User Awareness Design for Electronic Money User Using Protection Motivation Theory and NIST 800-50 Framework

Christian Andrean Pradigdya[1] and Raden Venantius Hari Ginardi[1]

Abstract*—Electronic money has emerged as the payment method. It becomes more popular because it is convenient and ubiquitous. However, the popularity has caused new security threats for the the user of electronic money. Personal data and financial information are the main target of the threats. Individuals need to protect and have certain responsibilities regarding their personal data and financial information used for electronic money services. Technology alone is unable to prevent the threats. Human behavior also becomes crucial factor to protect people against the threats and plays essential role in safe guarding personal data and financial information. This study uses Protection Motivation Theory (PMT) as a theoretical framework to empirically test why people do precautionary behavior on electronic money transaction. PMT is a social-cognitive model to predict and explain prevention behavior. Empirical research is conducted using survey methodology and collecting data from 186 respondents using online forms. Partial Least Square structural equation modelling provides support for factors influencing protection motivation in electronic money context. The results provide support for the use of threat and coping appraisal, in particular perceived security vulnerabilities, perceived security threat and perceived response efficacy to influence precautionary behavior in the context of electronic money. Those results contributes to the design of user awareness programs using NIST Special Publication 800-50. The awareness programs aimed at precaution behavior, thereby empowering electronic money user to protect themselves.

***Keywords*—Electronic Money, Information Security, NIST 800-50, Partial Least Square, Protection motivation Theory.**

I. INTRODUCTION

Bank Indonesia has reported that, throughout 2018, transactions using electronic money showed a very significant increase. The transactions recorded have reached more than IDR 3,8 trillion. The increasing popularity of transactions with electronic money cannot be separated from the role of technology that is considered as easy and inexpensive to access. Technology is the main axis in electronic money transactions and covers all aspects of electronic money including information security and privacy. Technology that supports information security and data privacy is required to constantly change and adapt as the security risk is also evolving. Technological sophistication must also be followed by the ability of users to use technology as both are deemed as complementary factors. A user's careless actions and attitudes are a weak point in the information security. Hence, the users must continue to realize in the form of awareness and behavior. They must also be sensitive to threats when dealing with electronic money. The biggest threat in the electronic money system is balance theft, account hijacking and identity theft.

The theory of protection motivation is a process of threat assessment and a response assessment process that results in an intention to implement an adaptive (protective motivation) or maladaptive response (placing at risk). It functions to develop interventions to reduce threats to individuals by integrating psychological, sociological and other related fields of concepts. The theory of motivation is a social-cognitive model that predicts behavior [1].

The aim of the present study is to obtain the factors that influence users of electronic money to take preventive measures to protect themselves from threats based on the theory of protection motivation. This study develops a research model then tests it using the Partial Least Square method. The PLS approach is more suitable because this approach assumes that all measures of variance are useful variances to be explained. The results are then used to develop a program in the form of user awareness to increase the awareness and skills of users in using electronic money.

II. METHOD

A. Electronic Money

Bank Indonesia Regulation number 20/6/PBI/2018 defines electronic money as a payment instrument that fulfills certain elements. These elements include the value of money deposited in advance to the publisher, the value of money stored electronically in a media server or chip and the value of electronic money managed by the publisher is not a deposit as referred to in the Act governing banking [2].

[1]Christian Andrean Pradigdya and Raden Venantius Hari Ginardi are with Departement of Business and Management Technology, Institut Teknologi Sepuluh Nopember, Indonesia. Email: Andrean.17092@mhs.its.ac.id; hariginardi@gmail.com

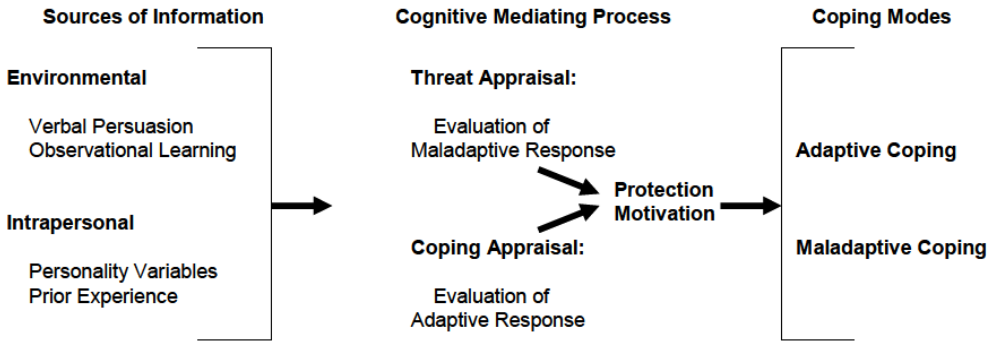

Figure 1. Protection Motivation Theory

B. Protection Motivation Theory (PMT)

The premise of PMT is a received information (sources of information), then the individual who receives it will assess the information (cognitive mediating process), and ultimately the individual takes action on the information received (coping mode). Sources of information are input variables on models that are accompanied by environmental conditions and interpersonal sources. Environmental sources of information include verbal persuasion and observational learning whereas interpersonal sources deal with the personal aspects of feedback from previous experience, including the experience that is associated to conduct a behavior that is in demand.

