The Impact of Online Campaign and Cybersecurity Knowledge on Protective Behaviour of Generation Z Customers of Bank BCA

Abstract. The purpose of this study was to determine whether the online campaign program “Don’t Know? Kasih No!” and cybersecurity knowledge affect the self-protection behavior of Generation Z Bank BCA customers against the rise of online fraud cases, through quantitative methods with data collected from 100 active BCA Bank Generation Z customers who have watched the online campaign. The results showed that online campaigns and cybersecurity knowledge have a positive and significant influence, both partially and simultaneously, on the self-protection behavior of Generation Z Bank BCA customers. These two variables together can explain 40.5% of the self-protection behavior of Generation Z Bank BCA customers. Overall, these findings suggest that online campaigns and cybersecurity knowledge programs are influential in shaping customers' self-protective behavior to deal with the risk of online fraud in the banking sector.

Keywords: Online Campaign, Cybersecurity Knowledge, Protective Behaviour, Online Fraud.

1 Introduction

The advancement of the digital world does not always have a positive impact; on the contrary, it also poses various threats, one of which is online fraud. Currently, personal data is being targeted by irresponsible parties for personal gain. Based on the Third Quarter Report of the Financial Services Authority (OJK) in 2024, Otoritas Jasa Keuangan (2024) Banking fraud, such as account breach, skimming, phishing, and social engineering, ranked second with 4,991 cases reported. This is supported by APJII survey data in the 2024 Survey & Respondent (2024), which recorded an increase in online fraud cases from 10.30% in 2023 to 32.50% in 2024. On the other hand, based on the results of the 2024 survey, the Indonesian Internet Service Providers Association (APJII) Survei & Responden (2024) noted that 22.78% of internet users in Indonesia have not made any efforts to keep their data safe, such as installing antivirus, using verified applications, being aware of applications that request data access, and changing passwords regularly. If the public has a good knowledge of cybersecurity, it will have an impact on increasing awareness of cybersecurity and personal data protection (Limna et al., 2023).

Seeing the increasing cases of online fraud and the lack of public action in maintaining data security, financial institutions such as banks began to initiate online campaigns. One of them is done by Bank BCA through the online campaign “Don’t Know? Kasih No!”. This online campaign can be accessed through social media such as YouTube, Twitter, and Instagram, or through the following link: https://youtu.be/KstzfWBUcf8?si=wGwfP6UOzvzrTQy6, as well as displayed in the form of posters in all BCA branch offices. Highlights of the online campaign include the presence of legendary comedian Indro as the main star and the use of the analogy of a fish being hooked as an illustration of customers being targeted by online fraud. The bait used by the perpetrators is delivered through fake messages on behalf of BCA Bank, such as PDF files containing invitations or links to attractive promos and discounts. This campaign invites the public to reject and be aware of all forms of information whose sources are unclear through the “Don’t Know? Kasih No!”. This online campaign is also in line with APJII data in 2024, which notes that Generation Z (aged 13-27 years) has the highest internet penetration rate of 34.40%. This generation actively accesses social media and platforms such as YouTube, making it a strategic target in delivering messages about digital security. In addition, referring to the research results, Jabali & Baher (2024) emphasized the importance of integrating digital security education into the college curriculum to equip the younger generation, especially students, with the knowledge and skills to deal with cyber threats such as online fraud.

