International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1577-1589
Journal homepage: http://iieta.org/journals/ijsse

Impact of 'Don't Know? Kasih No!' Campaign on Cybersecurity Awareness: Unraveling the Links to User Satisfaction, Trust, and Commitment

Arta Moro Sundjaja*, Ahmad Ridwan, Dewi Robbani, Rafly Ananda Soemantri

Management Department, Binus Business School Master Program, Bina Nusantara University, West Jakarta 11480, Indonesia

Corresponding Author Email: asundjaja@binus.edu

https://doi.org/10.18280/ijsse.140525

Received: 10 July 2024
Revised: 25 September 2024
Accepted: 9 October 2024
Available online: 31 October 2024

Keywords:
cybersecurity awareness, cyberattack threat, trust-commitment theory, user satisfaction, Don't Know? Kasih No!

ABSTRACT

The purpose of this study is to investigate the relationship between cybersecurity video campaigns, such as the "Don't Know? Kasih No!" campaign by Bank Central Asia, and their impact on cybersecurity awareness among online banking customers. This research integrates Uses-gratification Theory and Trust-Commitment Theory in the context of digital banking use in Indonesia, as studies examining the relationship between motivation and satisfaction towards cybersecurity video campaigns, cyberattack threats, and user trust and commitment to digital banking use are still limited. The research design is quantitative method using Partial Least Square Structural Equation Modeling (PLS-SEM) ver. 4.1.0.0. The researchers cannot determine the population size. Therefore, the sample size determination method is minimum 10 times of indicator, and the sample size is 259. The sampling method is convenience sampling with screening question. The results showed that content quality and social influence positively affect user satisfaction, while entertainment was not significant. User satisfaction with digital content has a positive impact on cyber security awareness, which further increases customer trust, even though perceived risk has a negative impact on trust. This finding is reinforced by very strong prediction results through PLS Predict testing. The rest of the results of the importance performance analysis show that the performance of content quality and entertainment needs to be maintained, while cyber-attack awareness, social influence, transaction risk perception, and user satisfaction need to be improved. This study integrates Uses-Gratification Theory with Trust-Commitment Theory to explain the impact of cybersecurity education content in Indonesia, and uses cutting-edge data analysis procedures.

1. INTRODUCTION

The digital banking revolution has brought about a transformative shift in the financial services landscape, offering unprecedented convenience and accessibility. However, this shift also introduces new challenges, most notably the rise of cybercrimes. have underscored the prevalence of cybersecurity breaches in Internet banking, emphasizing the critical role of customer education in preventing unauthorized account access. Similarly [1], have identified the escalating threat of cybercrime in the banking sector, highlighting the urgent need to bolster cybercrime awareness among customers to mitigate the risks associated with financial crimes in digital banking.

Cybersecurity in the banking sector is a critical area of focus, given the increasing reliance on digital platforms for financial transactions. Cybersecurity breaches in banking have become a significant concern, with cybercriminals employing sophisticated techniques to exploit vulnerabilities in online banking systems. These breaches can lead to unauthorized access to customer accounts, identity theft, and financial fraud, posing a direct threat to both individuals and institutions. Users may inadvertently provide personal information or click on malicious links, enabling cybercriminals to gain access to sensitive data. The complexity and evolving nature of cyber threats necessitate a comprehensive approach to cybersecurity education and awareness. This includes not only technical measures to secure digital platforms but also psychological strategies to enhance users' awareness and vigilance against potential threats. By understanding the mechanisms of cyberattacks and the psychological factors that influence users' behavior, banks and financial institutions can develop more effective strategies to protect their customers and mitigate the risks associated with cybercrime in the digital banking environment.

Customer trust is a cornerstone of the banking industry, often predicated on the psychological environment shaped by customers' expectations of products and services, as well as the perceived security measures in place to meet these expectations. The growing reliance on online banking transactions has the potential to reshape customers' trust in banks [2, 3]. These studies found a positive correlation between consumer trust and general information about banking technology systems, yet they also revealed evidence suggesting that a lack of trust may stem from internet banking. Consequently, further research is essential to advance the

dialogue about customer confidence in the banking sector, particularly in the context of digital transactions.

The importance of cybersecurity education is widely acknowledged, yet existing courses often focus on formal teaching, which may not be engaging for beginners. The previous research has recognized the need for interactive consumer education tactics that create a motivated learning environment to effectively engage audiences and simplify knowledge acquisition [4]. The researchers identify the research problem based on observation of mobile apps and entertaining videos application as innovative educational tools for cybersecurity awareness. In Indonesia, BCA has employed an entertaining video titled "Don't Know? Kasih No!" to educate consumers about cybersecurity. However, there is a limited studies that explore the use of other entertaining videos for this purpose.

The research objective is to investigate the relationship between cybersecurity video campaigns, such as the "Don't Know? Kasih No!" campaign by BCA, and their impact on cybersecurity awareness among online banking customers. This study employs the Uses-Gratification Theory to analyze the effectiveness of these campaigns in satisfying customer needs and desires, which in turn influences their satisfaction and trust. Additionally, the study examines the trust-commitment framework within the context of online banking customers, drawing on the Commitment-Trust Theory to understand how trust mediates the relationship between cyberattack awareness, cybersecurity measures and customer satisfaction to commitment, and on how user satisfaction mediate the relationship between perceived content quality, perceived social influence and perceived entertainment to cyberattack awareness. The findings are expected to contribute to the development of more effective educational campaigns and strategies for enhancing cybersecurity awareness among online banking customers, ultimately fostering a more secure and trustworthy digital banking ecosystem.

2. LITERATURE REVIEW

2.1 Trust - commitment theory

The Trust-Commitment theory was developed by Morgan and Hunt in 1994 in the context of relationship marketing [5]. The focus of this theory is to emphasize the importance of trust and commitment as two key elements that drive the success of long-term relationships between the parties involved [6]. The definition of trust is the belief in the integrity and reliability of the other party, while commitment is defined as a willingness to maintain a valuable relationship and invest resources to maintain the relationship [5]. In the context of using mobile banking, trust and commitment are the main pillars in building long-term relationships between customers and service providers [7]. Trust can be defined as a customer's confidence in mobile banking services can provide a sense of security, reliability, and be able to protect personal information from cybersecurity threats [8]. Meanwhile, commitment is an outcome based on a strong level of trust so that customers want to maintain relationships with service providers and use the banking services for a long period of time [9].

Awareness of the potential for cyberattacks plays an important role in shaping user trust [10]. The high awareness of cyber threats makes users cautious when using the service, which can reduce the trust level if the service is considered insecure [8]. However, through effective education efforts using social media, users can better understand the protection measures that need to be taken, so that their trust in mobile banking services increases [11, 12]. In addition, the perception of transaction risk also affects user trust and commitment [13]. Users who feel that the risk of transactions on mobile banking has increased can cause reluctance to use the service [8]. However, trust built through awareness of cyberattacks and cybersecurity measures can reduce this perception of risk, thereby increasing users' commitment to using mobile banking on an ongoing basis [14]. If users have a strong trust in mobile banking, then users tend to commit to using the service for a long period of time [15].

Trust-Commitment Theory is the right theoretical framework to explain the relationship between trust and commitment in using mobile banking. As threats to cybersecurity increase, the role of organizations in developing cybersecurity and reducing transaction risk with mobile banking can increase user trust. Therefore, customer trust in service security is an important factor for users to commit to using mobile banking. The strategy of educating users with digital storytelling through social media can increase cybersecurity awareness so that it is expected to increase user trust and commitment.

2.2 Extending trust and commitment theory with uses-gratification theory

The Uses-Gratification Theory (UGT) was introduced in the early 1940s in response to the traditional view that the audience is the passive recipient of media messages [16]. This view originated from Media Effect Theory where the media has a direct influence on the attitude and behavior of the audience [17]. However, UGT was developed in the 1970s which emphasized that the audience is an active agent who consciously chooses media to meet their psychological or social needs [18]. This theory highlights that cognitive, affective, personal, and social needs can be met through media consumption, and ultimately satisfaction with the choice of media is formed.