There are two cognitive processes that become process mediation which are threat appraisal process and coping appraisal process. The threat appraisal process consists of perceptions of severity and vulnerability of maladaptive actions. The threat appraisal process is an assessment of the security threats that occur. On the other hand, the coping appraisal process consists of individual confidence in the response to resolution that will reduce or alleviate the security threat (response efficacy) and the individual believes that the response can be done (self efficacy), only if the response does not require too high preventive costs. The expected result of the cognitive mediation process is the decision to apply an adaptive and applicable response. There are two types of adaptive behavior, namely adaptive behavior (to protect themselves) and maladaptive (not self-protecting) [1]. Figure 1 elaborates the process.

C. Partial Least Square

Partial Least Square (PLS) was first developed by Herman Wold in 1982. There are several methods developed related to PLS, for instance PLS Regression (PLS-R) and PLS Path Modeling (PLS-PM) models. PLS Path Modeling was developed as an alternative to structural equation modeling (SEM) with a weak theoretical basis. While PLS-PM is variant-based, the SEM method uses a covariant base. The difference of PLS analysis from the SEM analysis model is that the data on PLS do not have to be normally distributed, can use small samples, can be used as confirmation of theory, can be used to explain the presence or absence of relationships between latent variables. PLS can analyze the constructs formed along with reflective and formative indicators at once or be combined between the two. Moreover, PLS is able to estimate large and complex models with hundreds of latent variables and thousands of indicators. The model evaluation in PLS consists of two stages, namely the outer model evaluation or the model of measurement and inner model evaluation or structural models.

D. NIST Special Publication 800-50

NIST Special Publication 800-50, Building An Information Technology Security Awareness and Training Program, provides guidance for building an effective information technology (IT) security program. The document identifies the four critical steps in the life cycle of an IT security awareness and training program, awareness and training program design, awareness and training material development, program implementation, and post-implementation. Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information. Awareness relies on reaching broad audiences with attractive packaging techniques [3].

III. METHODOLOGY

A. Survey Questionnaire Design and Procedure

The data collection was conducted by generating questionnaires in the Google Forms platform. The questionnaires consist of 7 parts, namely the respondents' demographic questions and validation questions, such as "Have you ever made transactions using electronic money?" to ensure the respondents have used electronic money. The subsequent sections are threat appraisal information, respondent threat appraisal statements, coping appraisal information, respondent threat appraisal statements, and precautionary behavior statements

answered by respondents. The advantage of using the Google Forms Application is the arrangement to force the respondents to answer all questions before proceeding to the next section, which is required to avoid any missing value. For all independent variables and the dependent variables are measured by using the Likert Scale (5 points) with the following details:

a. Strongly disagree is given a score of 1
b. Disagree by a score of 2
c. Neutral is given a score of 3
d. Agree by a score of 4
e. Strongly agree is given a score of 1

The main target of consumers is electronic money users. The target number of respondents was 170 people obtained by counting the number of research indicators (17) multiplied by 10. The respondents were obtained by administering the links to the Google Forms questionnaire through chain messages and social media. Variables are presented in Table 1.

TABLE 1.
PMT CONSTRUCT DEFINITON

PMT construct	Definitions
Threat Appraisal	Individual assessment of the threats level that occur during transaction with electronic money.
Coping Appraisal	Individual assessment of confidence and ability to take preventive measures that are believed to be successful with minimum effort
Perceived Security Vulnerability	Perception of the assessment towards the possibility of a security threat to electronic money transactions
Perceived Security Threat	Perception of the assessment of the impact or loss as a result of the security threat of electronic money transactions
Perceived Security Self Efficacy	Perception of an individual's confidence in his ability to make a response or recommended preventive action
Perceived Response Efficacy	Perception of individual confidence in the effectiveness of a response or action to prevent the security threat of electronic money transactions
Perceived Prevention Cost	An individual's perception of the costs, time and effort that must be made to take the recommended precautions to prevent or reduce the impact of security threats on electronic money transactions

Partial-least-squares path-modelling (PLS) was used for data analysis using Smart PLS 3. The exploratory nature of PLS is the reason PLS is chosen. Thus this study is focusing on the predictive application.