Zwilling et al. (2022) stated that campaigns have a positive impact on raising awareness and knowledge. Meanwhile, Bada et al. (2020) mentioned that safety education should be targeted, applicable, and provide feedback from the community. In research, Chang & Coppel (2020) the cybersecurity campaign method in the form of a comic strip called Cyber Baykin proved to be influential because it was measured through the understanding of the general public, and the program was sustainable. Furthermore, according to Sekar et al. (2024). The influence of online campaigns on society can be measured using AIDA indicators. Attention refers to the audience's attention to the online campaign “Don’t Know? Kasih No!” through attractive visuals. Interest refers to the audience's interest in the jargon of the self-protection movement, “Don’t Know? Kasih No!”. Desire refers to the audience's desire to apply messages or tips in everyday life. While Action refers to the real action of the audience in keeping their data safe. Limna et al. (2023) argue that knowledge is key in protecting oneself from online fraud, especially in keeping personal data safe. However, according to Bada et al. (2020), Knowledge alone is not enough; it must be accompanied by the formation of positive habits in cyber behavior. Referring to research, Kovacevic et al. (2020) found that students failed to answer questions about cybersecurity correctly, despite the availability of many online educational resources. They identified two main indicators in measuring cybersecurity knowledge, namely general knowledge and perception of cybersecurity. General knowledge includes the ability to recognize threats such as phishing, social engineering, and pharming, and knowing how to take action to protect personal data. Meanwhile, perception of cybersecurity refers to an individual's attitude in assessing and realizing their ability to deal with cybersecurity threats.

Important aspects of information security include: (1) confidentiality, which is an effort to keep personal information from being accessed by unauthorized parties; and (2) integrity, which is an effort to ensure that data is not altered by unauthorized parties. (Dwijo Kangko et al., 2023). To support self-protection of information, two behavioral theories are used, namely: Theory of Planned Behaviour, which reflects individual attitudes and behavioral control; and Protective Motivation Theory, which considers two factors, namely perceived threat and perceived efficacy. (Jabali & Baher, 2024). These two theories will help measure the protective behavior of Generation Z Bank BCA customers through two supporting variables, namely online campaigns and cybersecurity knowledge.

2 Methodology

This research uses quantitative research methods through questionnaires distributed to Generation Z Bank BCA customers. This method of data collection is used by Sulaiman et al. (2022) with a sample of 446 respondents for a survey on cyber knowledge towards behavioral protection. This study examines two independent variables, namely: (X1) online campaign and (X2) cybersecurity knowledge, which were analyzed for their influence on the dependent variable (Y), namely, protective behavior. The sampling technique was non-probability sampling, specifically purposive sampling, where respondents were selected based on the following criteria: are active customers of BCA Bank, have watched BCA Bank's online campaign “Don’t Know? Kasih No!”, aged between 17 to 27 years old, and educational background as an additional criterion. The minimum targeted sample size was 100 respondents. Data collection was conducted through a questionnaire distributed through Google Forms.

3 . Results and Discussion

3.1 Result

Data was collected quantitatively through an online questionnaire distributed via social media to active BCA Bank customers aged 17-27 who had seen the online campaign “Don’t Know? Kasih No!”. Primary data was obtained from 100 respondents for classical assumption and hypothesis testing using SPSS version 30. The questionnaire consisted of 34 questions covering variables (X1) online campaign and (X2) cybersecurity knowledge, and protective behavior (Y), and categorized by gender, age, domicile, education, and occupation.

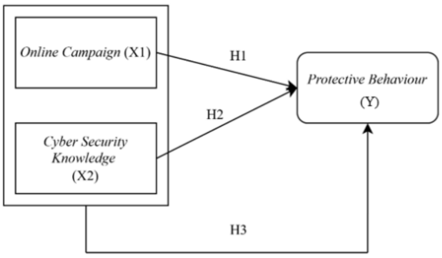

Figure 1. Research framework

Table 1. Respondent Characteristics based on Gender

No.	Gender	Amount	Percentage
1	Female	59	59%
2	Male	41	41%
	Total	100	100%

Data processed, 2025 [source]

Referring to Table 1. Characteristics of respondents based on gender, the largest result was obtained in the female gender at 59% (59 people), and the smallest was male at 41% (41 people). This is relevant to the results of the Online Gender-Based Violence (GBV) Safenet (2024), which notes that women are more vulnerable and prone to online crime.

