TESIS – BM185407

PERANCANGAN *USER AWARENESS* PENGGUNA UANG ELEKTRONIK MENGGUNAKAN TEORI *PROTECTION MOTIVATION* DAN KERANGKA KERJA NIST 800-50

CHRISTIAN ANDREAN PRADIGDYA
09211750053004

Dosen Pembimbing
Dr.Tech Ir. R. V. Hari Ginardi, Msc

Departemen Magister Manajemen Teknologi
Fakultas Bisnis dan Manajemen Teknologi
Institut Teknologi Sepuluh Nopember
2019

LEMBAR PENGESAHAN TESIS

Tesis disusun untuk memenuhi salah satu syarat memperoleh gelar

Magister Manajemen Teknologi (M.MT)

di

Institut Teknologi Sepuluh Nopember

Oleh:

CHRISTIAN ANDREAN PRADIGDYA

NRP: 09211750053004

Tanggal Ujian: 3 Juli 2019

Periode Wisuda: September 2019

Disetujui oleh:

Pembimbing:

1. **Dr.tech. Ir. R. V. Hari Ginardi, M.Sc.**
   NIP: 19650518 199203 1 003 .....

Penguji:

1. **Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom**
   NIP: 19730219 199802 1 001 .....

2. **Faizal Mahananto, S.Kom., M.Eng., Ph.D.**
   NIPH: 5200201301010 .....

Kepala Departemen Manajemen Teknologi
Fakultas Bisnis dan Manajemen Teknologi

Prof. Ir. I Nyoman Pujawan, M.Eng. Ph.D. CSCP
NIP: 196912311994121076

PERANCANGAN *USER AWARENESS* UNTUK PENGGUNA UANG ELEKTRONIK MENGGUNAKAN TEORI *PROTECTION MOTIVATION* DAN KERANGKA KERJA NIST 800-50

Nama : Christian Andrean Pradigdya

NRP : 09211750053004

Pembimbing : Dr.Tech Ir. Hari Ginardi, M.Sc

ABSTRAK

Uang elektronik telah muncul sebagai salah satu metode pembayaran yang populer. Namun, popularitas tersebut malah menyebabkan ancaman keamanan baru bagi penggunanya. Data pribadi dan informasi keuangan adalah incaran oknum pelaku. Individu perlu bertanggung jawab pada data pribadi dan informasi keuangan yang melekat pada uang elektronik. Teknologi saja tidak mampu mencegah ancaman. Perilaku manusia juga menjadi faktor penting untuk melindungi dari ancaman serta memainkan peran penting dalam menjaga data pribadi dan informasi keuangan. Penelitian ini menggunakan *Protection Motivation Theory* (PMT) sebagai kerangka teori untuk menguji secara empiris mengapa orang melakukan perilaku pencegahan. PMT dapat menjelaskan perilaku keamanan, memberikan penjelasan teoritis terkait mengapa orang melakukan tindakan tertentu. Penelitian empiris dilakukan dengan menggunakan metodologi survei dan berhasil mengumpulkan data dari 186 responden. Hasil R^2 dari metode Partial Least Square tidak mendukung *protection motivation theory*. Variabel yang diajukan hanya menjelaskan 31,2% dan sisanya dijelaskan oleh variabel lain yang tidak ada dalam penelitian ini. Namun, hasil tersebut masih berkontribusi pada rancangan *user awareness* menggunakan kerangka kerja NIST 800-50. Program *user awareness* ditujukan agar pengguna memiliki kesadaran sehingga dapat memberdayakan pengguna uang elektronik untuk melindungi diri mereka sendiri.

Kata kunci: Kerangka Kerja NIST 800-50, Protection Motivation Theory, Uang Elektronik, User Awareness.

(Halaman ini sengaja dikosongkan)

USER AWARENESS DESIGN FOR ELECTRONIC MONEY USERS USING PROTECTION MOTIVATION THEORY AND NIST 800-50 FRAMEWORK

Nama	:	Christian Andrean Pradigdya
NRP	:	09211750053004
Pembimbing	:	Dr.Tech Ir. Hari Ginardi, M.Sc

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. PMT can explain security behaviors, providing a theoretical explanation as to why people perform certain countermeasures. Empirical research is conducted using survey methodology and collecting data from 186 respondents. The results of R^2 from Partial Least Square method didn't support protection motivation theory. Proposed variables only explain 31,2% and the remainder is explained by other variables which are not presented in this study. However, those results still 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, NIST 800-50, Partial Least Square, Protection motivation Theory, User Awareness

(Halaman ini sengaja dikosongkan)