B. User Awareness Design

User awareness will be created using the NIST 500-80 framework [3] by following 4 main steps. These steps include awareness program design, awareness material development, implementation program, and post implementation. These steps need to be carried out to create a clear structured user awareness. However, not all existing measures will be followed because this framework also includes training programs for company organizations. Therefore, the steps of each stage of the NIST 500-80 framework that will be employed to design user awareness are as follows:

1) Awarenesss Program Design

This stage provides points that can assess needs and design user awareness.

1. Existing: a form of user awareness that currently exists
2. Scope of the awareness: the scope of user awareness to be taken from each hypothesis received.
3. Goals to be accomplished: goals to be achieved by adjusting the objectives of the accepted hypothesis.
4. Target audience: to whom user awareness is addressed, in this matter regarding age.
5. Mandatory: designing user awareness as an obligation
6. Topics to be addressed: delivered in accordance with the topic related to each accepted hypothesis.
7. Frequency: the number of user awareness delivery cycles at one time.

2) Developing Awareness Material

This stage will help form a supporting material with the aim that the target users have the ability to carry out the desired protective behavior. The selection of supporting material must also be specific, personal, interesting and up to date; hence, it does not become a mere formality.

1. Selecting awareness: choosing specific topics from each hypothesis that is accepted
2. Source of awareness material: inclusion of relevant scientific references

3) Implementing the Awareness Program

The next stage is implementation which provides input for media delivery of user awareness.

1. techniques for delivering awareness material: is a technique for choosing media delivery of material that depends on the complexity of the message

4) Post Implementation

The next stage is evaluation. This stage explains and generates input suggestions regarding what methods can be used.

1. evaluation feedback and success indicator: selecting the techniques to evaluate and determine indicators of success.

IV. RESULTS AND DISCUSSION

A. Measurement Model

Measurement model or outer model is conducted to measure the association between indicators with latent variables. It is completed by conducting a validity test and reliability test.

1) Validity Test

Validity test is carried out by testing convergent validity and discriminant validity. The assessment is selected due to the indicator research model is reflective (the indicator is caused by the construct). Convergent validity is tested by looking at the loading factor and average variance extracted while discriminant validity was tested using cross

loading. Following are the respective criteria that must be met:

1. Loading factor >0.7
2. Average variance extracted >0.5
3. Cross loading the indicator itself > the other indicators

Table 2 is the final results of loading factor. PST 1 was removed because it did not meet the criteria. Table 3 and Table 4 is the final results of AVE and Cross loading.

2) Reliability Test

An indicator is declared reliable if the answer given by the respondent is consistent and produces a consistent answer if used in a different sample. The level of consistency of the data towards the research indicators is obtained through reliability assessment. An outer model can be considered reliable if the composite reliability and cronbach's alpha values are greater than 0.6. Table 6 is the results of reliability test

B. Structural Model

The structural model or inner model is a model that links between latent variables. Evaluation of structural models can predict the causal relationship between latent variables. To assess structural models in Smart PLS, it is necessary to do bootsrapping by taking a subsample of 5000 to assess the significance of path coefficients with a test type of two tailed. Afterwards, it reveals the value of coefficient of determination (R^2) for the dependent variable and the path coefficient value for the independent variable. The significance value is then assessed based on the value t-statistics for each path. Figure 2 is the summary of the results.

TABLE 2.
OUTER LOADINGS RESULTS

	PPC	PRE	PSE	PST	PSV	Precautionary Behavior	Notes
PB1						0.808	Valid
PB2						0.921	Valid
PB3						0.894	Valid
PPC1	0.725						Valid
PPC2	0.727						Valid
PPC3	0.93						Valid
PRE1		0.796					Valid
PRE2		0.903					Valid
PRE3		0.872					Valid
PSE1			0.753				Valid
PSE2			0.765				Valid
PSE3			0.835				Valid
PST2				0.893			Valid
PST3				0.914			Valid
PSV1					0.877		Valid
PSV2					0.858		Valid

TABLE 3.
AVE RESULTS

	AVE	Notes
PPC	0.64	Valid
PRE	0.737	Valid
PSE	0.617	Valid
PST	0.817	Valid
PSV	0.753	Valid
Precautionary Behavior	0.767	Valid

