JURNAL
Riset Akuntansi dan Keuangan Indonesia
URL : http://journals.ums.ac.id/index.php/reaksi/index

INDONESIAN SMEs AND CYBERSECURITY: DEVELOPING INSTRUMENT TO TEST SMEs OWNERS' CAPABILITY IN DETECTING PHISHING EMAILS

Ratna Yudhiyati[1], Diana Rahmawati[2], Afrida Putritama[3]
[1]University of Wollongong, Australia
[2,3]Universitas Negeri Yogyakarta, Indonesia
*ryudhiyati@uow.edu.au

Keywords:
phishing email, small and medium-sized enterprises (SMEs), knowledge assessment, information system, cybersecurity

ABSTRACT
This study identified the characteristics of phishing emails and designed an instrument to assess the level of individual knowledge in detecting various phishing messages. This instrument is primarily designed for SMEs. The instrument is to be used not only as a testing tool for phishing detection skills, but also as the foundation for generating training materials or phishing detection guidelines for SMEs. This study developed a test of phishing susceptibility by collecting various real-life legitimate and phishing emails, and ask test takers to identify which emails are legitimate and which emails are phishing. Based on the validity and reliability tests, the created instrument has high content validity for all question items but only reaches medium reliability. The test reliability can be improved by adding questions, or modify the question by having multiple-choice of answers for each question instead of Yes/No answer choices.

p-ISSN:1411-6510
e-ISSN:2541-6111

INTRODUCTION

The risks of phishing are increasing due to increased uses of email in modern communication. Phishing attacks are acts of cybercriminals who manipulate electronic messages using social engineering tactics to deceive the recipients of the messages, so that they believe that the message came from a trustworthy or legitimate source (Wright *et al*., 2014). When individuals are deceived by phishing messages and follow the instructions listed, phishers (the perpetrator of phishing attacks) can steal information and identities, access accounts, and sell them to other parties or use them to commit financial fraud (Jensen *et al*., 2017).

Phishing attacks have gotten more sophisticated in recent years (Furnell, 2007; Symantec, 2016). Initially, most phishing attacks were carried out by sending mass e-mails to a large number of people, with an expectation that some of the receivers would be deceived (Wright *et al*., 2014). However, in recent years, phishing has evolved and harder to detect, as phishers develop custom messages to specific people or groups (Jensen *et al*., 2017; Symantec, 2016). Phishing that specifically targets specific individuals or small groups is called spear-phishing. Spear-phishing emails are typically designed to meet the expectations of their intended receivers, and some communications may even contain information that only the recipient or group of recipients is aware of, which improve the chance of success for the phishing attack. Symantec (2016), found that regular phishing attacks decreased between 2013 and 2015, while spear-phishing attacks increased significantly. Given the increasing number of spear-phishing where the phishing messages are developed specifically for each target group, technology-based safeguards are becoming unreliable. Email users are ultimately the most crucial factor in identifying phishing schemes (Wang *et al*., 2017).

Since the Covid-19 pandemic, many SMEs have relied on information technology to conduct their business (Falch *et al*., 2023). SMEs adoption of information technology is not only about generating competitive advantage, but also a matter of business survival (Yudhiyati *et al*., 2021); yet, the adoption of new technologies introduces new business risks for SMEs, namely cybersecurity risk (Rahmawati *et al*., 2019). Thus, cybersecurity is an important topic for SMEs.

However, most SMEs do not have proper cybersecurity measure. Most of them rely on the cybersecurity measures embedded in the solutions they bought form the third-party providers (Falch *et al*., 2023; Yudhiyati *et al*., 2021; Renaud, 2016). They have limited financial and human resources to devote to cybersecurity. (Burda *et al*., 2023; Corzo *et al*., 2018) , so they are generally considered vulnerable to cybersecurity threats (Yudhiyati *et al*., 2021). Several surveys also found that individuals in SMEs are more likely to be targeted by cybersecurity threat (Symantec, 2019; Wilson *et al*., 2019) . Phishing and email-based cyber-attacks are great concerns for SMEs (Falch *et al*., 2023). According to Wilson et al, (2023), phishing is one of the cybersecurity risks to which SMEs are most vulnerable. The frequency of phishing targeted on small firms has increased in recent years, and its success rate is relatively high. Email-based cyber-attacks have a greater chance of success in organisations with less formal procedures to manage information systems, such as SMEs (Falch *et al*., 2023). This situation is concerning since email service and other internet services that require email are the most commonly used information technology for SMEs.

Most research on phishing focus on large corporations, while SMEs are frequently not studied due to SMEs' low interest in this subject (Burda *et al*., 2023). However, SMEs have different business profiles, organisational cultures, and social dynamics, which may cause them to respond to phishing differently than large organisations, which are normally the focus of phishing study (Burda *et al*., 2023).

Given the growing number of spear-phishing attacks in which the phishing electronic messages are tailored to each target group, technology-based preventive measures are becoming ineffective. The users of email service are ultimately the final and most essential factor in identifying phishing attacks (Wang *et al*., 2017).

There were several studies examining the human or user side of phishing. The topics that were raised were diverse. Several studies examined factors that affect individuals' susceptibility to phishing attacks or their ability in detecting phishing attacks (Wright *et al*., 2014; Wang et *al*., 2017; Vishwanath *et al*., 2011; Kimpe *at al*., 2018).

Several research developed training strategies that are successful in educating individuals to recognise phishing attempts (Jensen *et al.*, 2017; Zielinska *et al.*, 2014). Unfortunately, only few studies about phishing specifically focus on SMEs (Burda *et al.*, 2023; Corzo *et al.*, 2018).

Most studies about phishing require an instrument to assess an individual's capacity to identify phishing. Researchers have a difficulty in selecting a suitable instrument to quantify these qualities. Several researchers conducted a phishing experiment by delivering a phishing message to respondents, aimed to be as authentic as possible, without their knowledge. However, this strategy is difficult to implement because it involves the agreement of many stakeholders and there are ethical concerns to be considered (Vishwanath *et al.*, 2011). Another strategy is to perform controlled experiments in which respondents are aware that they will get a phishing message, although not knowing the form of the message or the time of transmission. Unfortunately, this strategy has also been criticised for its potential bias (Vishwanath *et al.*, 2011).

Several studies employed a questionnaire to assess an individual's ability to detect phishing rather than a simulation of sending phishing messages in their study (Wang *et al.*, 2023), (Zielinska *et al.*, 2014). This technique enables researchers to assess how accurate respondents are in detecting individual phishing messages with minimum bias (Falch *et al.*, 2023). This instrument is not suitable for measuring the effect of psychological and environmental factors experienced by respondents after receiving phishing mails. However, this instrument is helpful when researchers want to examine the level of individual expertise in recognising the characteristics and signs of phishing emails.

