan Program SmartPLS 3.0.* Semarang: Universitas Dipenogoro Press

[33] Guriting, P., & Ndubisi, N. O. (2006). Borneo online banking: evaluating consumer perceptionsand behavioral intentions. *Management Research News*, *29*(1/2), 6–15.

[34] Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Thiele, K. O., & Thiele, K. O. (2017). Mirror , mirror on the wall : a comparative evaluation of composite-based structural equation modeling methods. *Journal of the Academy of Marketing Science*.

[35] Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. In *European Business Review* , 31(1), 1-10.

[36] Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling ( PLS-SEM ) An emerging tool in business research. *European Business Review*, *26*(2), 106–121.

[37] Halbouni, S. S., Obeid, N., & Garbou, A. (2016). Corporate governance and information technology in fraud prevention and detection. *Managerial Auditing Journal*, *31*(6), 589-628.

[38] Hikmany, A.-N. (2024). A legal analysis of the land planning authorities and sustainable tourism in Zanzibar. *SSRN Electronic Journal*, *11(1), 1-13.*

[39] Hsu, T. C., Chang, S. C., & Hung, Y. T. (2018). How to learn and how to teach computational thinking: suggestions based on a review of the literature. *Computers and Education*, *126*(1), 296–310.

[40] Hung, Y. H., & Lai, H. Y. (2015). Effects of facebook like and conflicting aggregate rating and customer comment on purchase intentions. *International Conference on Universal Access in Human-Computer Interaction,* 193–200.

[41] Imani, T. A. N., & Prastyanti, R. A. (2025). The human firewall: Increasing digital awareness and literacy for consumer protection. *Ex Aequo Et Bono Journal of Law*, *3*(1), 1-17.

[42] Ismaeel, S. (2025). The impact of digital literacy on cybercrime awareness, victimization, and prevention measures: a study of cyberbullying in saudi arabia. *Pakistan Journal of Criminology*, *17*(01), 77–95.

[43] Kaur, B., Sood, K., & Grima, S. (2023). A systematic review on forensic accounting and its contribution towards fraud detection and prevention. *Journal of Financial Regulation and Compliance*, *31*(1), 60–95.

[44] Kesharwani, A., & Bisht, S. S. (2012). The impact of trust and perceived risk on Internet bankingadoption in India: an extension of technology acceptance model. *International Journal OfBank Marketing*, *30(4),* 303-322.

[45] Kim, S., & Eastin, M. S. (2011). Hedonic tendencies and the online consumer: an investigation of the online shopping process. *Journal of Internet Commerce*, *10*(1), 68–90.

[46] Kont, K. R. (2025). Measuring Information Security Awareness of Librarians: A Case Study from Estonia, Latvia and Lithuania. *Slavic & East European Information Resources*, 1(1), 1-26.

[47] Li, Q., Bu, B., & Zhao, J. (2025). An enhanced blockchain-based collaborative intrusion detection approach for CBTC systems. *Cluster Computing*, *28*(8), 518.

[48] Lindell, T. L. (2020). Teachers calling for organizational support to digitalize teaching. *The International Journal of Information and Learning Technology*.

[49] Longstaff, T. A., & Schultz, E. E. (1993). Beyond preliminary analysis of the WANK and OILZ worms: a case study of malicious code. *Computers and Security*, *12*(1), 61–77.

[50] Mandal, A., & Amilan, S. (2025). Preventing financial statement fraud in the corporate sector: insights from auditors. *Journal of Financial Reporting and Accounting*, *23*(1), 56-80.

[51] Mann, B. J. S., & Sahni, S. K. (2012). Profiling adopter categories of internet banking in india: an empirical study. *Vision: The Journal of Business Perspective*, *16*(4), 283–295.

[52] Mehta, S., & Singh, V. (2013). A study of awareness about cyberlaws in the Indian society. *International Journal of Computing and Business Research*, *4*(1), 1-8.

[53] Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, *24*(1), 10–28.

[54] Nunnally, J., & Bernstein, I. (1994). The assessment of reliability: psychometric theory. *Eval Rev*, *21*(1) 614-35.

[55] Nwankpa, J. K., & Roumani, Y. (2016). IT Capability and Digital Transformation: A Firm Performance Perspective. *Proceedings of Thirty Seventh International Conference on Information Systems, Dublin, Ireland*, 1(1). 1-10.

[56] Parmar, A., & Patel, K. (2016). *Critical study and analysis of cyber law awareness among netizens*. In S. Tiwari, K. Trivedi, K. Mishra, & A. Misra (Eds.), *Proceedings of the International Conference on ICT for Sustainable Development,* 317–326).

[57] Pee, L. G., Woon, I. M. Y., & Kankanhalli, A. (2008). Explaining non-work-related computing in the workplace: A comparison of alternative models. *Information and Management*, *45*(2), 10-21.

[58] Pham, H. H., Nguyen, T. H. L., Doan, V. A., & Tran, M. T. (2025). Audit quality of financial statements of commercial banks, whether or not there is a difference in audit quality provided by

big4 and non-big4 audit firms. *International Journal of Economics and Financial Issues* , *15*(1), 159–181.

[59] Popham, J., McCluskey, M., Ouellet, M., & Gallupe, O. (2020). Exploring police-reported cybercrime in Canada: variation and correlates. *Policing*, *43*(1), 35–48.