TABLE 4.
CROSS LOADINGS RESULTS

	PPC	PRE	PSE	PST	PSV	Precautionary Behavior	Notes
PB1	0.044	0.34	0.178	0.248	0.142	0.808	Valid
PB2	0.103	0.411	0.236	0.246	0.169	0.921	Valid
PB3	0.108	0.488	0.333	0.381	0.206	0.894	Valid
PPC1	0.725	0.105	0.206	-0.024	0.03	0.056	Valid
PPC2	0.727	-0.038	0.017	0.051	0.191	0.022	Valid
PPC3	0.93	0.008	0.103	0.025	0.202	0.112	Valid
PRE1	0.123	0.796	0.559	0.115	0.063	0.327	Valid
PRE2	0.049	0.903	0.53	0.254	-0.053	0.459	Valid
PRE3	-0.053	0.872	0.453	0.278	-0.001	0.435	Valid
PSE1	0.033	0.448	0.753	0.104	-0.053	0.183	Valid
PSE2	0.042	0.427	0.765	0.138	0.003	0.159	Valid

PSE3	0.205	0.505	0.835	0.12	0.029	0.304	Valid
PST2	-0.001	0.196	0.136	0.893	0.168	0.293	Valid
PST3	0.028	0.272	0.136	0.914	0.125	0.325	Valid
PSV1	0.172	0.004	0.003	0.116	0.877	0.18	Valid
PSV2	0.135	-0.011	-0.004	0.164	0.858	0.168	Valid

TABLE 5.
RELIABILITY TEST RESULTS

	Composite Reliability	Cronbach's Alpha
PPC	0.84	0.761
PRE	0.893	0.822
PSE	0.828	0.714
PST	0.899	0.776
PSV	0.859	0.672
Precautionary Behavior	0.908	0.85

TABLE 6.
HYPOTESIS TEST RESULTS

	Hypotesis	PATH	Path Coefficients	T Statistics (|O/STDEV|)	P Values	Notes
H1	Perceived Security Vulnerability positively influences precautionary behavior	PSV -> Precautionary Behavior	0.16	2.207	0.027	Accepted
H2	Perceived Security Threat positively influences precautionary behavior	PST -> Precautionary Behavior	0.205	3.367	0.001	Accepted
H3	Perceived Security Self Efficacy positively influences precautionary behavior	PSE -> Precautionary Behavior	0.008	0.086	0.932	Rejected
H4	Perceived Security Response Efficacy positively influences precautionary behavior	PRE -> Precautionary Behavior	0.421	4.767	0	Accepted
H5	Perceived Prevention Cost negatively influences precautionary behavior	PPC -> Precautionary Behavior	0.052	0.61	0.542	Rejected

The value of R square (R^2) is used to measure the level of variation in changes in the independent variable on the dependent variable. The higher the value of R2, the better the prediction model tested will be. In this study, the value of R2 or determination coefficient is deemed as moderate with a value of 0.312.

C. Hypotesis Tessting

Hypothesis testing is carried out by looking at the value of t-statistics and significance level or also the value of the probability p-value. The expected t-statistics value must be greater than 1.96 with a significance level = 5%. Whereas, the probability value of p-value with alpha 5% (0.05) is less than 0.05. Therefore, the acceptance criteria for the hypothesis are when t-statistics > t-table (1.96) and p-value less than alpha 5% (0.05). Table 6 presents the results of the Smart PLS 3 hypothesis testing, where there are 3 accepted hypotheses, namely, PSV, PST, PRE and 2 rejected hypotheses which are PSE and PPC.

D. User Awareness Design

The current study designed user awareness by using the NIST 800-50 framework [3] and emphasizing messages on influencing factors why a user performs a precautionary behavior. Designing user a wareness is arranged by employing the stages of the NIST 800-50 framework. Results this research is expected to be used by publishers of electronic money to arrange user awareness of information security for electronic money users.

1) Awarenesss Program Design

a. Existing

Existing is a form of user awareness that has been created by the publisher of electronic money. Figures 3 describe examples of user awareness that OVO and GoPay have generated. User awareness created by OVO in Figure describes 2 security steps and usage tips.

b. Scope of the awareness

Scope of awareness is based on protection motivation theory. The protection motivation theory approach as a

basis for making user awareness has been exemplified previously [4]. Scope of the awareness of this study was perceived security vulnerabilities, perceived security threat, and perceived response efficacy. The scope of perceived security vulnerabilities is how electronic money crimes can be used to assess vulnerability. The scope of perceived security threat is to explain the impact of electronic money crimes. The scope of perceived response efficacy is the success of the precautionary behavior to run electronic money security guidelines.