This study identified the characteristics of phishing messages and developed an instrument to assess the individual's proficiency in detecting various phishing messages. This instrument is primarily designed for SMEs. There is a need to equip SMEs against phishing, because the frequency of spear phishing attacks on SMEs have increased significantly for recent years (Symantec, 2016). Indonesian SMEs are especially vulnerable in safeguarding against phishing since most Indonesian SMEs rely on internet-based applications offered by third parties, and they have limited understanding of information technology fraud prevention measures (Yudhiyati *et al.*, 2021). To the best of the researcher's knowledge, no study has assessed SMEs' abilities to prevent phishing in Indonesia. This instrument is also designed not only as a tool for testing individual abilities in detecting phishing messages, but also as a basis for creating training materials or guidelines in phishing prevention for SMEs.

LITERATURE REVIEW

Cybersecurity Threat for SMEs

Cybersecurity is an important issue for SMEs. Most cybersecurity studies focusing on SMEs explored how SMEs perceived cybersecurity threat and how they implement cybersecurity measures. Berry & Berry (2018), found that small business owners identified that three out of six top critical issues for small businesses are information technology-related. SMEs understand that when businesses use information technology, they risk being attacked by cybercriminals. However, for most SMEs, the cyber risks are ambiguous, and they do not know exactly what they can lose from cyber assaults (Yudhiyati *et al.*, 2021). Most SMEs also believe that they only need to adopt basic cybersecurity measures since most SMEs employ IT services provided by third-party (Rahmawati *et al.*, 2019; Berry & Berry, 2018), and they believe that the main burden of providing cybersecurity measures falls with the third-party providers (Yudhiyati *et al.*, 2021; Khan *et al.*, 2020; Le *et al.*, 2024).

SMEs' low cybersecurity awareness is a prevalent issue in most nations, such as the UK (Renaud, 2016; Wilson *et al.*, 2023), the US (Berry & Berry, 2018), Denmark (Falch *et al.*, 2023), and developing countries such as Indonesia (Yudhiyati *et al.*, 2021). They do not believe that they are worth being targeted by cybercriminals due to their size, thus they merely apply the minimal security measures (Symantec, 2019). However, while SMEs may experience fewer cyber-attacks compared to larger companies, cyberattack impacts are generally more severe for SMEs (Wilson *et al.*, 2023; Rawindaran & N, 2023; Fagbule & O, 2023). Cybercrimes also have a detrimental effect on SMEs' opportunities since many large companies avoid doing business with SMEs that have been victims of severe cyber attacks (Renaud, 2016; Le

p-ISSN:1411-6510
e-ISSN:2541-6111

et al., 2024).

Several studies observed that one of the reasons why most SMEs do not adopt proper security measures, although recognising that there are risks in employing information technology, is the high level of uncertainty they face in respect to cybersecurity. Research and knowledge gaps in cybersecurity awarness for small and medium-size enterprises (Chaudhary *et al*., 2023). Renaund (2016) claimed that many SMEs requested cybersecurity information and training, indicating the SMEs are experiencing a high degree of uncertainty about this topic. SMEs are overwhelmed by the options of internet security measures and recommendations provided by various institutions, which may be varied, and they are unclear about what they need to do. This uncertainty is the reason why most SMEs hope that they get cybersecurity training authorised from governments, which are regarded legitimate parties (Yudhiyati *et al*., 2021; Renaud, 2016; Papathanasiou *et al*., 2024).

Previous Studies about Phishing

Unfortunately, there are only few studies about phishing that focus on SMEs owners or entrepreneurs. Most phishing studies focus on individuals without differentiating their occupation background, so their findings are also relevant for this study.

Most studies about phishing aimed to identify factors that affect individuals susceptibility to phishing attacks. Kimpe et al, (2018) revealed that persons who frequently use online features for commerce or acquiring resources are more likely to be targeted by phishing attempts than those who rarely do so. They are more exposed to cyber community and they are used to received high number of emails. Viswanath et al, (2011) observed that individuals that receive a large number of emails and rely heavily on emails for important communication are more likely to fall victim to phishing because they frequently ignore several phishing signals due to the volume of emails they receive.

These findings appear to contradict another study, which revealed that individuals with more extensive internet experience and computer use are more likely to *not* be deceived by phishing attacks (Wright & Marett, 2020). However, it is important to understand the difference between being *targeted* by phishing and *falling victim* to phishing. The former implies that persons may receive a phishing message but are not necessarily deceived by it, whereas the latter focuses on those who are deceived by the message. The high frequency of internet use may raise the chance of being targeted by phishing; yet, less expertise and exposure to the internet will increase the chance of *successful* phishing attacks. Individuals who rarely use internet are more likely to have low computer self-efficacy and exposure, which increase their chance of being deceived when they receive phishing emails (Wright & Marett, 2010). Wright and Marett (2010) suggested that the best way to prepare against phishing is having adequate experience in internet and computer use, alongside proper security knowledge and a healthy dose of suspicion.

There are only handful phishing studies that focus on SMEs. Rodriguez-Corzo et al. Wright et al, (2014) suggested a cybersecurity risk management that can be implemented by SMEs which address characteristic of company, technology used, and the people in the company. Burda et al, (2023) conducted a phishing experiment with employees in an SME and observed that detection of inconsistent pattern was the primary method how these employees detect the spear-phishing attack. These employees know each other and the firm well and notice some inconsistent pattern of communication in the phishing message, such as the tiny variation in the corporate logo or the different email signature used by the CEO. This study showed a unique character of SMEs in relation to phishing susceptibility.

How Phishing was Measured in Previous Studies

Quantitative studies about phishing measure it in various ways. Several studies specifically selected phishing victims or people that ever receive phishing emails as respondents. These studies explored the characteristics of these respondents who were actually targeted by phishing attacks, and whether they fell victim to the attack or not (Vishwanath *et al*., 2011; Kimpe *et al*., 2018; Ascic & H.J, 2023). However, only a few studies use this method since the experience of being a fraud victim is sensitive and rarely discussed, thus researchers have a limited number of possible respondents.

Other studies conduct experiment by sending simulated phishing emails to respondents and assess whether they fall for the deception or not (Wright *et*

al., 2014; Burda *et al*., 2023; Wright & Marett, 2010). The key issue of using this approach is obtaining sufficient approval from relevant authorities and managing the unfavourable responses from the respondents after the research, because some of them may be unhappy to be deceived. Another limitation is that this technique can only assess individuals' abilities to identify phishing for a specific email. However, this approach arguably provides the best way to measure how individuals' environment contribute in their ability in detect phishing.

Another approach commonly used to measure phishing is to run a test to examine respondents' ability to detect phishing among a handful of phishing messages that researchers ask them to analyse (Furnell, 2007; Wang *et al*., 2017; Zielinska *et al*., 2014). This technique has limitations in its ability to simulate the environmental factors that may affect individuals' response to phishing emails, but this approach is the easiest to perform compared to the previous ones, and it is also a good measure to assess individuals' phishing susceptibility without any influence from other external factors.