Along with the development of technology and digital media, UGT has been adapted to explain interaction with the internet and social media [19]. In the context of the internet and social media, this theory remains relevant because internet and social media users are looking for content that suits their needs [20, 21]. In addition, UGT has been used to understand motivation for activities in sharing information through online streaming service [21], playing online games [22], problematic smartphone use [23], information security education [24, 25], fake news [26-28], and cyberbullying [29]. Therefore, trends of UGT application in the context of problematic use of social media and smartphone is emerging.

Problematic smartphone use can lead to illegal activities, such as misuse of personal data or unauthorized access to digital networks [23]. In addition, the use of smartphones can facilitate criminal activities through cyberbullying, online fraud or cybercrime [30]. Previous research has shown that social motivation and self-expression have an important role in encouraging social media users to interact with and spread fake news even as they seek fact-checking to ensure the authenticity of the news [27]. This can be suppressed by applying the principle of caution to social media users [28]. Therefore, information security education is important to reduce the risk of the impact of problematic smartphone use

[31]. The success of information security education is influenced by the satisfaction of social media users with the quality of content that is presented attractively so that it has the potential to be disseminated on a wider scope [24].

The satisfaction of social media users with the cybersecurity education video campaign "Don't Know Kasih No" can be explained by using Uses Gratification Theory. The theory can explain the relationship between content quality, entertainment elements, and social influence on satisfaction with educational content. Therefore, the researcher concluded that UGT is a relevant framework to understand how the education campaign can increase customer and public awareness and behavior of cybersecurity.

2.3 Hypothesis development

2.3.1 Perceived content quality and user satisfaction

Previous research has examined the relationship between perceived content quality and user satisfaction [32-34]. When users judge that educational video content related to cyber security is accurate and reliable, users will feel safer in using mobile banking services [32]. In addition, scenarios in cyber security education videos developed from real cases and can be verified, users tend to be more confident that they are receiving the correct information [33]. Ultimately, users who have watched educational videos about cyber security find the content useful and relevant, they will feel satisfied with new insights and a better understanding of how to protect against the threat of cyberattacks [34, 35]. Thus, this study posited the hypothesis as follows:

H_1: Perceived Content Quality positively affects user satisfaction

2.3.2 Perceived social influence and user satisfaction

Previous research has examined the relationship between social influence and user satisfaction [36-38]. Social media provides access to educational content to increase users' knowledge and confidence in protecting themselves online [36]. Enhanced user preparedness in addressing cybersecurity risks resulting from exposure to social media information tends to positively influence their satisfaction with their choice to utilize mobile banking services [37]. In addition, the inclusion of social media platforms in facilitating social connection and engagement within friend groups is exerting an impact on the acceptance of mobile banking, particularly by means of recommendations and dissemination of cybersecurity educational videos [38]. This social influence can increase their perception of the security and benefits of mobile banking services, thereby increasing their satisfaction [39]. Thus, this study posited the hypothesis as follows:

H_2: Perceived Social Influence positively affects user satisfaction

2.3.3 Perceived entertainment and user satisfaction

Previous research has examined the relationship between perceived entertainment and user satisfaction [39-42]. When users enjoy educational video content about cyber security, the absorption of information will be more effective [40]. Perceived entertainment can be influenced by attractive visuals, a compelling storyline, the right use of humor, and interactive delivery [40, 41]. When all aspects of entertainment perception are fulfilled, users will pay more attention and understand the message conveyed [42, 43]. This will encourage users to apply the information they get from the videos to their daily practices, ultimately increasing their satisfaction with mobile banking [39]. Thus, this study posited the hypothesis as follows:

H_3: Perceived Entertainment positively affects user satisfaction

2.3.4 User satisfaction and cyber attack awareness

Previous research has examined the relationship between user satisfaction and cyber-attack awareness [44-47]. High satisfaction with educational content about cyber security will increase awareness of cyber threats [44]. A good cyber security education video requires relevant and up-to-date content design, clear and simple storytelling, and the right duration [45, 48]. Satisfied customers tend to receive new information submitted by the bank [46]. For example, satisfaction with education about threats and mitigation of potential phishing attacks through social media will add to the positive customer experience when using digital banking services [49]. In addition, customers are also motivated to learn and follow additional security measures to be safer using digital banking services [47]. Thus, this study posited the hypothesis as follows:

H_4: User satisfaction positively affect cyber-attack awareness.

2.3.5 Transaction risk perception and customer trust

Previous research has examined the relationship between transaction risk perception and customer trust [8, 14, 50, 51]. The higher the customer's concern about the security of the transaction, the lower the customer's trust in digital banking services [14]. When customers feel that mobile banking services are not safe due to the potential for data theft or unauthorized access by hackers, phishing threats, and malware threats, then they will be reluctant to use the service [8, 51]. If banks fail to convince customers that their digital services are secure, then customers will choose to avoid using mobile banking or switch to conventional banking [50]. Therefore, customer confidence in the security of banking transactions is influenced by the bank's ability to manage and reduce transaction risk perception [14]. Thus, this study posited the hypothesis as follows:

H_5: Transaction risk perception negatively affect customer trust

2.3.6 Cyber-attack awareness and customer trust

Previous research has examined the relationship between cyber-attack awareness and customer trust [8, 35, 44, 51, 52]. The use of cyber security education videos to enhance consumer knowledge of the potential of cyber assaults can increase customer trust to believe in the security measures that have been implemented by the bank [8, 44]. When customers understand that banks are the target of cyberattacks, customers will be worried about the security of their data [10]. In addition, when customers understand the source of the threat of cyberattacks and how to protect themselves from cyberattacks, customers will trust digital banking services [51]. Ultimately, knowledge and experience of the threat of cyberattacks is an important factor in building customer trust [35]. This is due to transparency on the threat and impact of cyberattacks and how banks are committed to mitigating and responding to such cyberattacks [53]. Thus, this study posited the hypothesis as follows:

H_6: Cyber attack awareness positively affect customer trust

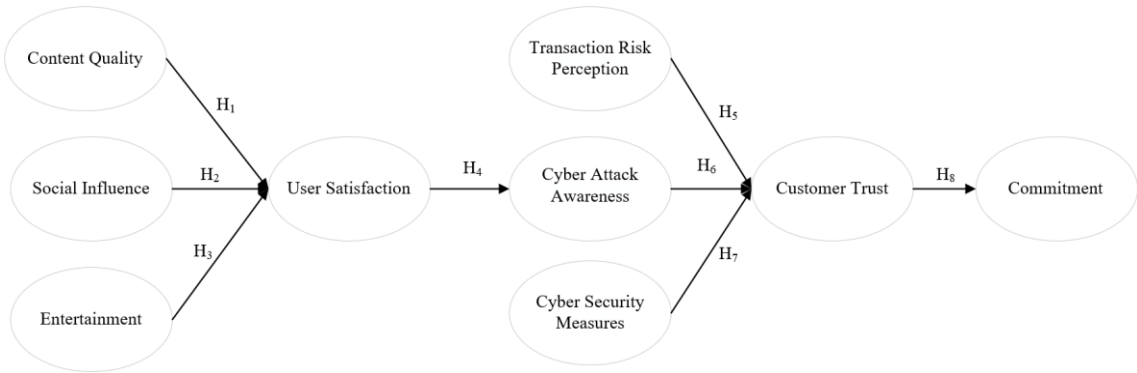

Figure 1. Research model

2.3.7 Cyber security measures and customer trust

Previous research has examined the relationship between cyber security measures and customer trust [8, 54, 55]. When customers know that the bank has taken appropriate security measures against cyber threats, customers are more confident in the digital banking services offered [8, 56]. Banks that proactively communicate the security protocols required of customers can enhance customer understanding and compliance with these measures, thereby contributing to increased confidence in the bank's ability to protect them from cyber threats [55]. Utilizing educational video content on cybersecurity promotes the use of robust passwords, adoption of two-factor authentication, and avoidance of divulging personal information to unfamiliar persons can alleviate fears and improve customer satisfaction [54]. Thus, this study posited the hypothesis as follows:

H_7: Cyber security measures positively affect customer trust

2.3.8 Customer trust and commitment

Previous research has examined the relationship between customer trust and commitment [37, 49, 57, 58]. When customers have strong trust in their banks, their commitment to continue using digital banking services is even stronger [37]. Conversely, when trust in digital banking services is lost, customer commitment can be reduced as customers feel insecure and disappointed after a cyberattack [49]. Cyber security education videos designed to strengthen customer trust can help mitigate negative impacts by demonstrating banks' efforts to improve and improve security after an incident [58]. Therefore, it is important for banks to use effective cyber security education videos to maintain and restore customer trust, so that their commitment to digital banking services remains strong [57]. Thus, this study posited the hypothesis as follows:

H_8: Customer trust positively affect commitment

Figure 1 shows the proposed research model. The model was developed based on the utilization of Trust - Commitment Theory in the context of mobile banking usage post cyber-attack risk. The researchers extend the Trust - Commitment theory with the transaction risk perception, cyber attack awareness, cyber security measures, and the customer motivations of consuming cyber security awareness educational content.