c. Goals to be accomplished

Goals to be accomplished must be able to answer the scope of awareness that is tailored to each hypothesis that is accepted. The purpose of perceived security vulnerabilities is to explain how the crime of electronic money reinforces the message of vulnerability; thus, the users have a perception of vulnerability by assessing how vulnerable themselves when encountered a threat. The purpose of perceived security threats is to convey the crime impact message of electronic money so that users have the perception of severity. The purpose of perceived response efficacy is to emphasize the message of the success of the precautionary behavior, namely the security guide. The message helps users have the perception that running a security guideline will protect themselves from electronic money crimes.

d. Target audience

The target audience of user awareness is electronic money users. Demographic data of this study indicate that most samples were aged 19-37 years which is 90% of the total sample. Age classification according to Brosdahl and Carpenter [5] is Gen Y or The Millennials born between 1982-2000 that have the age range of 19-37 years old in 2019. Generation Y has its own characteristics in receiving and processing information. Bolton, et all [6] states that generation Y is a generation born where technology is already in its environment (digital natives). In other words, generation Y is not a generation born where technology has not been developed (digital imigrants). Electronic money publishers in creating user awareness need to make adjustments to how user awareness is delivered and understood to meet the target audience. This is because the issue of information security is regarding human beings compared to technical matters.

Other demographic data from this study indicate that 58% of the sample (108 people) from the population have more than 3-year experience of using electronic money and 42% (78 people) under 3 years of experience. Implicitly, this shows that there has been an increase in the number of users in the last 2 years. This elevation indicates the presence of new users or novice users. Beginner users with an account period below 3 years can also be used as the main target audience. This needs to be done because according to reports from the European Payment Council [7], the main target of information security criminals is novice users.

e. Mandatory

Mandatory is a policy to design user awareness as an obligation. Seeing the current conditions, there has been no mandatory user awareness issued by electronic money publisher. User awareness is not mandatory to be seen, as OVO, users have the choice to comprehend user awareness further or ignore it. This is certainly not effective. It is recommended that user awareness to be mandatory but still delivered appropriately and fairly. This is to avoid users being exposed to privacy fatigue. If it is mandatory, the frequency of implementation is every 6 months or once a year. Implementation can be best done in certain moments, for instance, security month awareness. While the nature of routine can be in the form of a pop up message or also by using a newsletter.

f. Topics to be addressed

The topics to be addressed are delivered in accordance with each accepted hypothesis. The topic of perceived security vulnerabilities explains how electronic crime is committed. The topic of perceived security threat explains the impact of being a victim of electronic money crimes. Topics of perceived response efficacy explain security guidelines can protect users from electronic money crimes

g. Frequency

Frequency is the number of cycles of user awareness delivered at a given time. User awareness has a sustainable nature which means it must be done continuously. However, it should be noted that the frequency of user awareness is given to users of electronic money. Users can easily feel tired of the security procedures and processes inside. Security procedures and user awareness delivered continuously can give rise to perceptions if carrying out security procedures is a burden [8]. Excessive frequency makes user awareness waste information and causes users to be apathetic because it is constantly being conveyed. However, on the other hand, the rare frequency of delivery will result in ineffective user awareness. Distance when sending user awareness that is too far away will make the user easy to forget. In addition, choosing the right time also needs to be a concern and consideration.

2) Developing Awareness Material

a. Selecting awareness

The process of selecting specific topics is useful to arouse users to feel connected to the problem. The topic of specific perceived security vulnerabilities is social engineering and malware. The selection of social engineering and mobile malware is based on reports published by the European Payments Council entitled 2018 Payment Threats And Fraud Trends Report [7]. The European Payments Council asserted that the threat of information security through social engineering and malware still contributes greatly to a number of losses, even more significant.

Social engineering is a non-technical infiltration method that is used to trick users into submitting credential information from devices or systems that they have or even

infect malware. Social engineering can be utilized through various media such as e-mail, short messages, telephone calls, and social media. The perpetrator use social engineering because it is easier to exploit natural human tendencies to trust compared to finding a software vulnerability.

Examples of common social engineering attacks are email phishing, social media, and short messages and vishing (voice and phishing) through direct telephone calls. The general scenario of phishing is carried out by sending email and pretending to be an official/electronic money publisher. The perpetrator then ask the victim to verify the information by clicking the link that contains the user information form. If the victim is not careful and completes the form on the link, the perpetrator will get the user's personal information. A similar mode is a message stating that the recipient of the email is the winner of the quiz or lottery and must verify the data by clicking on a link. Vishing generally also uses the same mode as phishing but with telephone media. Perpetrators disguised themselves as official parties asking users to provide OTP codes sent by short message. In general, the OTP code is sent to the user by the system when trying to enter an electronic money application account or change the electronic money account PIN.