KATA PENGANTAR

Penulis mengucapkan syukur yang tak terhingga kepada Tuhan Yesus atas segala berkat, kasih karunia, kesehatan dan hikmat sehingga penulis dapat menyelesaikan tesis yang merupakan salah satu syarat dalam menyelesaikan Program Studi Magister di Institut Teknologi Sepuluh Nopember Surabaya. Tesis beserta laporannya ini dapat terselesaikan tak luput dari peran serta berbagai pihak yang telah memberikan bantuan dan dorongan semangat, baik secara langsung maupun tak langsung. Atas segala bantuan yang telah diberikan, penulis mengucapkan terima kasih serta penghargaan yang sebesar-besarnya antara lain kepada :

1. Bapak Dr. Tech. Ir. R. V. Hari Ginardi, M.Sc. selaku dosen wali dan dosen pembimbing yang senantiasa memberikan bimbingan, saran, dan motivasi selama perkuliahan dan penulisan thesis kepada penulis.
2. Bapak Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom, Prof. Dr. Ir. Joko Lianto Buliali, M. Sc. dan Bapak Faizal Mahananto, S.Kom., M.Eng., Ph.D. selaku dosen penguji yang telah banyak membantu penulis memberikan kritik dan saran yang membangun.
3. Seluruh dosen S2 Manajemen Teknologi MMT ITS yang telah memberikan ilmu, motivasi dan pengetahuan kepada penulis selama menempuh studi.
4. Bapak Chris Adji Prabanto, Ibu Sudiyarmi Astuti, Christian Andhika, Christian Aditya selaku orang tua dan saudara penulis yang senantiasa mendukung dan mendoakan.
5. Natalia Dian Christiani yang selalu memberikan doa dan dukungan moral kepada penulis.

Penulis menyadari bahwa dalam laporan tesis ini masih banyak kekurangan. Karena itu, masukan ataupun saran demi perbaikan dan penerapan tesis ini di masa mendatang tetap penulis harapkan.

Surabaya, 24 Juli 2019

Penulis

(Halaman ini sengaja dikosongkan)

DAFTAR ISI

DAFTAR TABEL

(Halaman ini sengaja dikosongkan)

DAFTAR GAMBAR

(Halaman ini sengaja dikosongkan)

BAB 1
PENDAHULUAN

Pada bab ini akan dijelaskan beberapa hal dasar dalam pembuatan proposal penelitian yang meliputi: latar belakang, perumusan masalah, tujuan, manfaat, kontribusi penelitian, dan batasan masalah.

1.1. Latar Belakang

Bank Indonesia menjelaskan uang elektronik sebagai alat pembayaran yang memiliki nilai yang disimpan dalam media elektronik tertentu. Dalam uang elektronik, uang harus disimpan terlebih dahulu kepada penerbit dan disimpan dalam media elektronik sebelum menggunakannya untuk keperluan bertransaksi. Nilai uang elektronik dapat digunakan dan diisi kembali dalam media elektronik. Media elektronik untuk menyimpan nilai uang elektronik dapat berupa chip atau server. Uang elektronik diharapkan dapat dijadikan alat pembayaran yang inovatif dan praktis. Uang elektronik diharapkan pula dapat digunakan sebagai alternatif alat pembayaran non tunai yang dapat menjangkau masyarakat yang selama ini belum mempunyai akses kepada sistem perbankan.

Bank Indonesia melaporkan bahwa sepanjang 2018 transaksi menggunakan uang elektronik menunjukkan peningkatan yang sangat signifikan. Nominal transaksi yang dicatat telah mencapai lebih dari 3,8 T rupiah. Peningkatan ini dicatat telah mencapai 216,46% dibandingkan dengan tahun sebelumnya. Sebagai respon atas peningkatan tersebut telah diterbitkan 4 peraturan baru yang dikeluarkan oleh Bank Indonesia dan Otoritas Jasa Keuangan yang terkait dengan uang elektronik. Peraturan Bank Indonesia Nomor 20/6/PBI/2018 mengenai uang elektronik mengatur secara ketat kriteria terkait uang elektronik dan syarat yang harus dipenuhi untuk menjadi penerbit uang elektronik. Sedangkan peraturan dari Otoritas Jasa Keuangan secara spesifik banyak mengatur manajemen resiko, tindakan antisipasi, perlindungan privasi dan perlindungan konsumen.