RESEARCH METHODS

This research is development research using the ADDIE model. The model provides a step-by-step process that are often used to develop training instrument (Pears & Konstantinidis, 2021). The five stages of the model are: **A**nalysis, **D**esign, **D**evelopment, **I**mplementation, and **E**valuation. Throughout the 5 stages, this research identified what are the topics to be tested, how it should be tested, develop the test, implement the test in real-world setting, and analyse the impact to both the test and process.

Phase I – Analyse the topics to be tested

The main objective of Phase I is identifying a list of phishing message characteristics and prioritise their importance to be included in the testing instrument This phase entailed doing a literature review to determine topics or skills required to identify phishing messages that should be included in the test. This literature review focuses on assessment tools used in past studies of competence and literacy in the use of information technology.

Based on the result of the literature review, the research team interviewed small business owners and IT practitioners to analyse the urgency of the identified topics, and prioritise the topics to be included in the test.

Phase II – Design the test

Phase II included designing the test design, such as choosing the format of the test and how many of question items in the test. The initial draft is designed using a simple template in Microsoft Word which clearly showed the aspect tested in each question. The research team analysed each question item to make sure that the test addressed all the topics identified in the Phase I. In this phase, the research team also decided on the arrangement of the test items.

The research team conducted content validity test based on the initial draft. Content validity test is carried out by a panel of experts. Each of the expert needs to fulfill one of the following conditions; (1) works in fields related to auditing, fraud or information systems, or (2) have an educational background in fraud or information systems. The testing technique used is the V formula suggested by Aiken (Azwar, 2019), (Retnawati, 2016). Each expert gave a score between 1 (very irrelevant) to 5 (very relevant) for each test item related to the targeted topic and subtopic. The form used by the raters for the validity test is shown in Table 1.

Phase III – Develop the test

Table 1. The Form for Expert to Evaluate the Content Validity

Subtopic	Indicator	Items	Relevance Assessment				
			1	2	3	4	5

Based on the original draft generated in Phase II, the research team inserted the picture of each selected email in the Google Form as a quiz and put the question and directions for the test that were designed in Phase II.

Phase IV – Implement the test

Phase IV involved the field test of the instrument. The research team distributed the developed instrument to respondents. The respondents of the field test are 31 SMEs owners

p-ISSN:1411-6510
e-ISSN:2541-6111

in DI Yogyakarta province which attended an information security workshop held by Faculty of Economics, Universitas Negeri Yogyakarta.

Phase V – Evaluate the test

The research team evaluate the test using the data collected form the fieldwork in Phase IV. There are two aspects that that the team evaluated. First, the research team evaluate the reliability of the test. Reliability refers to how consistent a measurement tool is. Consistency in this case suggests that the variety in scores obtained by test participants represents differences in the level of ability predicted by the test, instead of faults in the assessment instrument (Azwar, 2019). This research measures test reliability with a coefficient of α20 or KR-20 (Azwar, 2019). The research team tallied the scores of respondents who take the exam and calculate the reliability coefficient based on this data. The team evaluates if the instrument is acceptable or if there are any improvements that can be made.

Second, the research team also evaluate findings or interesting information about the Indonesian SMEs' capability in detecting phishing emails based on data collected from the field test. While the collected information may not be able to be generalised to the Indonesian SMEs as a whole, it can provide interesting information for future study.

RESULTS AND DISCUSSION

This research study produced an instrument for assessing individuals' proficiency in identifying phishing emails, particularly SMEs' owners or entrepreneurs.

Findings – Phase I

Table 2. The Aspects and Indicators in the Testing Instrument

Aspect	Indicator	How it will be incorporated in the test
Phishing cues	Attention to email source	The email address of the sender is not the legitimate email address for the assumed identity.
	Attention to grammar and spelling	There are misspelling and typos in the email that should not exist in formal emails sent by legal institutions.
	Attention to urgency cues	The email talks about urgent matter and important issues, which are relevant for those who have business interest with the (presumed) email senders.
	Attention to resources in the emails	The email contains attached file or hyperlink.
Influencing technique	Liking	The sentences in emails emphasises closeness to the recipient, such as "We'd like to give you the best shopping experience possible".
	Reciprocity	The sentences in the email asks for the recipient's help to repay for previous favours, such as "Please help us to keep your bank account secure by...."
	Social proof	The sentences in the email emphasises that there there are many people doing the same thing that the email's recipient are asked to do, such as "All bank account holders need to update ...".
	Consistency	The emails ask the recipients to take actions which are a continuation as their previous decision, such as "Because you registered as a new account holders, please update you personal information...."
	Authority	The emails look like that they were sent by people with proper authority to convey the message.
	Scarcity	The emails ask recipients to do some actions within certain time limit or imply that the recipients will lose an opportunity if the do not do what the emails ask.

Based on literature review, this study concluded that the test should include two main aspects: (1) the individuals capability in detecting physical cues in emails that indicate phishing emails (Vishwanath et al., 2011), and (2) the individuals ability to resist the influencing technique used in phishing emails (Wright et al., 2014). Influencing technique is how email writers select specific wordings for their sentences to lessen the reader's vigilance. The existence of influencing technique in emails does not mean that those emails are phishing, since this technique is also often used by advertisers. However, email readers can increase their vigilance when receiving emails if they notice

these techniques. The details of physical cues and influencing techniques are described in Table 2.

Based on initial interviews with SMEs' owners, SMEs are more likely to suffer financial loss due to emails purportedly sent by institutions SMEs' owners rarely communicated with individual peers and colleagues using emails, and most of them only use emails to communicate with the providers of internet-based applications they use in their business. Hence, the research team decided to focus on phishing messages purportedly sent by institutions, instead of personal emails.

Table 3. The Analysis of How Each Question in the Test Includes the Identified Topics

Aspect and Indicator	Question Number							
	1	2	3	4	5	6	7	8
Phishing Cues								
Attention to email source	V			V	V	V		V
Attention to grammar and spelling	V	V						
Attention to urgency cues	V			V				
Attention to resources in the emails		V	V			V		V
Influencing technique								
Liking			V			V	V	V
Reciprocity			V			V		
Social proof			V					V
Consistency	V					V		
Authority		V		V				
Scarcity				V				

Findings – Phase II

After deciding the main topics that should be included in the test, the research team decide on the how the test items are arranged and presented to the test takers. The designs are as follows:

- Each question will include a picture of an email that participants must identify as phishing or legitimate email. Emails included in the test were retrieved from the phishing email reporting database or the research team's email inbox, hence the emails included in the test are genuine emails.
- The emails shown in the test and test instructions are written in Indonesian since this test is targeted to Indonesian SMEs.
- Each question is multiple choice, with just two response options: (a) phishing/fake emails and (b) legitimate emails. The correct answer will receive a score of one, while the incorrect answer will receive a score of zero.
- There will be eight questions in the test, with the maximum score that the participant can obtain is 8.
- The test is delivered as a quiz on Google Forms.