Malware or malicious software is a term used for software that infiltrates an operating system or software. Perpetrators design malware to damage certain functions of a device, cut security access controls and steal data and send it without being known to the device owner. Mobile malware is malware that attacks devices such as smartphones. Mobile malware is usually infiltrated on a link that is automatically downloaded if clicked on by the user.

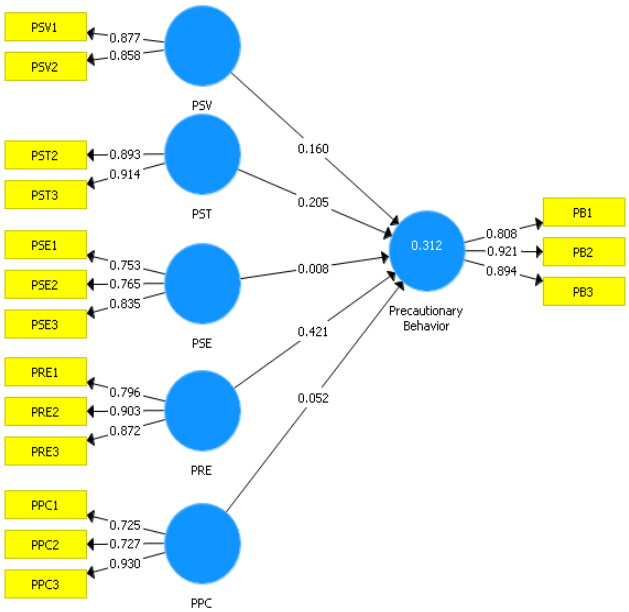

Figure 2. Final Structured Model.

Figure 3. Existing User Awareness by OVO.

A report from China [9] indicates that mobile malware is infiltrated on the QR Code, when users scan the QR Code then it also automatically downloads the mobile malware which then infects the user's smartphone. Topics related to the impact of electronic money crime have not been studied and reported empirically apart from the large number of cases and due to the reluctance of victims to report. The closest report is the note of the Institute for Community Research and Advocacy (ELSAM) in 2017. ELSAM reported 33 cases of misuse of personal data from 2013 to 2017 [10]. However, that does not mean that the possibility of a crime of electronic money is small and can be ignored.

The topic of perceived security threat discussed is the impact encountered by a victim of electronic money crime. In general, there are two main losses received by users of electronic money. Both of these impacts related to electronic money accounts, user data and personal information.

The aim of the crime of phishing is to obtain a login information. Information in the form of login information

is used by the perpetrator to fully take over the victim's electronic money account in a way to change e-mail and password for the e-money account. The victim will automatically lose their accounts and their balances as well as information inside.

Smartphones generally have user data and personal information. Smartphones infected with mobile malware can unknowingly send data and personal information of users via the internet. The user's personal data and information can be sold to third parties to commit crime. In addition, banking credential information that might exist on smartphones is also threatened by confidentiality.

The topic of perceived response efficacy is the explanation of the success of electronic money security guidelines that prevent users from becoming victims of electronic money crimes. Perceived response efficacy is the user's perception of response assessment (coping appraisal), how the suggested behavior can successfully prevent users from the threat of electronic money crime. Therefore, the topic of discussion is ways that users can use to protect themselves from electronic money crimes. The topic of the discussion must emphasize the message of success so that the user can trust it influences the users to do the precautionary behavior. Report of the European Payments Council, 2018 Payment Threats And Fraud Trends Report provides an example of the topic of security guidelines [7].

The security of smart phones is the main key to protection because it is a media that plays the role of a wallet for electronic money. The security of a smart phone can be done by locking a smart phone with a number, pattern or fingerprint password so that no one can use the smart phone. Another thing that can be done is to always update the electronic money and antivirus applications to get the latest security patches.

Login information is the information that the user uses to enter in his account. Login electronic money information in the form of a telephone number, e- mail address (e-mail), password (PIN), and OTP code may not be notified to anyone including electronic money publisher.

b. Source of awareness material

Source of awareness material or inclusion of relevant additional references. There are many material security awareness sources that can be linked to user awareness programs. Supporting material must be able to support the explanation of specific issues and provide guidelines for preparing user awareness. Supporting material can also be taken from information security sites such as [11], [12]. The two sites are providing material, infographics and guidelines for promoting information security awareness. Both sites are managed by the National Cyber Security Alliance and the US Department of Justice. Additional references can be added to the results of scientific research such as, 2018 Payment Threats and Fraud Trends Report [7], Promoting Personal Responsibility For Internet Safety [4], Cyber Security Awareness Campaign: Why do they fail to change behavior? [8].