Table 2. Respondent Characteristics based on Age

No.	Age	Amount	Percentage
1.	17 – 20 Year	28	28%
2.	21 – 24 Year	39	39%
3.	25 – 27 Years	33	33
	Total	100	100%

Data processed, 2025 [source]

Referring to Table 2. Characteristics of respondents based on age, the results obtained are scattered for the range of 17 - 27 years. The largest at the age of 21 - 24 years was 39% (39 people), in the range of 25 - 27 years was 33% (33 people), and for the lowest result at the age of 17 - 20 years, it was 28% (28 people). This also supports a survey conducted by the Association of Indonesian Internet Service Providers (APJII) Survei & Responden (2024), which states that the highest penetration rate and contribution is Generation Z.

Table 3. Respondent Characteristics based on Domicile

No.	Province	Amount	Percentage
1.	Aceh	1	1%
2.	Banten	9	9%
3.	DI Yogyakarta	11	11%
4.	DKI Jakarta	6	6%
5.	Jambi	3	3%
6.	West Java	27	27%
7.	Center Java	12	12%
8.	East Java	11	11%
9.	West Kalimantan	3	3%
10.	South Kalimantan	1	1%
11.	Center Kalimantan	1	1%
12.	Keplauan Riau	3	3%
13.	North Maluku	1	1%
14.	Riau	1	1%
15.	South Sulawesi	2	2%
16.	West Sumatera	4	4%
17.	North Sumatera	4	4%
	Total	100	100%

Data processed, 2025 [source]

Referring to Table 3. Characteristics of respondents based on domicile, respondents are spread across provinces in Indonesia. The largest province is West Java province at 27% (27 people), and for the provinces of DI Yogyakarta, Central Java, and East Java, more than 10 people are represented. Then, for the rest, each is represented by 1 - 9 respondents. This shows that Generation Z customers.

Table 4. Respondent Characteristics based on the Latest Education

No.	Latest Education	Amount	Percentage
1.	Senior High School	44	44%
2.	Diploma (D1, D2)	11	11%
3.	Bachelor (S1, S.Tr)	29	29%
4.	Postgraduate (S2, S3)	16	16%
	Total	100	100%

Data processed, 2025 [source]

Referring to Table 4, which presents the characteristics of respondents based on their most recent educational background, the highest proportion is from respondents whose last education level was senior high school, accounting for 44% (44 individuals). The lowest proportion is from respondents with a diploma-level education (D1, D2), accounting for 11% (11 individuals). This is consistent with a survey conducted by the Indonesian Internet Service Providers Association (APJII) Survei & Responden (2024), which notes that for the last education Senior High School has a greater penetration and contribution of 31.43% compared to other education levels

Table 5. Respondent Characteristics based on Occupational

No.	Occupational	Jumlah	Presentase
1.	College Student	51	51%
2.	Teacher/Lecturer	9	9%
3.	Employee	19	19%
4.	Bussinesman	21	21%
	Total	100	100%

Data processed, 2025 [source]

Referring to Table 5. Characteristics of respondents based on occupation, the largest results were obtained in Students / Students at 51% (51 people), and for the smallest results, there were 9% (9 people) of Teachers / Lecturers. This is relevant to the survey results of the Indonesian Internet Network Operator Association (APJII) Survei & Responden (2024), where students and college students have the highest penetration rate at 95.92%.

3.2 Discussion

The distribution of statements on the three variables-Online Campaign (X1), Cybersecurity Knowledge (X2), and Protective Behavior (Y)-is measured using specific indicators that have been defined for each variable.