Based on the analysis Table 2, the research team selected eight emails, which cover both phishing and legitimate emails, to be included in the test. The team analysed each email and make sure that all question items covered the identified topics as described in the Phase I. The analysis was described in Table 3.

A brief explanation of each email is as follows.

1. Email presumed to have been sent by LinkAja (phishing email)
2. Email presumed to have been sent by JNE (phishing email)
3. Email presumed to have been sent by Eraclub (legitimate email)
4. Email presumed to have been sent by BCA (phishing email)
5. Email presumed to have been sent by IMF (phishing email)
6. Email presumed to have been sent by COVID-19 Committee (phishing email)
7. Email presumed to have been sent by Grab (legitimate email)
8. Email presumed to have been sent by Tokopedia (phishing email)

Developing questions that incorporated all of the identified characteristics of phishing emails is tough because the research team used real-life emails, admittedly with small alterations to suit the intended participants of test, which are the Indonesian SMEs owners.

The research team conducted the content validity test based on the initial draft. The expert panel consists of five people who meet predetermined criteria. Based on their assessment in the provided form, the team calculated the V-Aiken score as shown in the Table 4. Every test item has a high V-Aiken score, indicating good content validity, as the table illustrates.

p-ISSN:1411-6510
e-ISSN:2541-6111

Table 4. V-Aiken Calculation Result

Expert Reviewer	Question Item							
	1	2	3	4	5	6	7	8
A	5	5	4	5	5	5	4	5
B	5	4	5	4	4	5	5	4
C	5	4	4	5	5	5	4	5
D	5	5	5	5	5	5	5	5
E	5	5	4	5	4	5	5	5
Aiken	1.00	0.90	0.85	0.95	0.90	1.00	0.90	0.95

Findings – Phase III

The research team finalised the test by putting the pictures of selected emails in the Google Form. The detailed pictures of the eight emails and an explanation for each email were shown in the Appendix 1.

Findings – Phase IV

The research team delivered the test to 31 respondents which were SMEs' owner manager who use email to communicate and conduct business regularly.

The research team observed that the greatest score that respondents manage to earn in the test is 7, while the lowest score is 1. The scores obtained by the respondents are shown in Table 5. Respondents can be classified into four groups based on their test score: very high, high, low, and very low. Table 5 shows that the majority of respondents, 52.8% of the total respondents, can be classified into Very High category.

Table 5. The Scores of Test Takers in the Field Test

Test Score	Percentage of Respondents	Category
$X \geq 6$	52.8%	Very high
$4 \leq X < 6$	36.1%	High
$2 \leq X < 4$	8.3%	Low
$X < 2$	2.8%	Very low

Table 6. The Calculation of the KR-20

Subject	Question Item							
	1	2	3	4	5	6	7	8
p	0.94	0.23	0.26	0.84	0.94	0.65	0.78	0.61
KR-20	0.5054							

Findings – Phase V

The research team conducted reliability test based on data collected from Phase IV. The study performed the reliability test using the α-20 or KR-20 coefficient. The calculation result was shown in Table 6.

There are several ways to determine if a test has strong reliability or not. One commonly used guideline defines a test as having low reliability if the KR-20 is less than 0.50, medium reliability for score between 0.50 and 0.80, and high reliability for the KR-20 which is greater than 0.80 (Tan, 2009). The KR-20 of the test developed in this study yields a value of 0.5054, as shown in Table 6, indicating that the degree of reliability of this exam is barely reach the Medium level. The more reliable a test is, the more accurately the differences in results achieved by test takers represent different levels of skill intended by the tests. The questions in this test is a Yes/No question which only provides two possible option for each question. The test also only has eight questions. Hence, it may be possible that the test cannot generate adequate level of variance to assess individuals' skills reliably.

Table 7. Correct Answer Analysis for Each Question

Question Number	Percentage of Respondents who answer correctly
1	91.7%
2	25.0%
3	22.2%
4	83.3%
5	94.4%
6	66.7%
7	77.8%
8	61.1%

Considering that the KR-20 value is significantly affected by the number of items, it is necessary to consider increasing the number of item items to increase the reliability of the test. Another alternative is to increase the number of response options for each question, which will also fit the respondents' recommendation to avoid having too many questions in the test.

The research team also evaluate each question to find out how many respondents answer each question perfectly. This evaluation is helpful for two reasons. First, in order for the test to be reliable, the difficulty level of the questions must vary. Second, the team can determine what kinds of phishing or legitimate emails that may mislead the test takers. The result of analysis was shown in Table 7.

Two questions have a much lower percentage of respondents who answer correctly than other

questions, as shown in Table 7. Question 2 is a phishing email, although most respondents failed to identify it as such, whereas Question 3 is a legitimate email that most respondents mistook for a phishing email. The presence of images, colours, and logos tend to be more convincing to email recipients than plain text (Furnell, 2007), and Question 2 and 3 have images in the emails. However, it is important to note that most respondents believed Email 2 was legitimate, despite multiple strong indications of a phishing email. First, there are multiple typos that should not be in an official email issued by a major organisation. Second, the email includes an attached file with the .zip extension, which is a major warning indicator because .zip files are a kind of file we should only get from colleagues, friends, or associates, not from an email sent by an organisation without a close relationship with the recipients.

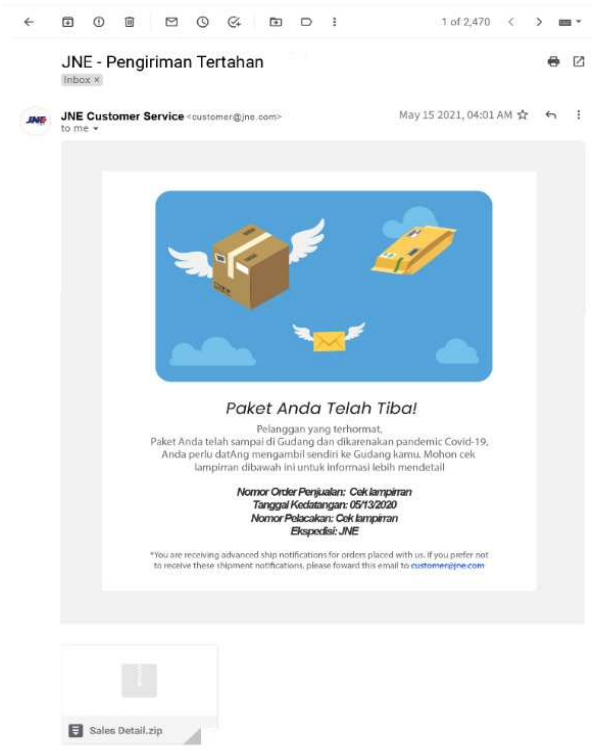


Figure 1. Email 2 – Phishing Email

Another interesting aspect is how Email 3 was identified by most respondents as phishing email, despite it is actually a legitimate email. Follow-up interviews with some SMEs owners found that SMEs owners have preference to trust urgent and relevant emails, where the emails are designed with proper logo and pictures, as supported by Furnell (2007). However, they are suspicious of emails with too many pictures and over-fancy wordings. Legitimate emails who have these features may be regarded as phishing email.