3. MATERIAL AND METHODOLOGY

Research design is a quantitative approach using cross sectional study. The study setting is non-contrived setting with the customer bank as unit of analysis. The data analysis method is structural equation modelling with SmartPLS version 4.1.0.3. The researchers selected the data analysis method and software due to the complexity of the proposed model and it's commonly used for examining the theories formulation, especially in digital storytelling of cyber security awareness.

The researchers cannot determine the population size due to limited access to the data. Therefore, the sampling technique is convenience sampling. Since convenience sampling has potential issues on selection bias. The researchers apply screening questions. The selection criteria are the respondent have watch digital content with title "Don't Know? Kasih No!" in social media. The data collection method is an online survey using Google Form. The sample size determination method is 10 times the indicator. Total indicator in this study is 25 items. Therefore, the minimum sample size is 250 respondents. The researchers distributed the questionnaire through social media and whatsapp groups.

The questionnaire was structured into two main sections. The first section consists of demographic respondent profile. The second section focused on the variables under study, including cybersecurity measures [10], transaction risk perception [10], user satisfaction [59, 60], customer trust [10], commitment [61, 62], cyberattack awareness [10], perceived content quality [63], perceived entertainment [63, 64], and perceived social influence [65]. The researchers used likert scale ranging 1 (strongly disagree) and 5 (strongly agree).

Since the items were modified from the previous study, the researchers conduct preliminary investigation by inviting three scholars that are experts in marketing, management and information systems to review the items. The scholars provide inputs for increasing clarity, refining the question format, and decreasing the ambiguity. In addition, a consent statement was included at the beginning of the questionnaire, by informing the research objective, privacy and data security policy, researchers name and contact information, respondent right, data for publication purposes, and respondent approval.

The previous research proposed a conceptual paradigm that employs a reflective approach [66]. The data was assessed using internal consistency, factor reliability, convergent validity, and discriminant validity [67]. The structural model and its corresponding hypothesis were assessed after the confirmatory factor analysis phase was effectively completed and all necessary conditions were met [67]. Additionally, the predictive capability of the proposed model was assessed using the PLS-Predict method [68]. The importance-performance map analysis (IPMA) was undertaken to identify predecessors that were of high importance to the target structures but had comparatively low performance [69]. The results and discussions section provided additional detail on

the comprehensive protocol.

4. RESULTS AND DISCUSSIONS

First, the researchers perform data screening using the standard deviation function in Ms. Excel to ensure the data quality [70]. The researchers collect 282 data and remove 23 data. Therefore, the researchers used 259 data for final analysis. Table 1 presents a descriptive analysis of the respondent profile. Based on the age group, 103 respondents (39.8) were between 25 and 35 years old, 118 respondents (45.7%) were over 35 years old, and 37 respondents (14.4%) were under 25 years old. Based on the marital status, 168 respondents (65%) are married, and 90 respondents (34.9%) are still single. Based on the education background, 212 respondents (82.1%) have completed a bachelor's degree, 22 respondents (8.1%) have completed a master's degree, 13 respondents (5%) have completed high school or equivalent, and 11 respondents (4.2%) have completed a diploma degree.

Table 1. Descriptive analysis of respondent profile

Item	N	%
Age Group		
25-35 y.o	104	40.15%
Above 45 y.o	65	25.10%
35-45 y.o	53	20.46%
Below 25 y.o	37	14.29%
Marital Status		
Married	168	64.86%
Single	91	35.14%
Education		
Bachelor's Degree	213	82.24%
Master's Degree	22	8.49%
Highschool or Equivalent	13	5.02%
Diploma	11	4.25%
*N=259		

Next, the researcher performs a common method bias to ensure the reliability and robustness of findings [71]. This is due to research that relies on survey data where the variance produced in the study is caused by the data collection method rather than the measured construct. The researcher conducted a collinearity test using SmartPLS, the cut-off value used was less than 3.3 [72]. The researcher created a dummy variable and conducted a regression analysis to test all the research variables against the dummy variable. The results of the collinearity test are presented in Table 2. The internal VIF measurement is in the value range of 1,065 (social influence) to 1,880 (cyber-attack awareness). This indicates that the bias procedure does not affect the accuracy of the results of the study.

Next, the researchers perform the data normality test by examining skewness and kurtosis values from SmartPLS software [66]. The cut-off value for skewness and kurtosis values are ± 1 [73]. Table 3 shows the normality test results using skewness and kurtosis value. Most indicators did not meet the criteria for normality test. Therefore, the researchers conclude that the data is not normally distributed. The SmartPLS usage allows the researchers to perform the data analysis even if the data is not normally distributed [74]. However, the researchers need to perform bias-corrected and accelerated bootstrapping (BCa) to ensure that the highly skewed or kurtosis data does not affect the PLS estimate [75].

The researchers examine confirmatory factor analysis by evaluating individual reliability, convergent validity, and discriminant validity [76]. Table 3 shows individual reliability, convergent validity, and internal consistency reliability. First, the researchers evaluate individual reliability using outer loading value. the cut-off value of outer loading is 0.6 [66]. The researchers conclude that 25 indicators meet the cut-off value with a range from 0,618 (CA2) to 0,925 (US2). Second, the researchers inspect internal consistency reliability using composite reliability (CR). The cut-off value of CR is 0.7 [66]. The researchers conclude that all variables meet the CR criteria ranging from 0,747 (Cyber-attack awareness) to 0.905 (Entertainment). Third, inspect the convergent validity using the Average Variance Extracted (AVE). The cut-off value of AVE is 0.5 [66]. Therefore, the researchers conclude that all variables meet the criteria ranging from 0.525 (Cyber-attack awareness) to 0.827 (Entertainment).

Discriminant validity is the final stage of confirmatory factor analysis and is essential for examining the connection between latent variables, grouped as a subcategory of construct validity [66]. The researchers employ Fornell-Larcker criterion for evaluating discriminant validity evaluation [77]. The justification for the selection of these criteria is because the criteria are more pragmatic and easier to understand. The researchers compared the square root of the Average Variance Extracted for each construct with the correlation between the constructs. Table 4 shows the discriminant validity analysis using Fornell-Larcker criterion. Based on the findings, the researchers conclude that the results of the discriminant validity test have met the criteria.

Next, the researchers examine the path analysis using bootstrapping features. The bootstrapping parameter is as follows: One-tailed test, sub-sample size is 5,000, bias-corrected and accelerated (Bca) bootstrap, and significance level 5%. Moreover, the f^2 statistics were used to demonstrate the impact of independent variables on the dependent variables. Different levels of effect are presented as follows; high ($f^2 > 0.350$), moderate ($f^2 > 0.150$), and small ($f^2 > 0.020$) [78]. Table 5 shows the hypothesis test result.

Based on the hypothesis testing results, content quality (H_1, $\beta = 0.390$, t-stat = 3.810, small effect) and social influence (H_2, $\beta = 0.184$, t-stat = 2.854, small effect) positively affect user satisfaction. However, entertainment (H3, $\beta = 0.112$, t-stat = 1.078, no effect) was not significant. User satisfaction positively affects cybersecurity awareness (H_4, $\beta = 0.418$, t-stat = 6.726, moderate effect). Moreover, cybersecurity measures (H_7, $\beta = 0.490$, t-stat = 6.386, moderate effect) and cybersecurity awareness positively affect customer trust (H_6, $\beta = 0.160$, t-stat = 2.690, small effect). However, transaction risk perception negatively affects customer trust (H_5, $\beta = -0.177$, t-stat = 3.584, small effect). Finally, customer trust negatively affects commitment (H_8, $\beta = -0.251$, t-stat = 4.304, small effect).