Table 6. Distribution of Each Question on the Online Campaign Variable (X1)

Pernyataan	**Jawaban**					**Total**	**Skor**	**Skor**	**Capaian**
	STS	**TS**	**N**	**S**	**SS**		**Empiris**	**Maksimum**	**Hasil**
Online Campaign (X1)									
									Attention
X1.1	0	0	1	85	64	100	444	500	89%
X1.2	1	4	16	81	48	100	409	500	82%
X1.3	0	0	7	76	68	100	440	500	88%
									Interest
X1.4	0	0	7	54	89	100	452	500	90%

X1.5	0	1	10	76	63	100	437	500	87%
X1.6	0	0	8	67	75	100	441	500	88%
									Desire
X1.7	0	0	5	63	82	100	449	500	90%
X1.8	0	1	6	82	61	100	432	500	86%
X1.9	0	0	5	67	78	100	448	500	90%
									Action
X1.10	0	1	9	61	79	100	440	500	88%
X1.11	1	0	8	74	67	100	435	500	87%
X1.12	0	2	10	71	67	100	431	500	86%

Data processed, 2025 [source]

Table 4.1, the highest questionnaire item on the Online Campaign variable is in statement X1_4 (interest indicator) with an empirical score of 452 and 90% achievement. The second and third highest scores are X1_7 and X1_9 (desire indicator), with scores of 449 and 448, respectively, also with 90% achievement. Based on the statement items, it shows interest in the online campaign program and an increase in vigilance and caution after seeing the “Don’t Know? Kasih No!”.

Table 7. Distribution of Each Question on the Cybersecurity Knowledge (X2)

Pernyataan	**Jawaban**					**Total**	**Skor**	**Skor**	**Capaian**
	STS	**TS**	**N**	**S**	**SS**		**Empiris**	**Maksimum**	**Hasil**
Cybersecurity Knowledge (X2)									
									General Knowledge
X2.1	0	6	15	70	59	100	417	500	83%
X2.2	0	1	10	58	81	100	445	500	89%
X2.3	0	2	4	47	97	100	457	500	91%
									Cybersecurity Perceptions
X2.4	2	4	11	69	64	100	421	500	84%
X2.5	3	4	12	74	57	100	411	500	82%
X2.6	0	4	15	64	67	100	425	500	85%

Data processed, 2025 [source]

Table 4.2, the highest item on the Cybersecurity Knowledge variable is X2_3 (general knowledge indicator) with an empirical score of 457 and 91% achievement. This item states that respondents know suspicious links can steal personal data. The respondents' results from the statement item show that customers already have general knowledge about online fraud crimes in the form of suspicious links.

Table 8. Distribution of Each Question on the Protective Behaviour (Y)

Pernyataan	**Jawaban**					**Total**	**Skor**	**Skor**	**Capaian**
	STS	**TS**	**N**	**S**	**SS**		**Empiris**	**Maksimum**	**Hasil**
Online Campaign (X1)									
									Attitude Toward Forward
Y.1	0	0	6	47	97	100	455	500	91%
Y.2	0	1	7	47	95	100	451	500	90%
Y.3	1	0	9	80	60	100	431	500	86%
Y.4	1	0	6	56	87	100	449	500	90%
									Perceived Behavioral Control
Y.5	0	2	11	65	72	100	433	500	87%
Y.6	1	0	4	72	73	100	435	500	87%
Y.7	1	1	12	73	63	100	433	500	87%
Y.8	0	0	6	58	86	100	453	500	91%

									Perceived Threat
Y.9	0	0	3	58	89	100	461	500	92%
Y.10	1	8	7	67	67	100	416	500	83%
Y.11	0	1	5	61	83	100	454	500	91%
Y.12	1	1	7	61	80	100	443	500	89%
									Perceived Efficacy
Y.13	1	3	15	75	56	100	422	500	84%
Y.14	0	1	6	78	65	100	440	500	88%
Y.15	0	1	7	65	77	100	447	500	89%
Y.16	0	0	9	76	65	100	433	500	87%

Data processed, 2025 [source]

Table 4.3 lists the highest item on the Protective Behavior variable as Y_9 (Perceived Threat indicator), with an empirical score of 461 and an achievement rate of 92%. This item states that online fraud on behalf of BCA Bank is considered a serious threat. This indicates that self-protection is perceived because customers sense the threat faced by Generation Z Bank BCA customers.