3) Implementing The Awareness Program

a. Techniques for delivering awareness material

It is the process of selecting media to deliver material. Material delivery media depends on the complexity of the message. NIST 800-50 provides several alternative media to convey messages. Messages on user awareness can be physically shaped such as banners, calendars, souvenirs and advertisements in print media. Whereas in digital form, among others, e-mail messages, advertisements through social media, computer based sessions and images for wallpapers for smart phones or computer. User awareness research is mostly conducted in formal organizations such as companies for employees. However, it does not rule out the possibility that user awareness is applied to the public or consumers because concerning the same topic. The main difference is that there are reward and punishment and necessity. Research from Abawajy et al [13] provides several techniques for conveying user awareness.

1. Conventional delivery methods

The conventional method includes paper based and electronic sources. The paper method is usually in the form of leaflets and posters, delivered in the form of short slogans, highlighting one specific topic, and giving advice that must be done. Flyers or posters are in public places that can be seen by many people. Flyers or posters are usually used to strengthen a particular message. The shortage of leaflets or posters is that message user awareness is being overlooked because it is constantly being seen. Another form of conventional method is the bulletin. Newsletters are published periodically monthly, quarterly or certain period of times and can be in the form of print or digital. Bulletins are generally used to strengthen or follow up on existing user awareness programs. The advantage of the bulletin compared to posters is that the bulletin can deliver several messages compared to poster.

2. Instructor-led delivery methods

Instructor-led delivery methods are methods of delivering in the form of presentations led by one or several people who are usually experts. This method is a top-down method with the aim of providing user awareness from the expert's point of view.

3. Web-based delivery methods

User awareness is delivered through the website. This method is user friendly while offering time flexibility. Users can access user awareness through website sessions. This method can also be used to offer interactive information security training if it is equipped with activities.

4. Game-based delivery methods

User awareness can be delivered in the form of games that combine graphic concepts, games and user awareness. The advantage of this method is that it can encourage users to participate. Besides this method can be used as a

measure of the success of user awareness through the value of the game that the user gets.

5. Video-based delivery methods

Educational videos can play an important role as part of user awareness. Video can be a medium that provides user awareness in a very interactive way. It can be seen many times, anytime, anywhere, which making user awareness very effective.

4) Post Implementation

a. Evaluation feedback and success indicator

Evaluation feedback and success indicators are the process of selecting techniques to evaluate and determine indicators of success. The selection of evaluation techniques must be preceded by an understanding that the user security awareness program is a continuous process. The most important thing is to start the process and complete it. Electronic money publisher may use the ways suggested by Gardner and Thomas [14] as seen below:

1. Number of hits on the security awareness

It is interpreted as the number of clicks or visits of users in the pop up message related to user awareness. Electronic money publishers can find out whether user awareness attracts the attention of users through the number of clicks: the more the number of clicks shows the users' interestusers' interest in the topic of security information.

2. Number of general questions e-mailed to the security group

It is defined as the number of questions, reports and complaints related to information security to the call center. The increasing number of questions, reports or complaints shows the increasing awareness of users to protect themselves. This means that user awareness can be considered to successfully increase.