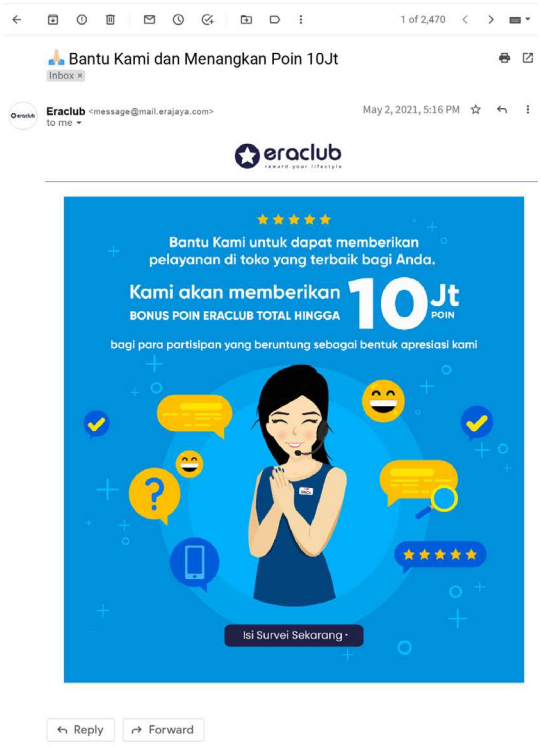


Figure 2. Email 3 – Legimate Email

CONCLUSION

SMEs owners needs to know the various ways to identify phishing messages so as not to become victims of phishing. Phishing emails can be identified based on several physical cues, and recipients can also increase vigilance when receiving an email that contains several influencing techniques. Several physical cues of phishing emails are original sender's email that does not match the topic discussed in the email, spelling and typos in emails supposedly sent by official institutions, and emails which talks about urgent matters, and emails that have files or hyperlink attached in it. Influencing technique does not provide obvious sign of phishing emails, but indicating that email recipients must be very careful when receiving email related to banking, credit cards, investment institutions, or other things that are considered important by the recipients.

This study developed a test of phishing susceptibility by collecting various real-life legitimate and phishing emails, and ask test takers to identify which emails are legitimate and which

p-ISSN:1411-6510
e-ISSN:2541-6111

emails are phishing. Based on the validity and reliability tests, the created instrument has high content validity for all question items but only reaches medium reliability. The test reliability can be improved by adding questions, or modify the question by having multiple-choice of answers for each question instead of Yes/No answer choices.

This study contributes to cybersecurity studies focusing on SMEs, particularly in Indonesia, by presenting preliminary findings on the characteristics of phishing emails that SMEs find difficult to identify. The test developed during this study can also be used as an instrument in future phishing studies in Indonesia.

REFERENCE

R. T. Wright, M. L. Jensen, J. B. Thatcher, M. Dinger, and K. Marett, "Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," *Information Systems Research*, vol. 25, no. 2, pp. 385–400, Jun. 2014, doi: 10.1287/isre.2014.0522. https://doi.org/10.1287/isre.2014.0522

M. L. Jensen, M. Dinger, R. T. Wright, and J. B. Thatcher, "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems*, vol. 34, no. 2, pp. 597–626, 2017, doi: 10.1080/07421222.2017.1334499.

S. Furnell, "Phishing: can we spot the signs?," *Computer Fraud & Security*, vol. 2007, no. 3, pp. 10–15, Mar. 2007, doi: 10.1016/S1361-3723(07)70035-0.

Symantec, *Internet security threat report*, vol. 21. 2016. doi: 10.1016/S1353-4858(05)00194-7. https://doi.org/10.1016/S1353-4858(05)00194-7

J. Wang, Y. Li, and H. R. Rao, "Coping responses in phishing detection: An investigation of antecedents and consequences," *Information Systems Research*, vol. 28, no. 2, pp. 378–396, 2017, doi: 10.1287/isre.2016.0680.

M. Falch, H. Olesen, K. E. Skouby, R. Tadayoni, and I. Williams, "Cybersecurity Strategies for SMEs in the Nordic Baltic Region," *JCSANDM*, Jan. 2023, doi: 10.13052/jcsm2245-1439.1161.

R. Yudhiyati, A. Putritama, and D. Rahmawati, "What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case," *Journal of Information, Communication and Ethics in Society*, 2021, doi: 10.1108/JICES-03-2021-0035.

D. Rahmawati, R. Yudhiyati, and A. Putritama, "How Micro and Small Enterprises Perceive Information Technology Fraud: A Study of Indonesian' Small Businesses," *5th International Conference on Computing Engineering and Design, ICCED 2019*, 2019, doi: 10.1109/ICCED46541.2019.9161104.

K. Renaud, "How smaller businesses struggle with security advice," *Computer Fraud and Security*, vol. 2016, no. 8, 2016, doi: 10.1016/S1361-3723(16)30062-8.

P. Burda, A. M. Altawekji, L. Allodi, and N. Zannone, "The Peculiar Case of Tailored Phishing against SMEs: Detection and Collective DefenseMechanisms at a Small IT Company," in *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Delft, Netherlands: IEEE, Jul. 2023, pp. 232–243. doi: 10.1109/EuroSPW59978.2023.00031.

J. A. Rodriguez-Corzo, A. E. Rojas, and C. Mejia-Moncayo, "Methodological model based on Gophish to face phishing vulnerabilities in SME," in *2018 ICAI Workshops (ICAIW)*, Bogota: IEEE, Nov. 2018, pp. 1–6. doi: 10.1109/ICAIW.2018.8555006.

Symantec, "Internet Security Threat Report (Vol.24) February 2019," 2019, [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1353485805001947

M. Wilson, S. McDonald, D. Button, and K. McGarry, "It Won't Happen to Me: Surveying SME Attitudes to Cyber-security," *Journal of Computer Information Systems*, vol. 63, no. 2, pp. 397–409, Mar. 2023, doi: 10.1080/08874417.2022.2067791.

A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Systems*, vol. 51, no. 3, pp. 576–586, 2011, doi: 10.1016/j.dss.2011.03.002.

L. D. Kimpe, M. Walrave, W. Hardyns, L. Pauwels, and K. Ponnet, "You' ve got mail! Explaining individual differences in becoming a phishing target," *Telematics and Informatics*, vol. 35, no. 5, pp. 1277–1287, 2018, doi: 10.1016/j.tele.2018.02.009.

O. A. Zielinska, R. Tembe, K. W. Hong, X. Ge, E. Murphy-Hill, and C. B. Mayhorn, "One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 58, no. 1, pp. 1466–

p-ISSN:1411-6510
e-ISSN:2541-6111

1470, Sep. 2014, doi: 10.1177/1541931214581306.