Table 9. Results of multiple linear regression analysis and partial T

Coefficients

Model	Unstandardized - B	Coefficient Std. Error	Standardized Coefficient Beta	t	Sig.
(Constant)	16.853	7.915		2.129	.036
X1	.688	.171	.358	4.023	.000
X2	.681	.158	.383	4.296	.000

The data were processed using SPSS version 26.0, 2024 [source]

The analysis results show that the constant value of protective behavior is 20.742. The online campaign coefficient is 0.606 and Cybersecurity Knowledge is 0.699. This means that each one unit increase in each variable will increase protective behavior by 0.606 and 0.699, assuming other variables remain constant.

Based on the partial T test results, online campaigns have a positive and significant influence on protective behavior. When BCA's Generation Z customers show attention and interest in the online campaign, they tend to apply the messages and tips conveyed, thus encouraging protective actions against online fraud. This finding is in line with the concept of individual attitudes and perceived efficacy, where customers perceive online fraud as a serious threat and respond by protecting themselves based on campaign messages. This result is consistent with research by Chang & Coppel (2020), which found that a comic campaign in Myanmar was effective in increasing public understanding of cybersecurity. Similarly, Tasevski (2016) found that campaigns through websites, videos, and posters in Macedonia had a significant impact on students' self-protection against cyber threats.

Based on the partial T-test results, cybersecurity knowledge has a positive and significant influence on protective behavior. This shows that Generation Z Bank BCA customers have general knowledge, such as recognizing suspicious links, as well as perceptions of cybersecurity, including the ability to distinguish between official and unofficial information. According to aspects of behavioral control and perceived threat, these factors influence self-protective behavior. When individuals are aware of the threat of online fraud, they tend to control their behavior by using their knowledge to implement safe digital practices. This finding is supported by research Limna et al. (2023) and Zwilling et al. (2022) which shows that cybersecurity knowledge has a significant effect on protective behavior. In addition, Lameck Mkilia et al. (2023) also emphasized that cybersecurity self-awareness is closely related to knowledge of cyber threats and their potential impact.

Table 10. Results of Simultaneous Test (F)

ANOVA

Model	**Sum of Squares**	**Df**	**Mean Square**	**f**	**Sig.**
Regression	909.244	2	454.622	33.072	.000[b]
Residual	1333.396	97	13.746		
Total	2242.640	99			

The data were processed using SPSS version 26.0, 2024 [source]

Referring to Table 10. The results of the F test (simultaneously) obtained a significance value of 0.000, which means that the two independent variables - online campaigns and cybersecurity knowledge jointly affect the protective behavior of Generation Z Bank BCA customers.

Table 11. Results of R Square

Model Summary [b]

Model	**R**	**R Square**	**Adjusted R Square**	**Std.Error of the Estimate**
1	.637[a]	.405	.393	3.708

The data were processed using SPSS version 26.0, 2024 [source]

Model Summary, the R Square value is 0.405. This indicates that 40.5% of the variation in protective behavior (Y) can be explained by the online campaign (X1) and Cybersecurity Knowledge (X2) variables. These two variables represent the four components in the theoretical framework. The online campaign variable reflects TPB through attitude towards behavior, and PMT through perceived efficacy. This shows that online campaigns are influential in shaping the behavioral attitudes of Generation Z customers in responding to online fraud through online campaign programs. Meanwhile, the cybersecurity knowledge variable reflects behavioral control in TPB and perceived threat in PMT theory. This shows that Generation Z customers are able to recognize the threat of online fraud and use their knowledge to protect themselves. Overall, by applying the tips and messages conveyed in the online campaign, BCA's Generation Z customers demonstrate awareness of cybersecurity and can protect themselves from online fraud. In addition, 59.5% are factors that are not examined by the author, such as those found by Tarrad et al. (2022), where there are other factors, such as information security, creative behavior, cyber education, and cyber training, that help people's self-protection attitudes.