Table 2. Full collinearity estimate

	1	2	3	4	5	6	7	8	9
VIF	1.327	1.228	1.587	1.880	1.190	1.228	1.065	1.403	1.549

1 = Commitment; 2 = Content quality; 3 = Customer trust; 4 = Cyber-attack awareness; 5 = Cyber security measure; 6 = Entertainment; 7 = Social influence; 8 = Transaction risk perception; 9 = User satisfaction

Table 3. Normality, individual indicator consistency, convergent validity, and internal consistency reliability

Variable and Indicator	1	2	3	4
Cyberattack Awareness (AVE = 0.525, CR = 0.766): I am familiar with the term cybersecurity. [CA1]	4.309	-1.463	2.409	0.822
I am aware of the new cyber-attacks on banks in Indonesia. [CA2]	4.729	-2.478	6.816	0.618
I know that banks are a target in cyber-attacks. [CA4]	4.757	-3.008	11.524	0.719
Commitment (AVE = 0.658, CR = 0.885): After the cyber-attack, I feel insecure when making banking transactions via mobile. [CO1]	4.649	-2.526	8.287	0.839
After the cyber-attack, I feel insecure when making online banking transactions. [CO2]	4.517	-1.623	2.567	0.833
My level of trust has decreased after the cyber-attack on the bank. [CO3]	4.587	-2.604	8.355	0.815
As a result of this cyber-attack, I feel disappointed with online banking services. [CO4]	4.537	-1.277	1.084	0.754
Content Quality (AVE = 0.596, CR = 0.853): The content "Don't Know? Give No" is accurate. [CONT1]	1.829	1.187	0.433	0.860
The content "Don't Know? Give No" is factual. [CONT3]	3.486	-0.574	-1.004	0.776
The content "Don't Know? Give No" is informative. [CONT4]	3.232	-0.311	-1.273	0.823
Cybersecurity Measure (AVE = 0.601, CR= 0.747): I prefer to use online banking services regularly. [CS1]	4.606	-1.397	1.366	0.882
I always read bank/electronic media guidelines for cybersecurity issues. [CS3]	4.699	-2.387	8.274	0.652
Cybersecurity Trust (AVE = 0.586, CR= 0.808): I feel more comfortable with mobile banking services. [CT1]	4.625	-2.23	6.402	0.761
I trust mobile banking services. [CT2]	4.726	-2.706	9.185	0.851
I trust Indonesian banks. [CT3]	4.807	-3.166	10.988	0.676
Entertainment (AVE = 0.827, CR = 0.905): I really enjoy the "Don't Know? Give No" advertisement. [ENT1]	4.525	-2.138	5.292	0.904
I feel very interested when I see the "Don't Know? Give No" advertisement. [ENT2]	4.359	-1.699	3.377	0.915
Transaction Risk Perception (AVE = 0.552, CR = 0.787): I feel insecure when using direct branch banking transactions, due to legal and orderly situations. [PR1]	2.726	0.179	-1.317	0.752
I am worried about giving my credit card number or logging into the bank's website. [PR2]	2.722	0.223	-1.289	0.692
When I send data to the bank's website, I am worried that the data will be stolen and altered by unauthorized third parties like hackers. [PR3]	2.595	0.295	-1.200	0.782
Social Influence (AVE = 0.706, CR = 0.827): Using social media platforms supports my need for social interaction and helps me feel more involved in my friends' group. [SI1]	4.591	-2.732	8.185	0.855
I use social media platforms to access challenging content and educational sources that challenge my thinking and problem-solving skills. [SI2]	4.784	-1.676	1.607	0.825
User Satisfaction (AVE = 0.669, CR= 0.798): I feel I have done the right thing by deciding to use e-banking services. [US1]	2.278	0.655	-0.649	0.693
My experience using my e-bank is very satisfying. [US2]	4.764	-2.241	5.366	0.925

1 = Mean; 2 = Skewness; 3 = Kurtosis; 4 = Outer Loading

Table 4. Discriminant validity Fornell-Larcker criterion

	1	2	3	4	5	6	7	8	9
1	0.811								
2	-0.084	0.772							
3	-0.239	0.492	0.766						
4	-0.024	0.460	0.354	0.724					
5	-0.101	0.415	0.561	0.402	0.776				
6	-0.017	0.743	0.432	0.414	0.410	0.909			
7	-0.023	0.244	0.273	0.247	0.394	0.213	0.840		
8	0.515	-0.140	-0.214	-0.015	-0.088	-0.087	-0.008	0.743	
9	-0.195	0.509	0.634	0.409	0.526	0.433	0.302	-0.143	0.818

1 = Commitment; 2 = Content quality; 3 = Customer trust; 4 = Cyber-attack awareness; 5 = Cyber security measure; 6 = Entertainment; 7 = Social influence; 8 = Transaction risk perception; 9 = User satisfaction

Table 5. Hypothesis test results

Hypotheses	β	Stdev	T Statistics	P Values	f^2
H_1: Content Quality → User Satisfaction	0.390	0.100	3.810	0.000	0.092
H_2: Social Influence → User Satisfaction	0.184	0.065	2.854	0.002	0.046
H_3: Entertainment → User Satisfaction	0.112	0.102	1.078	0.140	0.008
H_4: User Satisfaction → Cyberattack Awareness	0.418	0.061	6.726	0.000	0.201
H_5: Transaction Risk Perception → Customer Trust	-0.177	0.047	3.584	0.000	0.045
H_6: Cyberattack Awareness → Customer Trust	0.160	0.059	2.690	0.004	0.033
H_7: Cybersecurity Measures → Customer Trust	0.490	0.076	6.386	0.000	0.303
H_8: Customer Trust → Commitment	-0.251	0.056	4.304	0.000	0.061

Table 6. PLS predict

Indicator	1	2	3	4
[CO1]	0.022	-1.416	1.331	-2.747
[CO2]	0.030	-1.420	1.390	-2.810
[CO3]	0.033	-1.360	1.279	-2.639
[CO4]	0.031	-1.252	1.206	-2.457
1: Q^2predict; 2: PLS-SEM_RMSE; 3: LM_RMSE; 4: ΔPLS-SEM-LM_RMSE				

The final procedure of assessing the structural model included the evaluation of its predictive capability using PLS Predict [68]. Table 6 shows the PLS predict results. Our research applied a 10-fold cross-validation method with ten repeats as experimental design. To demonstrate prediction skills, the RMSE value of the PLS-SEM model must be lower than that of the linear regression model (LM). If all Δ PLS-SEM-LM_RMSE values are negative, the model has a significant level of predictive capacity. If most Δ PLS-SEM-LM_RMSE values are negative, the model is considered to have a modest level of predictive capacity. If few or none of the Δ PLS-SEM-LM_RMSE values are negative, the model has low predictive capability. In this case, all Δ PLS-SEM-LM_RMSE values are negative, indicating that the PLS-SEM model's RMSE values are consistently higher than those of the linear regression model for all commitment indicators (CO1 - CO4). This finding demonstrates that the model has excellent predictive capability. Specifically, the negative Δ PLS-SEM-LM_RMSE values suggest that the PLS-SEM model predicts the commitment variables better than the linear regression model.

Hypotheses Discussions

First, the result shows that content quality (H_1 accepted) and social influence (H_2 accepted) positively affect user satisfaction. This finding is consistent with the previous research [32-38]. This shows that the quality of content to educate bank customers to avoid online fraud increases the satisfaction of the responses involved in this study. Content "don't know? Kasih No!" provides useful education so that bank customers are always careful before downloading files from suspicious or unofficial sources so that bank customers can maintain personal security. When associated with respondent profiles, respondents with younger age groups and higher education tend to appreciate the quality of relevant and comprehensive content so that it can increase user satisfaction. However, married respondents and older age groups prioritize content that is relevant to family life and informative. Therefore, the researcher concluded that the higher the quality of educational content, the higher the user satisfaction.