C. T. Berry and R. L. Berry, "An initial assessment of small business risk management approaches for cyber security threats," *International Journal of Business Continuity and Risk Management*, vol. 8, no. 1, pp. 1–10, 2018, doi: 10.1504/IJBCRM.2018.090580.

M. I. Khan, S. Tanwar, and A. Rana, "The Need for Information Security Management for SMEs," in *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, Moradabad, India: IEEE, Dec. 2020, pp. 328–332. doi: 10.1109/SMART50582.2020.9337108.

R. T. Wright and K. Marett, "The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived," *Journal of Management Information Systems*, vol. 27, no. 1, pp. 273–303, 2010, doi: 10.2753/MIS0742-1222270111.

M. Pears and S. Th. Konstantinidis, "Cybersecurity Training in the Healthcare Workforce – Utilization of the ADDIE Model," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, Vienna, Austria: IEEE, Apr. 2021, pp. 1674–1681. doi: 10.1109/EDUCON46332.2021.9454062.

S. Azwar, *Konstruksi Tes Kemampuan Kognitif*. Yogyakarta: Pustaka Belajar, 2019.

H. Retnawati, "PROVING CONTENT VALIDITY OF SELF-REGULATED LEARNING SCALE (THE COMPARISON OF AIKEN INDEX AND EXPANDED GREGORY INDEX)," *Research and Evaluation in Education*, vol. 2, no. 2, 2016. https://doi.org/10.21831/reid.v2i2.11029

Ş. TAN, "Misuses of KR-20 and Cronbach's Alpha Reliability Coefficients," *Education and Science*, vol. 34, no. 152, 2009. http://hdl.handle.net/11452/23105

Papathanasiou, A., Liontos, G., Katsouras, A., Liagkou, V., & Glavas, E. (2024). Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era. *Journal of Information Security*, *16*(1), 1-4 doi: 10.4236/jis.2025.161001.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, *50*, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2024). Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises. Technology in Society, 76, 102470. https://doi.org/10.1016/j.techsoc.2024.102470

Rawindaran, N. (2023). *Impact of cyber security awareness in small, medium enterprises (SMEs) in Wales* (Doctoral dissertation, Cardiff Metropolitan University). https://figshare.cardiffmet.ac.uk/ndownloader/files/41412072

Fagbule, O. (2023). Cyber security training in small to medium-sized enterprises (SMEs): Exploring organisation culture and employee training needs (Doctoral dissertation, Bournemouth University). https://eprints.bournemouth.ac.uk/39148/1/FAGBULE%2C%20Omolola_Ph.D._2022.pdf

Ascic, H. J. (2023). *Effectiveness of cybersecurity awareness training in lowering the risks of email-borne attacks for Irish SME* (Doctoral dissertation, Dublin, National College of Ireland). https://norma.ncirl.ie/id/eprint/7112

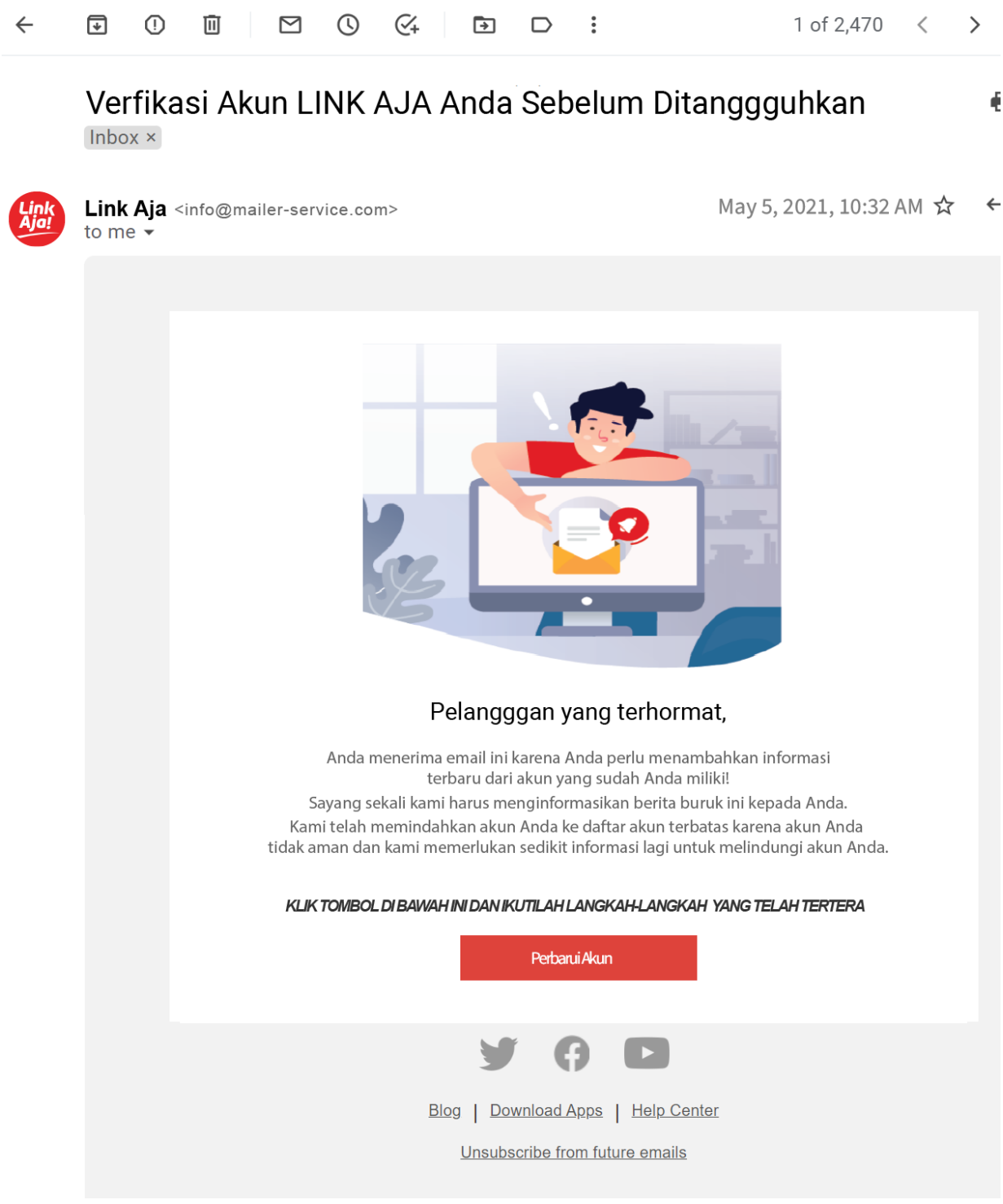
Ansar, N., Parveen, S., Alankar, B., & Khan, I. R. (2024, March). Cost-Effective Cybersecurity Framework for Small and Medium-Sized Enterprises. In *International Conference on Deep Learning and Visual Artificial Intelligence* (pp. 133-155). Singapore: Springer Nature Singapore. https://doi.org/10.1287/isre.2014.0522

p-ISSN:1411-6510
e-ISSN :2541-6111

Appendix

Appendix 1. The Emails Included in the Test

Email 1



p-ISSN:1411-6510
e-ISSN:2541-6111

Email 2

1 of 2,470

JNE - Pengiriman Tertahan

Inbox ×

JNE Customer Service <customer@jne.com>
to me

May 15 2021, 04:01 AM

Paket Anda Telah Tiba!