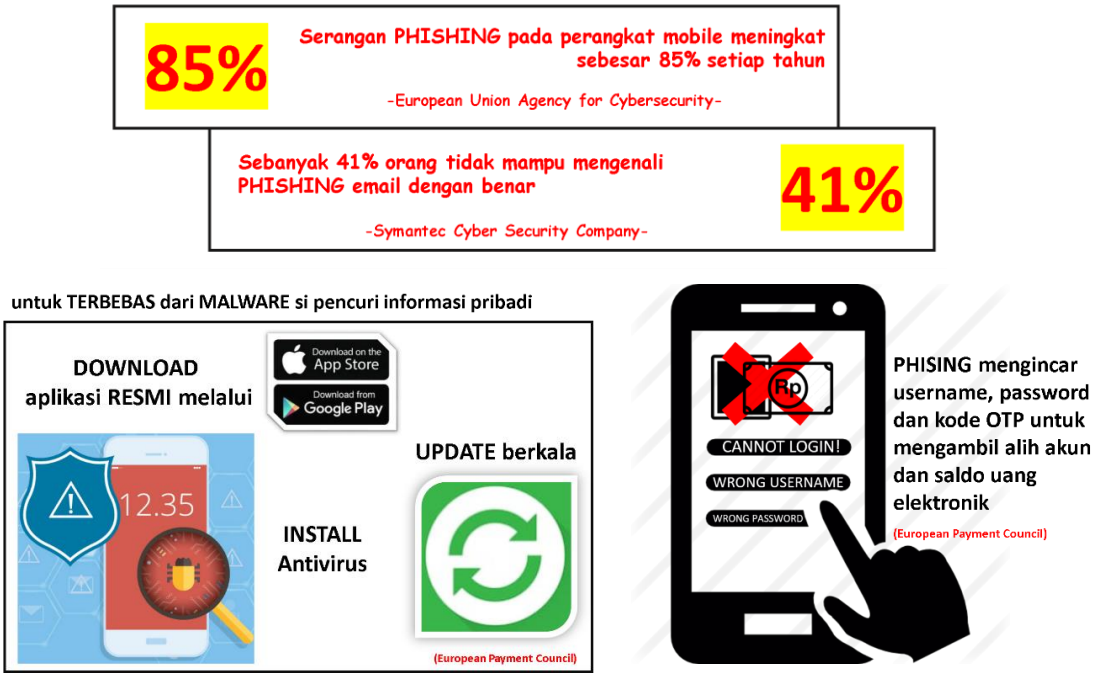

Figure 4. User Awareness by applying NIST 800-50 and PMT

V. CONCLUSION

This study aims to approach the protection motivation theory to obtain factors that influence the users to carry out precautionary behavior. These factors are then used as a basis for designing user awareness which is intended for users of electronic money.

1) The present research identifies the factors that influence users to conduct precautionary behavior that is tested in the population of electronic money users in Surabaya with a sample of 186 people.
2) This research supports protection motivation theory. The threat appraisal approach has proven to have a positive influence on the user to carry out precautionary behavior. The threat assessment is perceived security vulnerabilities, user perceptions of vulnerability to security threats and perceived security threat, the user's perception of the adverse effects that will be received. On the other hand, the approach to coping appraisal is obtained perceived response efficacy that is known to have a positive influence. As for The perceived security self efficacy and perceived prevention cost does not have an influence on the precautionary behavior of users of electronic money.
3) The NIST 800-50 framework can be used to design user awareness by applying the theory of protection motivation.

4) The NIST 800-50 framework produces topics that can be used on user awareness for electronic money users.

REFERENCES

[1] R. E. Crossler, "Protection motivation theory: Understanding determinants to backing up personal data," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2010.

[2] Bank Indonesia, "Peraturan Bank Indonesia Nomor 20/6/PBI/2018, Tentang Uang Elektronik." Jakarta.

[3] M. Wilson and J. Hash, "SP 800-50, Building an Information Technology Security Awareness and Training Program," Washington D.C., 2003.

[4] R. LaRose, N. J. Rifon, and R. Enbody, "Promoting personal responsibility for internet safety," *Commun. ACM*, vol. 51, no. 3, pp. 71–76, 2008.

[5] D. J. C. Brosdahl and J. M. Carpenter, "Shopping orientations of US males: A generational cohort comparison," *J. Retail. Consum. Serv.*, vol. 18, no. 6, pp. 548–554, 2011.

[6] R. N. Bolton *et al.*, "Understanding Generation Y and their use of social media: A review and research agenda," *J. Serv. Manag.*, vol. 24, no. 3, pp. 245–267, 2013.

[7] European Payment Council, "Payment Threats and Fraud Trends Report," 2018. [Online]. Available: availableat:https://www.europeanpaymentscouncil.eu. [Accessed: 24-Apr-2019].

[8] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," in *International Conference on Cyber Security for Sustainable Society*, 2015.

[9] Techinasia.com, "Connecting Asia's Startup Ecosystem," *Tech in Asia*, 2019. [Online]. Available: https://www.techinasia.com/fake-qr-code-scams-china. [Accessed: 18-Jun-2019].

[10] ELSAM Multimedia, "Infografis Kasus Penyalahgunaan Data Pribadi Sepanjang 2013-2017," *ELSAM Multimedia*, 2019. [Online]. Available: https://multimedia.elsam.or.id/infografis-kasus-penyalahgunaan-data-pribadi-sepanjang-2013-2017/. [Accessed: 13-Jun-2019].

[11] Stay Safe Online, "Get Online Safety Resources From the National Cyber Security Alliance," 2019. [Online]. Available: https://staysafeonline.org/. [Accessed: 13-Jun-2019].

[12] I-SAFE.org, "i-SAFE Home Content | iSAFE Ventures," 2019. [Online]. Available: http://www.isafe.org/. [Accessed: 13-Jun-2019].

[13] J. Abawajy, "User preference of cyber security awareness delivery methods," *J. Behav. Inf. Technol.*, vol. 33, no. 3, pp. 237–248, 2014.

[14] V. Thomas and B. Gardner, *Building an Information Security Awareness Program: Defending Against Social Engineering Hacks and Technical Threats*. Waltham, MA: Syngress Publishing, 2014.