Meanwhile, from the perspective of social influence, bank customers will be interested in interacting after watching educational advertisements because of their innovative, simple, planned and unique content packaging strategies. After customers give likes and comments on the educational content, customers who are satisfied with the educational content will share the post with their relatives. Customers can discuss preventing online crime by commenting on the educational ad post. When associated with respondent profiles, younger and unmarried age groups tend to be influenced by recommendations from friends, family or online reviews that reinforce the relationship with user satisfaction. In addition, respondents with lower education are also more susceptible to the influence of recommendations from friends, family, or online reviews, thereby increasing user satisfaction. Therefore, the researcher concluded that the higher the social influence, the higher the user satisfaction.

However, the relationship between entertainment and user satisfaction is not significant (H_3 rejected). This finding argues the previous research findings [39-42]. Based on the contradictory findings in the study, the researcher suspects that the main purpose of the content is to educate customers on how to prevent online crime through data theft and the spread of viruses through apps from suspicious sources. In addition, the main character of this educational content is a legendary comedian who reminds that Dono and Kasino are close friends so that if someone claims to be a close friend of Indro and sends a virus in the form of an invitation via WhatsApp, Indro will not be fooled. In the end, if the title of this educational content is pronounced, it will remind the audience of the late Dono and Kasino. Finally, the older age group, married, or highly educated groups of respondents focus more on informative or educational content so the relationship between entertainment and user satisfaction may be weaker.

The relationship between user satisfaction and cyber-attack awareness is significant and positive (H_4 accepted). This finding supports the previous research findings [42, 79, 80]. The researchers concluded that customer satisfaction after watching educational content about online crime prevention by stealing identity through text messages or advertisements from suspicious sources can increase cyber-attack awareness. Educational content presented in a clear, informative, relevant, and innovative manner can help customers understand the threat of cyberattacks and the steps they can take to protect themselves. When considering younger age groups and higher education, users tend to be more aware of cybersecurity if they are satisfied with educational videos related to cyber attacks. In addition, married respondents are aware of cyber potential if they are satisfied with educational videos to prevent cyber attacks.

There are positive relationships of cyber security measures (H_7 accepted) and cyber-attack awareness (H_6 accepted) on customer trust. These findings are consistent with previous research findings [8, 35, 44, 51, 54, 55]. The researchers concluded that customers who understood the risks of cyberattacks and realized that their banks had strict security measures in place, felt more secure and trusted in the protection of their personal data and financial transactions. When associated with demographic profiles in measuring the cyber security measures, respondents in older and married age groups tend to be more concerned about cybersecurity, thus strengthening the relationship between security awareness and customer trust. However, respondents who have higher education are more aware of security risks and are more critical in protecting data. Finally, the researchers also evaluate the insight of demographic profiles when measuring the cyber attack awareness. The findings show that younger and more educated respondents tend to be more aware of the risk of cyber attacks, thus strengthening cyber security awareness and customer trust. However, married respondents are more worried about protecting family data so that they can strengthen the relationship [81]. Therefore, the importance of awareness of cyber-attacks and cyber security measures can increase the trust of bank customers in Indonesia [56].

Our research finding shows that perceived risk of transaction negatively affects customer trust (H_5 accepted). These findings are consistent with previous research findings [8, 14, 50, 51]. The researchers conclude that the bank customers feel high potential risks related to data security and banking transactions, customer trust in banks tends to

decrease. This risk perception can be obtained by customers through media reports on data leaks, the experiences of other customers affected by online crimes, and the low transparency of the bank in the event of a cyberattack. Based on the demographic profile, older and married respondents tend to be more worried about transaction risk. Meanwhile, respondents with higher education can understand and consider risk factors in transactions. Therefore, bank management needs to proactively manage and reduce risk perceptions by providing transparent and educational information on the security measures that have been implemented.

Our findings shows that customer trust negatively affect commitment (H_8 accepted). This finding argues the previous research findings [10, 57, 58, 62, 82, 83]. Researchers suspect that customer commitment to banks remains high even though bank customer trust has declined after cyberattacks. Moreover, older and married respondents value commitments built on trust. However, respondents who have higher education will demand a stronger commitment from those they trust. This is due to the bank's ability to respond to attacks quickly, transparently, and effectively so that it can prevent customers from losing trust in the bank. When bank management is proactive in communicating with their customers through various communication channels to explain the steps taken to mitigate attacks and improve security, customers will feel valued and prioritized.

This research is also implemented with the IPMA method to enhance the understanding of PLS-SEM results and facilitates the identification of crucial areas for improvement. Using the IPMA approach improves comprehension of PLS-SEM results and makes it easier to identify critical areas for development [69]. Figure 2 presents the Importance performance map analysis results. Prior research had stated that the IPMA offers valuable insight in assisting company in identifying various attributes that are crucial for improvement [84]. In the IPMA results, customer trust and cybersecurity measures are in quadrant of low priority, depicting a positive impact but impractical. Meanwhile, content quality and entertainment are in quadrant of keeping up the good work, means both indicators are already good and should be maintained. The cyber-attack awareness, social influence, transaction risk perception, and user satisfaction are in quadrant of concentrate here, depicting areas for improvement. Finally, the researchers perform important performance map analysis for strengthening the PLS SEM results and facilitate the important factors for improvement [69]. Figure 2 shows the IPMA of security behaviour intention. The researchers classify security awareness, self-efficacy, perceived vulnerability, and threat awareness in quadrant II (concentrate here). Moreover, the perceived severity falls in quadrant IV (possible overkill) and response efficacy falls in quadrant III (low priority).

Finally, the management required to prepare and implement detection and curration approach when the prevention failed to protech the organization from hacker attack. Management need to invest for security tools analyst such as data and system backup, incident response, threat detection, and perform risk analysis periodically.

Based on the IPMA result, the researchers proposed several suggestions to the management. Regarding the cyber-attack awareness strategic initiative and its satisfaction, the researchers suggested that the top management should focus on developing relevant and easy to understand education content based on real case study of cyber security threat in banking context. The education content consists of real case examples, risk management and mitigation plan, practical tips that developed using various media formats such as short videos, articles, infographics, webinars, and podcast.

Next, the cyber-security team needs to partner with cyber-security experts or independent organizations to get the latest developments regarding cyber threats and how to deal with them. Based on their insight, the top management should implement cutting edge security technology for reducing the transaction risk. Those security technologies need to be communicated to their bank customers to reduce the cyber-attack risk and protect the financial transaction. Using digital marketing technology and personalized marketing campaigns, the bank management will be able to design personalized educational marketing campaigns to its customer for the risk of cyber-attack.

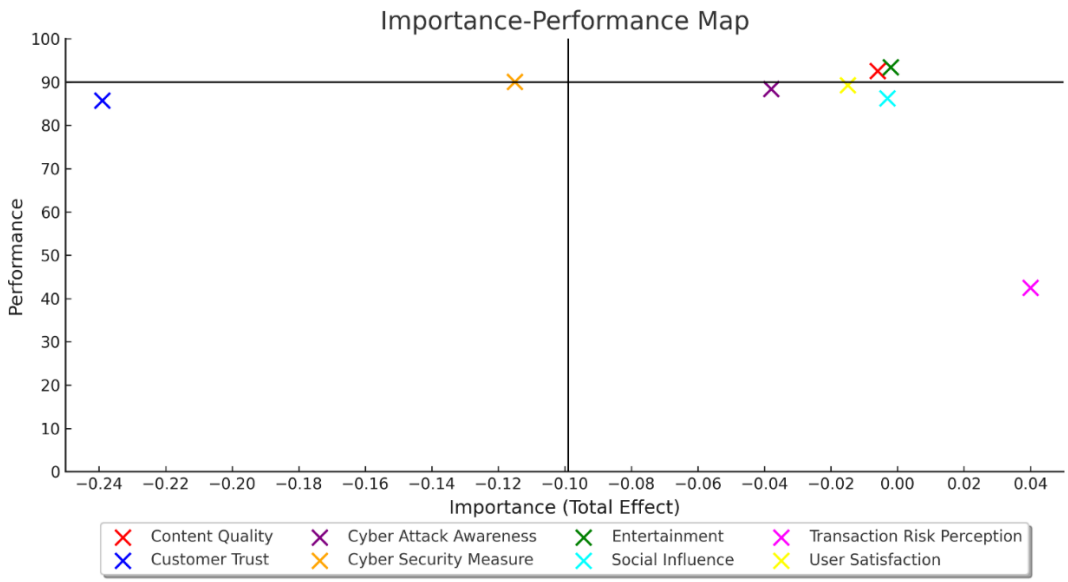

Figure 2. Importance performance map analysis results

Next, the cyber security strategic initiative implementation will enhance the detection and curation capabilities for overcoming the cyber-attack risk. The cyber-attack threat detection strategies are the implementation of monitoring system to detect and analyze real-time financial transaction for suspicious transaction patterns, the implementation of big data analytic technology for classifying anomalies in customer transactions, the implementation of intrusion detection system will help cyber-security to monitor network traffic and detect any potential threat, and conducting periodic system and network activity logs assessment for identifying new potential threat.