Pelanggan yang terhormat,
Paket Anda telah sampai di Gudang dan dikarenakan pandemic Covid-19, Anda perlu datAng mengambil sendiri ke Gudang kamu. Mohon cek lampirran dibawah ini untuk informasi lebih mendetail

Nomor Order Penjualan: Cek lampirran
Tanggal Kedatangan: 05/13/2020
Nomor Pelacakan: Cek lampirran
Ekspedisi: JNE

*You are receiving advanced ship notifications for orders placed with us. If you prefer not to receive these shipment notifications, please foward this email to customer@jne.com

Sales Detail.zip

p-ISSN:1411-6510
e-ISSN:2541-6111

Email 3

1 of 2,470

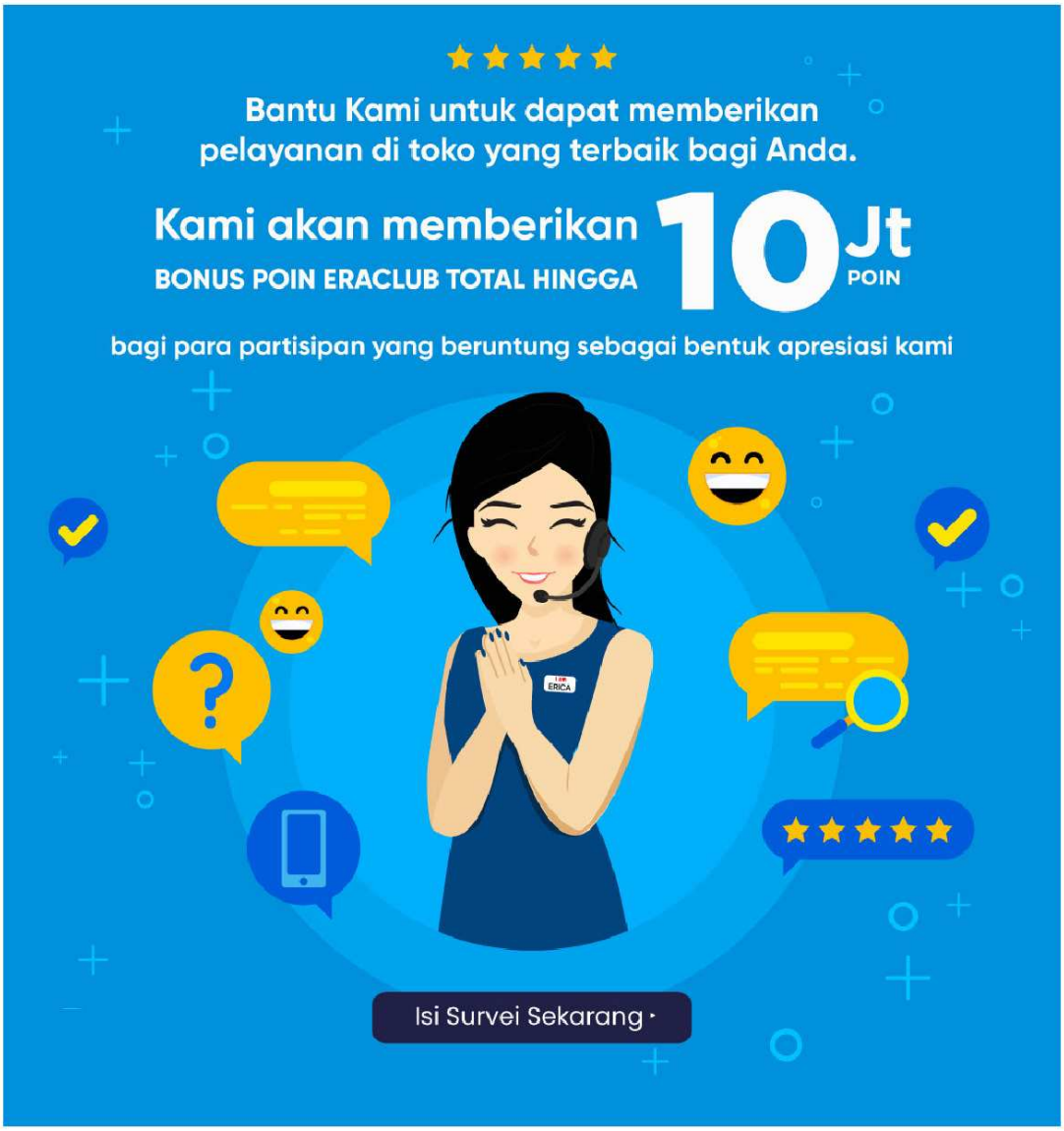
🙏 Bantu Kami dan Menangkan Poin 10Jt

Inbox ×

Eraclub <message@mail.erajaya.com>
to me

May 2, 2021, 5:16 PM

eraclub
reward your lifestyle



Reply Forward

Email 4

1 of 2,470

Deactivation Confirmation : Your BCA Credit Card Is Blocked

Inbox ×

Kartu Kredit BCA <KartuKreditBCA@vicodep.org>
to me

April 15, 2021, 4:01 PM

Kartu Kredit BCA

Yth. Pemegang Kartu Kredit BCA

KARTU KREDIT ANDA TELAH DINONAKTIFKAN KARENA ALASAN SEBAGAI BERIKUT.

* EMAIL BELUM DIVERIFIKASI
* ALAMAT TAGIHAN YANG TIDAK VALID
* NOMOR PIN YANG TIDAK TEPAT

Anda tidak dapat melakukan Pengiriman Dana dan Pembayaran dengan kartu Anda sebelum ada memperbarui informasi melaui jalur aman kami pada link berikut
CLICK HERE TO REACTIVATE YOUR CARD
Dalam jangka waktu 48 jam sejak Anda menerima pesan ini.

Hapus dan biarkan pesan ini jika Anda berniat untuk menghapus kartu Anda secara permanen.

Hubungi kami melalui link berikut.

BCA

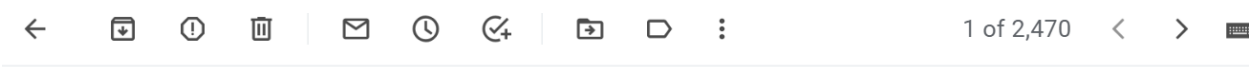
BCA terdaftar dan diawasi oleh Otoritas Jasa Keuangan
BCA merupakan peserta penjaminan LPS
Halo BCA 1500888
www.bca.co.id | halobca@bca.co.id

BCA tidak pernah memberi kuasa pihak manapun untuk mengambil Kartu Kredit BCA Anda.
Segera hubungi Halo BCA 1500888 apabila Anda mengalami Penipuan tersebut.