Popularitas transaksi dengan uang elektronik yang semakin meningkat juga tentunya juga tak lepas dari peran teknologi. Teknologi yang semakin mudah diakses dan semakin murah turut menjadi faktor pendukung. Teknologi adalah

poros utama dalam transaksi uang elektronik dan mencakup keseluruhan aspek uang elektronik termasuk keamanan informasi dan privasi. Teknologi yang menunjang keamanan informasi dan privasi data dituntut untuk senantiasa berubah dan beradaptasi terhadap dinamika yang ada karena pencurian informasi dan privasi juga senantiasa berkembang.

Akan tetapi kecanggihan teknologi saja tidak cukup untuk melindungi pengguna dari ancaman yang ada. Kecanggihan teknologi juga harus diikuti dengan kecakapan pengguna dalam menggunakan teknologi. Faktor teknologi dan pengguna adalah faktor yang saling melengkapi. Karena tindakan dan sikap yang sembrono seorang pengguna adalah titik lemah dalam keamanan informasi dan privasi. Peran aktif pengguna juga amat sangat diperlukan untuk antisipasi. Peran aktif tersebut harus terus-menerus diwujudkan dalam bentuk kesadaran dan tindakan. Pengguna juga harus memiliki kepekaan terhadap ancaman saat bertransaksi dengan uang elektronik. Kepekaan tersebut terkait dengan pengenalan ancaman dan bagaimana mengatasi ancaman tersebut. Adapun ancaman terbesar dalam sistem uang elektronik adalah pencurian saldo, pembajakan akun serta pencurian informasi pribadi pengguna.

Di saat yang bersamaan, tindakan dan sikap seorang pengguna juga adalah faktor penentu keberhasilan pengamanan transaksi elektronik. Penelitian terkait juga menunjukkan bahwa faktor manusia memegang peranan penting dalam proses pengamanan keamanan informasi dan privasi, oleh karena itu pendekatan *socio-technical* perlu untuk terus dikembangkan. Pertanyaan yang diajukan selanjutnya adalah bagaimana meningkatkan kesadaran dan kepekaan pengguna untuk melakukan tindakan pencegahan. Sebaliknya bagi penyedia jasa uang elektronik pertanyaan yang diajukan adalah bagaimana meningkatkan kesadaran pengguna untuk senantiasa melakukan tindakan pencegahan. Secara keseluruhan yang diperlukan adalah bagaimana mendapatkan pemahaman menyeluruh terkait motivasi pengguna untuk melindungi dirinya saat bertransaksi dengan uang elektronik.

Perilaku pengguna dalam melakukan tindakan pencegahan ancaman dapat diketahui menggunakan teori *protection motivation*. Teori ini dikembangkan

oleh Rogers pada 1975 yang berdasarkan apa yang dikerjakan oleh Lazarus pada 1966 dan Leventhal pada 1970. Teori *protection motivation* adalah suatu proses penilaian ancaman dan proses penilaian tanggapan yang mengakibatkan niat untuk melaksanakan tanggapan adaptif (motivasi perlindungan) atau maladaptif (menempatkan pada resiko). Teori *protection motivation* berfungsi mengembangkan intervensi untuk mengurangi ancaman pada individu dengan mengintegrasikan konsep psikologis, sosiologis dan bidang lain yang terkait. Teori *protection motivation* adalah model *social-cognitive* yang memprediksi perilaku. Teori ini memang lebih banyak diaplikasikan di bidang kesehatan guna memprediksi dan menjelaskan perilaku antisipatif seseorang (Milne, Sheeran, & Orbell, 2000; Maddux & Rogers, 1983; Floyd, Prentice-Dunn, & Rogers, 2000). Sampai pada akhirnya teori *protection motivation* mulai banyak digunakan untuk penelitian terkait keamanan informasi. Penerapan teori *protection motivation* diaplikasikan pada kepatuhan terhadap kebijakan keamanan informasi (Herath & Rao, 2009; Ifinedo, 2012; Vance et al., 2012), adopsi perangkat lunak anti-spyware (Johnston & Warkentin, 2010; Liang & Xue, 2010), perilaku pencadangan data pribadi (Crossler, 2010), perilaku protektif terhadap pencurian identitas, (Lai, Li, & Hsieh, 2012) dan perilaku pengguna terhadap *online banking* (Jurjen Jansen & Paul van Schaik, 2017).