Based on the cyber security detection outcome, the top management will be able to develop effective responds for threat source isolation and system recovery after cyber-attack happened. The cyber-security team must regularly execute the data recovery procedure to recover the system after cyber-attack happened. Moreover, the cyber security team need to ensure the security systems updated to prevent any security gaps and develop mitigation plan. Finally, the top management need to allocate training budget for updating the employee knowledge related to cyber-security threats and how to mitigate the cyber-attack risks.

Lastly, the top management should evaluate the cyber-security initiative and its education campaign using digital marketing periodically. In certain cases, the cyber security team might enforce the security implementation for ensuring the safety of customers' financial transactions. Moreover, evaluating and reformulating the educational campaign to ensure the effectiveness of an educational marketing campaign is important.

5. CONCLUSION

This study was conducted to examine the influence of perceived content quality, perceived social influence, and perceived entertainment on user satisfaction with the cybersecurity campaign "Don't Know? Kasih No!" and its impact on customer commitment. Our research explored the combination of the Uses-Gratification Theory (UGT) and the Trust Commitment theory to analyze the effect of the "Don't Know? Kasih No!" campaign on cybersecurity awareness and its role in fostering customer commitment. The results of this study demonstrate that cybersecurity campaigns are crucial for improving cybersecurity awareness and can generate customer trust, leading to commitment. However, the entertainment factor in cybersecurity campaigns was found to be insignificant. Interestingly, the fear of cybercrime and real evidence of cyberattacks led to a decrease in customer confidence in using digital banking services.

Theoretical contribution

Our study contributes to the advancement of relational marketing from cyber-attack threat perspective. By integrating Uses-Gratification Theory with Trust-Commitment Theory, the researchers proven the relationship between those theory for explaining the effect of educational content related to cyber-security in Indonesia. Next, the researchers employ cutting-edge data analysis procedurjsse for investigating the phenomenon ruinously. Lastly, there are limited research exploring the "Don't Know? Kasih No!" campaign, cyber-security awareness, cyber security implementation, and transaction risk on customer trust and commitment.

Managerial implication

Our study has several managerial implications. By providing continuous cybersecurity education with good quality education and interesting content to increase customer satisfaction, increase security against cyber-attacks, provide the perception that the risk of digital transactions can be mitigated, but if a cyber-attack occurs, it will reduce customer trust and result in reducing customer commitment to using digital transactions at the bank. Therefore, the bank management must be continuous and consistent to educate their customer about cybersecurity for maintaining customer trust and customer commitment to conduct digital transactions at the bank.

Research limitation and future research

The researchers identify several limitations and offer the future research direction. First, the researchers detect a potential selection bias when choosing convenience sampling. However, the researchers employ a screening question for reducing the respondent bias. Therefore, the researchers suggest using purposive sampling with attention trap question for the future research. Moreover, the researchers suggest employing experimental design for ensuring the contextual framing. Second, the researchers only use age group, marital status, and education for respondent demographic profiling. Therefore, the researchers suggest adopting relevant demographic, geographic, and psychographic question for understanding the cyber-attack awareness and its impact on customer trust and commitment. Second, the research does not focus on specific cyber-security of electronic channel technology such as ATM, mobile banking, e-banking, or other types of digital transactions. Since the cyber security threat on specific electronic channel might differ in nature, this might affect the findings. Therefore, the researchers suggest replicating the study on specific electronic channel in banking for generalizing the findings. Lastly, our study integrates Uses-Gratification Theory and Trust-Commitment Theory for understanding the phenomenon from relational marketing perspective. The researchers suggest to employ theories related to security technology adoption or mental health for advancing the cyber-security behaviour research.

REFERENCES

[1] Malik, M.S., Islam, U. (2019). Cybercrime: An emerging threat to the banking sector of Pakistan. Journal Finance Crime, 26(1): 50-60. https://doi.org/10.1108/JFC-11-2017-0118

[2] Mostafa, R.B. (2020). Mobile banking service quality: A new avenue for customer value co-creation. International Journal of Bank Marketing, 38(5): 1107-1132. https://doi.org/10.1108/IJBM-11-2019-0421

[3] Naveed, R.T., Irfan, M., Aslam, H.D., Anwar, B., Ayub, A. (2019). The effect of general banking information technology system on customers' satisfaction with the moderating effect of customer trust: An empirical study from Pakistani commercial (Islamic) banks. Al-Qalam, 24(1): 387-401.

[4] Ying, C.X., Kasmin, I.F., Amin, S., Zainal, N.K. (2022). Cybersecurity education through mobile application to prevent cyber attacks during COVID-19. International Journal of Data Science and Advanced Analytics, 4: 27-33. https://doi.org/10.69511/ijdsaa.v4i0.139