E-info ini adalah fasilitas bagi Pemegang Kartu Kredit BCA
Semua Informasi dan data yang terdapat dalam e-Info adalah bersifat pribadi dan rahasia. Semua konsekuensi dari penyalahgunaan informasi dan data yang terdapat dalam e-Info sebagai akibat dari kelalaian Pemegang Kartu akan menjadi tanggung jawab penuh dari Pemegang Kartu. Dengan ini, Pemegang Kartu Kredit BCA melepaskan PT Bank Central Asia, Tbk. dari segala bentuk tuduhan dan tuntutan hukum yang diajukan oleh pihak manapun dalam hal penyalahgunaan informasi dan data yang terdapat dalam e-Info.

p-ISSN:1411-6510
e-ISSN:2541-6111

Email 5



Penerima yang terhormat!

Inbox ×

Mrs. Kristalina Georgieva <bopo5886@gmail.com> May 6, 2021 18:26 PM
to me

Penerima yang terhormat!

Nama saya Nyonya Kristalina Georgieva, Ketua IMF. Anda meninggalkan Satu Juta lima ratus ribu dolar Amerika Serikat Anda dengan UNITED BANK FOR AFRICA. Apa alasannya, siapa yang mencoba menipu Anda? karena ini adalah satu-satunya bank resmi dengan Tuan Segun Agbaje sebagai agen yang Disetujui.

Jika Anda menolak untuk menghubungi Tn. Segun Agbaje, IMF tidak akan mengizinkan Anda menerima pembayaran dan Anda akan terus bekerja dengan orang yang salah sepanjang hidup Anda tanpa kabar baik. Uang Anda masih ada di United bank for Africa di Togo dan Anda harus menghubungi Tn. Segun Agbaje jika Anda peduli dengan tanda tangan dan persetujuan IMF.

Agen Resmi: Mr Segun Agbaje
Nama bank: United Bank for Africa
email: ubagrouptg02@gmail.com
telp: +22870496864

Ini adalah bank yang disetujui dari Perserikatan Bangsa-Bangsa, IMF, bank dunia dan ECOWAS dan tanpa bank yang disebutkan ini tidak ada dari semua agen ini yang akan mendukung Anda atau menyetujui pembayaran untuk Anda.
silakan hubungi bank sekarang dan terima dana Anda dari mereka tanpa penundaan.

Ini adalah bank yang disetujui dari Perserikatan Bangsa-Bangsa, IMF, bank dunia dan ECOWAS dan tanpa bank yang disebutkan ini tidak ada dari semua agen ini yang akan mendukung Anda atau menyetujui pembayaran untuk Anda.
silakan hubungi bank sekarang dan terima dana Anda dari mereka tanpa penundaan.

Hormat kami
Kristalina Georgieva
Ketua IMF.

Email 6

1 of 2,470

[WARNING: MESSAGE ENCRYPTED][WARNING: MESSAGE ENCRYPTED] Informasi Vaksinasi COVID-19

Inbox ×

Komite Penanganan COVID-19 <kpcpen@yahoo.co. Inbox × June 25, 2021, 10:32 AM

to me

Email ini berisi informasi penting terkait hasil penelitian terbaru dari KPCPEN terkait vaksin untuk COVID-19

Statistik dari Komite Penanganan COVID-19 dan Pemulihan Ekonomi Nasional (KPCPEN) terkait dengan kasus serius dan gejala setelah vaksinasi (lebih lengkap tercantum di file terlampir), kami belum mempelajari secara menyeluruh tentang bahaya vaksin ini. Banyaknya opsi vaksin yang tersedia menciptakan ilusi terkait keamanan vaksin dan persepsi bahwa kita memiliki opsi untuk memilih.

Penelitian menunjukkan kemungkinan terinveksi COVID-19 meningkat secara signifikan setelah vaksinasi, dan juga menciptakan komplikasi seperti masalah kesuburan, kemungkinan munculnya penyakit terkait paru-paru, sistem syaraf pusat, dan bahkan kebutaan

Beberapa negara bahkan telah memvaksinasi terpidana seumur hidup dan hukuman mati di belakang layar. Telah muncul juga peningkatan drastis COVID-19 dan kematian di daerah dimana dilakukan vaksinasi masal. Anda dapat menghindari risiko terinfeksi melalui vaksin yang belum teruji.

KPCPEN telah mengompilasi data lengkap terkait kontraindikasi, peluang kematian, dan komplikasi dari penggunaan berbagai vaksin yang ada di Indonesia (baik Astrazeneca dan Sinovac) dan negara lain, serta harga yang harus dibayar oleh masyarakat. Ketahuilah situasi dimana vaksin tertentu tidak dapat Anda gunakan, serta vaksin yang menghasilkan kontraindikasi untuk anak-anak, ibu hamil, warga lanjut usia, individu dengan komorbid dan alergi. Informasi ini valid per Mei 2021.

Anda terpilih untuk memperoleh akses ke data ini berkat kepatuhan Anda dalam melaporkan sejarah perjalanan dan kasus COVID-19 di lingkungan Anda. Password untuk mengakses data ini: **aDb2021xT**

Bantu KPCPEN untuk terus memperbarui data implikasi vaksin COVID-19 melalui Link berikut.

Document.xlsm
79 KB

p-ISSN:1411-6510
e-ISSN:2541-6111

Email 7

1 of 2,470

Mau makan yang enak tapi tetap hemat?

Inbox ×

Grab Indonesia <no-replay@grab.com>
to me

19 Mei 2021

Banyak menu yang siap dipilih untukmu

Hai [redacted], sepertinya sudah lama ya aku nggak antar pesanan untuk kamu. Tahu ngga sejak itu aku sudah banyak berubah?

Sekarang kamu bisa mencari makanan atau minuman dari berjuta pilihan menu yang tersedia, ada juga berbagai kategori menu yang bisa kamu pilih kalau lagi ngga ada ide. Dan jangan lewatkan berbagai penawaran menarik dari restoran pilihan di kotamu ya.

PESAN SEKARANG →

p-ISSN:1411-6510
e-ISSN:2541-6111

Email 8

1 of 2,470

Kupon Spesial di Hari Senin. Save up to 50%!

Inbox ×

Tokopedia <Not Found>
to me

9 June 2021

HAI **TOPPERS,**

Sebagai ucapan terima kasih karena telah menjadi pelanggan setia Tokopedia, kami memberikan TokoPoint sebesar Rp900.000 untuk semua pelanggan Tokopedia yang beruntung.

TokoPoint Anda akan ditambahkan secara otomatis ke akun Anda dan hanya dapat digunakan untuk CYBER MONDAY SALE!
Klik Link berikut untuk melihat promonya.

SAVE UP TO 50%!

12-13 Juli 2021

Get your Cyber Monday coupon.

2009-2021, PT Tokopedia