Hasil yang ingin dicapai dari penelitian ini adalah untuk mendapatkan gambaran pada faktor-faktor yang mempengaruhi pengguna uang elektronik untuk mengambil tindakan penccegahan guna melindungi dirinya dari ancaman berdasarkan teori *protection motivation*. Untuk itu, penelitan ini mengembangkan sebuah model penelitian kemudian mengujinya menggunakan metode *Partial Least Square*. Pendekatan PLS lebih cocok karena pendekatan ini mengasumsikan bahwa semua ukuran varians adalah varians yang berguna untuk dijelaskan. Hasilnya kemudian digunakan guna mengembangkan sebuah program berupa *user awareness* untuk meningkatkan kesadaran dan kecakapan pengguna dalam menggunakan uang elektronik.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan diatas maka penulis merumuskan masalah dalam penelitian ini yaitu sebagai berikut :

1. Faktor-faktor apa saja yang mempengaruhi pengguna melakukan *precautionary behavior* untuk melindungi dirinya saat bertransaksi dengan uang elektronik?
2. Bagaimana merancang *user awareness* menggunakan kerangka kerja NIST 800-50 dengan menggunakan protection *motivation theory* sebagai landasan?

1.3. Tujuan

Tujuan dari penelitian ini adalah dapat mengidentifikasi faktor-faktor apa saja yang mempengaruhi motivasi pengguna mengambil tidakan pencegahan untuk melindungi dirinya saat bertransaksi dengan uang elektronik. Sehingga penelitian ini tidak hanya membantu penerbit untuk memahami motivasi pengguna untuk melindungi dirinya, tetapi juga dapat membantu pembuatan program *user awareness* terkait keamanan informasi.

1.4. Manfaat

Manfaat dari penelitian ini adalah dapat memberi manfaat sebagai berikut

a. Dapat memberi referensi tambahan untuk penelitian dengan topik terkait kemanan informasi.
b. Dapat membantu pemahaman lebih mendalam mengenai faktor-faktor yang mempengaruhi motivasi pengguna untuk melindungi dirinya dari ancaman terkait keamanan informasi dan privasi.
c. Dapat dijadikan pertimbangan bagi penerbit dan pihak-pihak terkait dalam merancang program *user awareness* untuk meningkat perilaku antisipatif dan protektif terhadap keamanan informasi dan privasi.

1.5. Kontribusi Penelitian

Hasil dari penelitian ini akan menghasilkan model baru dalam penelitian terkait perilaku pengguna dan kemanan informasi teknologi khususnya teknologi uang elektronik.

1.6. Batasan Masalah

Untuk memfokuskan permasalahan penelitian ini, batasan masalah yang ditentukan adalah sebagai berikut:

1. Populasi penelitian adalah responden kuesioner yang pernah menggunakan uang elektronik.
2. Penelitian terbatas menganalisis faktor yang mempengaruhi motivasi pengguna uang elektronik melakukan perlindungan dengan pendekatan *Protection Motivation Theory* (PMT).
3. Uang elektronik dalam penelitian ini adalah uang elektronik yang berbasis perangkat lunak (*server-based product)* yaitu, GoPay, OVO dan LinkAja.

1.7. Sistematika Penulisan

Berikut ini adalah sistematika penulisan yang akan diterapkan pada proses penelitian ini :

Bab I Pendahuluan

Bab ini menyajikan tentang latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, kontribusi penelitian, dan sistematika penulisan.

Bab II Kajian Pustaka

Dalam bab ini terdapat sub bab dan landasan teori dari penelitian terdahulu yang memaparkan teori-teori yang berhubungan dengan masalah yang diteliti serta beberapa penelitian yang telah dilakukan pada penelitian-penelitian sebelumnya.

Bab III Metode Penelitian

Bab ini menguraikan deskripsi tentang bagaimana penelitian nantinya akan dilakukan dan menjelaskan variabel penelitian, definisi operasional, penentuan populasi, jenis dan sumber data, jalannya penelitian dan alur penelitian.

Bab IV Hasil Penelitian dan Pembahasan

Bab ini menjelaskan tentang pengumpulan data dan pengolahan data serta menguraikan tentang deskripsi objek penelitian melalui gambaran umum dan proses pengintegrasian data yang diperoleh untuk mencari makna dari hasil analisa.

Bab V Kesimpulan dan Saran

Bab ini menyajikan kesimpulan dan saran yang didapatkan dari pembahasan pada hasil penelitian.

BAB 2
KAJIAN PUSTAKA

Pada bab ini akan dijelaskan tentang dasar teori yang digunakan dalan penelitian. Dasar teori yang digunakan antara lain Uang Elektronik, *Protection Motivation Theory* (PMT), *Partial Least Square* (PLS), dan NIST 800-50.