[60] Prihanto, H., & Usmar. (2024). Pengaruh regulasi, pengawasan, dan perilaku masyarakat terhadap efektivitas pencegahan pinjaman online ilegal. *Jurnal Akuntansi dan Bisnis Indonesia*, *5*(2), 115–128.

[61] Prihatini, D. (2022). Turnover auditor di kantor akuntan publik studi kasus pada salah satu kap big 4 (KAP "XYZ"). *Jurnal Akuntansi, Keuangan, Pajak Dan Informasi (JAKPI)*, *2*(2), 122–141.

[62] Putri, R. A. T. P., & Sugiyono, H. (2023). Tanggung jawab bank terhadap tindakan phising dalam sistem penggunaan e-banking ( studi : kasus phising pada Pt . Bank Rakyat Indonesia (PERSERO) TBK). *Jurnal Interpretasi Hukum*, *4*(3), 682–690.

[63] Rahakbauw, I. K. (2024). Analisis potensi ancaman siber pada bidang ekonomi di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *7*(1), 1-10.

[64] Rahim, S. A. A., Nawawi, A., & Salin, A. S. A. P. (2017). Internal control weaknesses in a cooperative body : Malaysian experience. *Int. J. Management Practice*, *10*(2), 131–151.

[65] Robertson, B., & Sribar, V. (2001). *The adaptive enterprise: IT infrastructure strategies to manage change and enable growth.* Reading, MA: Addison-Wesley Longman Publishing Co., Inc.

[66] Robinson, J. (2010). Triandis' Theory of Interpersonal Behaviour in understanding software piracy behaviour in the South African context. *Semantic Scholar*, *1(*1), 1–10

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

[68] Roy, N. C., & Prabhakaran, S. (2022). Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management*, *75*(2), 1-12.

[69] Scherer, R., Siddiq, F., & Tondeur, J. (2019). The technology acceptance model (TAM): a metaanalytic structural equation modeling approach to explaining teachers' adoption of digital technology in education. *Computers and Education*, *128*, 13–35.

[70] Singaravelu, S., & Pillai, K. P. (2014). Students awareness on cybercrime in Perambalur district. *International Journal of Teacher Educational Research*, *3*(3).

[71] Singh, H. (2013). Cybercrime–a threat to persons, property, government and societies. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5), 997–1002.

[72] Siregar, S. V., & Tenoyo, B. (2015). Fraud awareness survey of private sector in Indonesia. *Journal of Financial Crime, 22*(3), 329–346.

[73] Slovic, P. (1987). Perception of Risk. *Science*, *236*(4799), 280–285.

[74] Smith, K. T., Jones, A., Johnson, L., Smith, L. M., & Smith, L. M. (2018). Examination of cybercrime and its e ff ects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, 1(2), 1-10/

[75] Sorebo, A. M., Sorebo, O., & Sein, M. K. (2007). The influence of user involvement and personal innovativeness on user behavior. *International Journal of Industrial and Manufacturing Engineering*, *1*(8), 338–343.

[76] Sugiyono. (2017). *Metode Penelitian Kuantitatif, Kualitatif, R & D.* Bandung: Alfabeta.

[77] Symons, D., & Blannin, J. (2020). Empowerment and disempowerment in peer observation within pre-service teacher, technology-assisted integrated STEM Education. *Encyclopedia of Education and Information Technologies; Springer International Publishing:Cham, Switzerland*, 699–706.

[78] Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, *23*(2), 1–11.

[79] Tibi, M. H., Hadeje, K., & Watted, B. (2019). Cybercrime Awareness among Students at a Teacher Training College. *International Journal of Computer Trends and Technology*, *67*(6), 11–17.

[80] Tim, W., Ruhwanya, Z., & Ophoff, J. (2024). Using the theory of interpersonal behaviour to explain employees' cybercrime preventative behaviour during the pandemic. *Information and Computer Security*, *32*, 436–458.

[81] Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarter*, *36*(1), 157–178.

[82] Wang, B. C. L., & Ahmed, P. K. (2003). *Knowledge management orientation and organisational performance*. *44*(0).

[83] Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). Dampak cyber crime terhadap keamanan nasional dan strategi penanggulangannya: ditinjau dari penegakan hukum. *Jurnal Bevinding*, *2*(1), 44–55.

[84] Wilson, S., Hassan, N. A., Khor, K. K., Sinnappan, S., Abu Bakar, A. R., & Tan, S. A. (2023). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime*, *11*(1), 1-13.

[85] Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape. *Continuity & Resilience Review*, *5*(1), 1-12.

[86] Zaied, A. N. H. (2012). An integrated knowledge management capabilities framework for assessing organizational performance. *I.J. Information Technology and Computer Science*, *2*(1), 1–10.

[87] Zhan, H., Cheng, K. M., Wijaya, L., & Zhang, S. (2024). Investigating the mediating role of self-

efficacy between digital leadership capability, intercultural competence, and employability among working undergraduates. *Higher Education, Skills and Work-Based Learning*, *14*(4), 1-12.

[88] Zia, A., Memon, M. A., Mirza, M. Z., Iqbal, Y. M. J., & Tariq, A. (2024). Digital job resources, digital engagement, digital leadership, and innovative work behaviour: a serial mediation model. *European Journal of Innovation Management*, *1*(2), 1-12.