[5] Morgan, R.M., Hunt, S.D. (1994). The commitment-trust theory of relationship marketing. Journal Marketing, 58(3): 20-38. https://doi.org/10.1177/002224299405800302
[6] Gundlach, G.T., Achrol, R.S., Mentzer, J.T. (1995). The structure of commitment in exchange. Journal of Marketing, 59(1): 78-92. https://doi.org/10.1177/002224299505900107
[7] Mochammad, A., Siti, A.E., Nayati, U.H. (2020). Islamic compliance and quality of e-banking services build trust and customer commitment using e-banking islamic bank. Eurasia: Economics e Business, 34(4): 2020-2024. https://doi.org/10.18551/econeurasia.2020-04
[8] Hanif, Y., Lallie, H.S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust. Technology in Society, 67: 101693. https://doi.org/10.1016/j.techsoc.2021.101693
[9] Roberts-Lombard, M. (2020). Antecedents and outcome of commitment in Islamic banking relationships–An emerging African market perspective. Journal of Islamic Marketing, 11(6): 1851-1871. https://doi.org/10.1108/JIMA-09-2018-0164
[10] Bajwa, I.A., Ahmad, S., Mahmud, M., Bajwa, F.A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: An empirical evidence from the Pakistani banking sector. Information & Computer Security, 31(5): 635-654. https://doi.org/10.1108/ICS-11-2022-0179
[11] Rajaobelina, L., Prom Tep, S., Arcand, M., Ricard, L. (2021). The relationship of brand attachment and mobile banking service quality with positive word-of-mouth. Journal of Product and Brand Management, 30(8): 1162-1175. https://doi.org/10.1108/JPBM-02-2020-2747
[12] Shankar, A., Jebarajakirthy, C., Ashaduzzaman, M. (2020). How do electronic word of mouth practices contribute to mobile banking adoption? Journal of Retailing and Consumer Services, 52: 101920. https://doi.org/10.1016/J.JRETCONSER.2019.101920
[13] Boateng, S.L. (2021). Enhancing calculative commitment and customer loyalty through online relationship marketing: The mediating role of online trust. Research Anthology on E-Commerce Adoption, Models, and Applications for Modern Business, 1221-1241. https://doi.org/10.4018/978-1-7998-8957-1.ch063
[14] Kaur, S., Arora, S. (2020). Role of perceived risk in online banking and its impact on behavioral intention: Trust as a moderator. Journal of Asia Business Studies, 15(1): 1-30. https://doi.org/10.1108/JABS-08-2019-0252
[15] Banerjee, S., Sreejesh, S. (2022). Examining the role of customers' intrinsic motivation on continued usage of mobile banking: A relational approach. International Journal of Bank Marketing, 40(1): 87-109. https://doi.org/10.1108/IJBM-06-2021-0216
[16] Chesebro, J.W., Bertelsen, D.A. (1998). Analyzing Media: Communication Technologies as Symbolic and Cognitive Systems. Guilford Press, London.
[17] Scheufele, D.A. (1999). Framing as a theory of media effects. Journal of Communication, 49(1): 103-122. https://doi.org/10.1111/J.1460-2466.1999.TB02784.X
[18] Katz, E., Blumler, J.G., Gurevitch, M. (1973). Uses and gratifications research. The Public Opinion Quarterly, 37(4): 509-523. http://www.jstor.org/stable/2747854.
[19] Masrom, M.B., Busalim, A.H., Abuhassna, H., Mahmood, N.H.N. (2021). Understanding students' behavior in online social networks: A systematic literature review. International Journal of Educational Technology in Higher Education, 18: 1-27. https://doi.org/10.1186/S41239-021-00240-7
[20] Larimo, F., Li, J., Leonidou, L.C. (2023). Social media in marketing research: Theoretical bases, methodological aspects, and thematic focus. Psychology & Marketing, 40(1): 124-145. https://doi.org/10.1002/MAR.21746
[21] Camilleri, M.A., Falzon, L. (2021). Understanding motivations to use online streaming services: Integrating the technology acceptance model (TAM) and the uses and gratifications theory (UGT). Spanish Journal of Marketing-ESIC, 25(2): 217-238. https://doi.org/10.1108/SJME-04-2020-0074
[22] Kaur, P., Dhir, A., Chen, S., Malibari, A., Almotairi, M. (2020). Why do people purchase virtual goods? A uses and gratification (U&G) theory perspective. Telematics and Informatics, 53: 101376. https://doi.org/10.1016/J.TELE.2020.101376
[23] Nawaz, S. (2024). Distinguishing between effectual, ineffectual, and problematic smartphone use: A comprehensive review and conceptual pathways model for future research. Computers in Human Behavior Reports, 14: 100424. https://doi.org/10.1016/J.CHBR.2024.100424
[24] Ma, S., Zhang, S., Li, G., Wu, Y. (2019). Exploring information security education on social media use: Perspective of uses and gratifications theory. Aslib Journal of Information Management, 71(5): 618-636. https://doi.org/10.1108/AJIM-09-2018-0213
[25] Kim, S.E., Kim, H.L., Lee, S. (2021). How event information is trusted and shared on social media: A uses and gratification perspective. Journal of Travel & Tourism Marketing. 38(5): 444-460. https://doi.org/10.1080/10548408.2021.1943600
[26] Wei, D., Chan, L.S., Du, N., Hu, X., Te Huang, Y. (2024). Gratification and its associations with problematic internet use: A systematic review and meta-analysis using use and gratification theory. Addictive Behaviors, 155: 108044. https://doi.org/10.1016/J.ADDBEH.2024.108044
[27] Shirsat, A.A.R., González, A.F., May, J.J. (2022). Proposing a model of social media user interaction with fake news. Journal of Information, Communication and Ethics in Society, 20(1): 134-149. https://doi.org/10.1108/JICES-10-2020-0104
[28] Sampat, B., Raj, S. (2022). Fake or real news? Understanding the gratifications and personality traits of individuals sharing fake news on social media platforms. Aslib Journal of Information Management, 74(5): 840-876. https://doi.org/10.1108/AJIM-08-2021-0232
[29] Tanrikulu, I., Erdur-Baker, Ö. (2019). Motives behind cyberbullying perpetration: A test of uses and gratifications theory. Journal of Interpersonal Violence, 36(13-14): NP6699-NP6724. https://doi.org/10.1177/0886260518819882
[30] Paat, Y.F., Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. Social Work in Mental Health, 19(1): 18-40. https://doi.org/10.1080/15332985.2020.1845281

[31] Taha, N., Dahabiyeh, L. (2021). College students information security awareness: A comparison between smartphones and computers. Education and Information Technology, 26(2): 1721-1736. https://doi.org/10.1007/s10639-020-10330-0
[32] Daengsi, T., Pornpongtechavanich, P., Wuttidittachotti, P. (2022). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. Education and Information Technologies, 27(4): 4729-4752. https://doi.org/10.1007/s10639-021-10806-7
[33] Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Applied Sciences, 10(16): 5702. https://doi.org/10.3390/APP10165702
[34] McIlwraith, A. (2021). Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness. Routledge, London. https://doi.org/10.4324/9780429281785
[35] Quader, F., Janeja, V.P. (2021). Insights into organizational security readiness: Lessons learned from cyber-attack case studies. Journal of Cybersecurity and Privacy, 1(4): 638-659. https://doi.org/10.3390/JCP1040032
[36] Tang, Z., Miller, A.S., Zhou, Z., Warkentin, M. (2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. Goverment Information Quartely, 38(2): 101572. https://doi.org/10.1016/J.GIQ.2021.101572
[37] Krishna, B., Krishnan, S., Sebastian, M.P. (2022). Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: An institutional trust theory perspective. Information Systems Frontiers, 25(5): 1713-1741. https://doi.org/10.1007/S10796-022-10280-7
[38] Afzal, M., Ansari, M. S., Ahmad, N., Shahid, M., Shoeb, M. (2024). Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: An integrated model approach. Journal of Financial Services Marketing, pp. 1-21. https://doi.org/10.1057/S41264-024-00279-3
[39] Kar, A.K. (2021). What affects usage satisfaction in mobile payments? Modelling user generated content to develop the 'Digital Service Usage Satisfaction Model'. Information Systems Frontiers, 23(5): 1341-1361. https://doi.org/10.1007/S10796-020-10045-0
[40] Chen, H., Zhang, Y., Zhang, S., Lyu, T. (2023). Exploring the role of gamified information security education systems on information security awareness and protection behavioral intention. Education and Information Technologies, 28(12): 15915-15948. https://doi.org/10.1007/S10639-023-11771-Z
[41] Kasilingam, D., Ajitha, S. (2022). Storytelling in advertisements: Understanding the effect of humor and drama on the attitude toward brands. Journal of Brand Management, 29(4): 341-362. https://doi.org/10.1057/S41262-021-00253-7
[42] Hwang, M.I., Helser, S. (2022). Cybersecurity educational games: A theoretical framework. Information and Computer Security, 30(2): 225-242. https://doi.org/10.1108/ICS-10-2020-0173
[43] Hwang, M.I. (2024). Teaching information systems. Edward Elgar. Northampton, pp. 1-310. https://doi.org/10.4337/9781802205794
[44] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H.N. (2022). Cybersecurity awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1): 82-97. https://doi.org/10.1080/08874417.2020.1712269
[45] Khan, N.F., Ikram, N., Murtaza, H., Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. Computer and Security, 125: 103049. https://doi.org/10.1016/J.COSE.2022.103049
[46] Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. South African Journal of Business Management, 51(1). https://doi.org/10.4102/SAJBM.V51I1.1941
[47] Li, F., Lu, H., Hou, M., Cui, K., Darbandi, M. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. Technology in Society, 64: 101487. https://doi.org/10.1016/J.TECHSOC.2020.101487
[48] Al-Qahtani, E., Sahoo, L., Javed, Y., Shehab, M. (2022). 'Why would someone hack me out of thousands of students': Video presenter's impact on motivating users to adopt 2FA. In 2022 Proceedings of ACM Symposium on Access Control Models and Technologies (SACMAT), pp. 139-150. https://doi.org/10.1145/3532105.3535013
[49] Lestari, S., Adawiyah, W.R., Alhamidi, A.L., Prayogi, J., Haryanto, R. (2024). Navigating perilous seas: Unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. Safer Communities, 23(4): 444-464. https://doi.org/10.1108/SC-04-2024-0018
[50] Zhao, C., Noman, A.H.M., Asiaei, K. (2022). Exploring the reasons for bank-switching behavior in retail banking. International Journal of Bank Marketing, 40(2): 242-262. https://doi.org/10.1108/IJBM-01-2021-0042
[51] Johri, A., Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. Human Behavior and Emerging Technolgy, 2023(1): 2103442. https://doi.org/10.1155/2023/2103442
[52] Abed, M.S., Al-Doori, Q.F., Abdullah, A.T., Abdallah, A.A. (2023). Security vulnerabilities and threats in robotic systems: A comprehensive review. International Journal of Safety and Security Engineering, 13(3): 555-563. https://doi.org/10.18280/ijsse.130318
[53] Perera, S., Jin, X., Maurushat, A., Opoku, D.G.J. (2022). Factors affecting reputational damage to organisations due to cyberattacks. Informatics, 9(1): 28. https://doi.org/10.3390/informatics9010028
[54] Mayer, P., Zou, Y., Lowens, B.M., Dyer, H.A., Le, K., Schaub, F., Aviv, A.J. (2023). Awareness, intention, (in)action: Individuals' reactions to data breaches. ACM Transactions on Computer-Human Interaction, 30(5): 1-53. https://doi.org/10.1145/3589958
[55] Asif, M., Wang, S., Shahzad, M.F., Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital

transformation of the banking sector. Computer & Security, 147: 104051. https://doi.org/10.1016/J.COSE.2024.104051
[56] Mutleg, M.L., Mahmood, A.M., Al-Nayar, M.M.J. (2024). A comprehensive review of cyber-attacks targeting IoT systems and their security measures. International Journal of Safety and Security Engineering, 14(4): 1073-1086. https://doi.org/10.18280/ijsse.140406
[57] Eriksson, K., Hermansson, C., Jonsson, S. (2020). The performance generating limitations of the relationship-banking model in the digital era - effects of customers' trust, satisfaction, and loyalty on client-level performance. International Journal of Bank Marketing, 38(4): 889-916. https://doi.org/10.1108/IJBM-08-2019-0282
[58] Aslam, M., Khan Abbasi, M.A., Khalid, T., Shan, R.U., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D.A., Ahmad, R. (2022). Getting smarter about smart cities: Improving data security and privacy through compliance. Sensors, 22(23): 9338. https://doi.org/10.3390/S22239338
[59] Mehrad, J., Tajer, P. (2016). Uses and gratification theory in connection with knowledge and information science: A proposed conceptual model. International Journal of Information Science and Management (IJISM), 14(2): 1-14.
[60] Sanchez-Franco, M.J. (2009). The moderating effects of involvement on the relationships between satisfaction, trust and commitment in e-banking. Journal of Interactive Marketing, 23(3): 247-258. http://doi.org/10.1016%2Fj.intmar.2009.04.007
[61] Kassim, N. Asiah Abdullah, N. (2010). The effect of perceived service quality dimensions on customer satisfaction, trust, and loyalty in e-commerce settings: A cross-cultural analysis. Asia Pacific Journal of Marketing and Logistics, 22(3): 351-371. https://doi.org/10.1108/13555851011062269
[62] Yuan, Y., Feng, B., Lai, F., Collins, B.J. (2018). The role of trust, commitment, and learning orientation on logistic service effectiveness. Journal of Business Research, 93: 37-50. https://doi.org/10.1016/j.jbusres.2018.08.020
[63] Hsu, C.L., Lin, J. C.C. (2023). The effects of gratifications, flow and satisfaction on the usage of livestreaming services. Library Hi Tech, 41(3): 729-748. https://doi.org/10.1108/LHT-02-2021-0069
[64] Sung, Y., Kim, Y., Kwon, O., Moon, J. (2010). An explorative study of Korean consumer participation in virtual brand communities in social network sites. Journal of Global Marketing, 23(5): 430-445. https://doi.org/10.1080/08911762.2010.521115
[65] Ho, V.T., Garg, S., Rogelberg, S.G. (2021). Passion contagion at work: Investigating formal and informal social influences on work passion. Journal of Vocational Behavior, 131: 103642. https://doi.org/10.1016/j.jvb.2021.103642
[66] Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M. (2021). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). SAGE Publication, Thousand Oaks. https://lccn.loc.gov/2016005380.
[67] Sarstedt, M., Hair, J.F., Ringle C.M. (2022). 'PLS-SEM: Indeed a silver bullet'–Retrospective observations and recent advances. Journal of Marketing Theory and Practice, 31(3): 261-275. https://doi.org/10.1080/10696679.2022.2056488
[68] Shmueli, G., Sarstedt, M., Hair, J.F., Cheah, J.H., Ting, H., Vaithilingam, S., Ringle, C.M. (2019). Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. European Journal of Marketing, 53(11): 2322-2347. https://doi.org/10.1108/EJM-02-2019-0189
[69] Ringle, C.M., Sarstedt, M. (2016). Gain more insight from your PLS-SEM results: The importance-performance map analysis. Industrial Management & Data Systems, 116(9): 1865-1886. https://doi.org/10.1108/IMDS-10-2015-0449
[70] Gaskin, J. (2012). Data screening. https://youtube.com/watch?v=eiIJNToqGa0&si=EnSIkaIECMiOmarE.
[71] Podsakoff, P.M. Organ, D.W. (1986). Self-reports in organizational research: Problems and prospects. Journal of Management, 12(4): 531-544. https://doi.org/10.1177/014920638601200408
[72] Kock, N., Lynn, G.S. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. Journal of the Association for Information Systems, 13(7): 546-580. https://doi.org/10.17705/1jais.00302
[73] Mishra, P., Pandey, C.M., Singh, U., Gupta, A., Sahu, C., Keshri, A. (2019). Descriptive statistics and normality tests for statistical data. Annals of Cardiac Anaesthesia, 22(1): 67. https://doi.org/10.4103/ACA.ACA_157_18
[74] Sarstedt, M., Hair, J.F., Ringle, C.M., Thiele, K.O., Gudergan, S.P. (2016). Estimation issues with PLS and CBSEM: Where the bias lies! Journal of Business Research, 69(10): 3998-4010. https://doi.org/10.1016/J.JBUSRES.2016.06.007
[75] Guenther, P., Guenther, M., Ringle, C.M., Zaefarian, G., Cartwright, S. (2023). Improving PLS-SEM use for business marketing research. Industrial Marketing Management, 111: 127-142. https://doi.org/10.1016/J.INDMARMAN.2023.03.010
[76] Sarstedt, M., Hair, J.F., Pick, M., Liengaard, B.D., Radomir, L., Ringle, C.M. (2022). Progress in partial least squares structural equation modeling use in marketing research in the last decade. Psychology & Marketing, 39(5): 1035-1064. https://doi.org/10.1002/mar.21640
[77] Tolah, A., Furnell, S.M., Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. Computer & Security, 108: 102354. https://doi.org/10.1016/J.COSE.2021.102354
[78] Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences. Routledge, London.
[79] Bae, M. (2018). Understanding the effect of the discrepancy between sought and obtained gratification on social networking site users' satisfaction and continuance intention. Computers in Human Behavior, 79: 137-153. https://doi.org/10.1016/j.chb.2017.10.026
[80] Kävrestad, J., Fallatah, W., Furnell, S. (2023). Cybersecurity training acceptance: A literature review. In International Symposium on Human Aspects of Information Security and Assurance, pp. 53-63. https://doi.org/10.1007/978-3-031-38530-8_5
[81] Amine, A.A.M., Chakir, E.M., Issam, T., Khamlichi, Y.I. (2023). A review of cybersecurity management standards applied in higher education institutions. International Journal of Safety and Security Engineering, 13(6): 1109-1116. https://doi.org/10.18280/ijsse.130614
[82] Mohd Kassim, N., Kader Mohammed Ahmed Abdulla, A. (2006). The influence of attraction on internet

banking: An extension to the trust-relationship commitment model. International Journal of Bank Marketing, 24(6): 424-442. https://doi.org/10.1108/02652320610701744

[83] Lestari, A.D., Asyik, N.F. (2015). Pengaruh kualitas sistem informasi dan pengetahuan akuntansi terhadap kualitas informasi akuntansi. Jurnal Ilmu & Riset Akuntansi, 4(9): 20. http://eprints.umg.ac.id/id/eprint/694.

[84] Fakfare, P. (2021). Influence of service attributes of food delivery application on customers' satisfaction and their behavioural responses: The IPMA approach. International Journal of Gastronomy and Food Science, 25: 100392. https://doi.org/10.1016/j.ijgfs.2021.100392