4 Conclusion

Based on the results and discussion, it can be concluded that the online campaign program succeeded in attracting the attention and interest of BCA's Generation Z customers, as well as encouraging them to apply the messages conveyed, which ultimately resulted in protective actions against online fraud. In addition, Generation Z customers have demonstrated the ability to distinguish legitimate information, reflecting strong cybersecurity perceptions, thereby reducing the risk of falling victim to fraud. The research also shows that the online campaign “Don’t Know? Kasih No!” and cybersecurity knowledge simultaneously contribute to increasing the protective behavior of Generation Z Bank BCA customers in dealing with online fraud. Future researchers are advised to expand the coverage of respondents' age groups, including Millennials, Generation X, and Baby Boomers. This broader coverage is necessary to gain insights from various generational perspectives regarding the influence of online campaigns and cybersecurity knowledge on protective behavior against online fraud.

Acknowledgment

The author would like to thank the thesis supervisor at the Finance and Banking Study Program, Politeknik Negeri Jakarta, for her support and assistance in providing input for this writing. Likewise, to the Head of the Applied Finance and Banking Study Program, the Head of the Accounting Department, and the Director of Politeknik Negeri Jakarta, for conducting this research.

References

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2020). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*

Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers and Security*, *97*. https://doi.org/10.1016/j.cose.2020.101959

Dwijo Kangko, D., Putri Tungga Dewi, E., & Yahya Maulana, A. (2023). *PENGARUH KESADARAN KEAMANAN INFORMASI REMAJA TERHADAP PENYALAHGUNAAN DATA PRIBADI DALAM PENGGUNAAN MEDIA SOSIAL TWITTER* (Issue 2).

Jabali, A., & Baher, N. (2024). *DEGREE PROJECT Exploring the impact of cybersecurity knowledge and awareness on behavioral choices for protection among university students in Sweden*.

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, *8*, 125140–125148. https://doi.org/10.1109/ACCESS.2020.3007867

Lameck Mkilia, E., Lameck, E., Jones, M., Kaleshu, T., & Sife, A. S. (2023). Cybersecurity Risks and Customers' Protective Behavior on Usage of Mobile Banking Services: Evidence from Selected Banks in Tanzania. In *Local Administration Journal* (Vol. 16, Issue 3).

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The Relationship between Cybersecurity Knowledge, Awareness and Behavioural Choice Protection among Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research*, *7*, 1133–1151. https://doi.org/10.25147/ijcsr.2017.001.1.123

Otoritas Jasa Keuangan. (2024). *Laporan Kinerja Triwulan II-2024*.

Safenet. (2024). kriteria gender responden. *kekerasan berbasis gender di ranah online*.

Sekar, A., Umami, N., Lutfi, A. M., Kusumawati, A., Hayyu, D., Muna, R., & Ningsih, T. D. (2024). Efektivitas Startegi Kampanye Iklan Edukasi Bank Bca "Don't Know? Kasih No!" Terhadap Maraknya Fenomena Phishing Di Masyarakat. In *Jurnal Ekonomi Manajemen dan Akuntansi* (Vol. 2, Issue 1). https://jsr.lib.ums.ac.id/index.php/determinasi▪page57

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information (Switzerland)*, *13*(9). https://doi.org/10.3390/info13090413

Survei, M., & Responden, S. (2024). *DAFTAR ISI*.

Tarrad, K. M., Al-Hareeri, H., Alghazali, T., Ahmed, M., Al-Maeeni, M. K. A., Kalaf, G. A., Alsaddon, R. E., & Mezaal, Y. S. (2022). Cybercrime Challenges in Iraqi Academia: Creating Digital Awareness for Preventing Cybercrimes. *International Journal of Cyber Criminology*, *16*(2), 15–31. https://doi.org/10.5281/zenodo.4766564

Tasevski, P. (2016). IT and Cyber Security Awareness – Raising Campaigns. *Information & Security: An International Journal*, *34*, 7–22. https://doi.org/10.11610/isij.3401

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269