2.1. Uang Elektronik

Bank for International Settlement (BIS) dalam publikasinya mendefinisikan uang elektronik sebagai produk *stored value* atau prabayar dimana sejumlah nilai uang disimpan dalam suatu media elektronis yang dimiliki seseorang. Sedangkan dalam Peraturan Bank Indonesia nomor 20/6/PBI/2018 tentang uang elektronik, Bank Indonesia mendefinisikan uang elektronik sebagai instrumen pembayaran yang memenuhi unsur-unsur tertentu. Unsur-unsur tersebut yaitu, nilai uang yang disetor terlebih dahulu kepada penerbit, nilai uang disimpan secara elektronik dalam suatu media *server* atau *chip* dan nilai uang elektronik yang dikelola oleh penerbit bukan merupakan simpanan sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai perbankan. Lebih lanjut dijelaskan bahwa nilai uang elektronik dapat dipindahkan untuk kepentingan transaksi pembayaran dan/atau transfer dana. Disamping itu, uang elektronik yang dimaksudkan berbeda dengan *single purpose prepaid card* lainnya seperti kartu telepon, karena uang elektronik yang dimaksudkan dapat digunakan untuk berbagai macam jenis pembayaran (*multipurposed*). Uang elektronik yang dimaksudkan juga berbeda dengan alat pembayaran elektronis seperti kartu kredit dan kartu debet. Kartu kredit dan kartu debet bukan merupakan *prepaid products* melainkan *access products*.

2.1.1 Manfaat Uang Elektronik

Berikut kelebihan penggunaan uang elektronik dibandingkan dengan uang tunai maupun alat pembayaran nontunai lainnya:

1. Uang elektronik dapat digunakan untuk transaksi bernilai kecil.
2. Proses transaksi lebih praktis karena pengguna tidak perlu menyediakan uang pas atau memiliki uang kembalian tunai.

3. Tidak memiliki resiko kesalahan perhitungan
4. Lebih hemat waktu karena proses autentikasi relatif lebih mudah dan cepat.
5. Selain itu, dengan transaksi luring, maka biaya komunikasi dapat dikurangi.
6. Pengisian ulang mudah dilakukan kapanpun, dimanapun dan dapat menggunakan berbagai sarana.

2.1.2 Pembagian Uang Elektronik

Bank Indonesia dalam Peraturan Bank Indonesia nomor 20/6/PBI/2018 tentang uang elektronik membedakan uang elektronik menurut media penyimpanan berupa:

1. *server based,* yaitu uang elektronik dengan media penyimpan berupa *server*;
2. *chip based*, yaitu uang elektronik dengan media penyimpan berupa *chip*;

Menurut pencatatan data identitas pengguna uang elektronik dibedakan menjadi:

1. *unregistered,* yaitu uang elektronik yang data identitas penggunanya tidak terdaftar dan tidak tercatat pada penerbit;
2. *registered,* yaitu uang elektronik yang data identitas penggunanya terdaftar dan tercatat pada penerbitt pekerjaan meningkat baik pada kualitas dan kuantitas dengan menggunakan sistem.

Sedangkan menurut lingkup penyelenggaraan uang elektronik dibedakan sebagai berikut

1. *closed loop,* yaitu uang elektronik yang hanya dapat digunakan sebagai instrumen pembayaran kepada penyedia barang dan/atau jasa yang merupakan penerbit uang elektronik tersebut;
2. *open loop,* yaitu uang elektronik yang dapat digunakan sebagai instrumen pembayaran kepada Penyedia Barang dan/atau Jasa yang bukan merupakan penerbit uang elektronik tersebut.

2.1.3 Kejahatan dalam Transaksi Uang Elektronik

Keuntungan finansial adalah target utama seseorang untuk melakukan kejahatan terhadap uang elektronik. Selain itu pencurian data pribadi pengguna juga merupakan target lainnya. Hal ini tentunya dapat menyebabkan kerugian bagi pihak-pihak yang terkait seperti penerbit maupun pengguna uang elektronik. Dalam

penyelenggaraan uang elektronik, faktor utama yang mempengaruhi tingkat keamanan penggunaannya antara lain adalah instrumen/peralatan (*hardware*) yang digunakan, baik oleh konsumen maupun oleh *merchant*, aplikasi (*software*) serta proses pertukaran data elektronik pada saat terjadi transaksi. Berikut bentuk kejahatan yang ditimbulkan:

1. *Phising*

   Kejahatan ini merupakan upaya untuk memancing pengguna memberikan informasi tertentu dengan menyamar sebagai pihak yang memiliki otoritas, misal penerbit uang elektronik. Secara umum, pengguna akan diminta untuk memberikan informasi tertentu melalui *hyperlink* yang dikirimkan lewat surat elektronik. Pengguna umumnya terpancing karena karena alamat surat elektronik pelaku kejahatan sangat meyakinkan atau juga karena iming-iming hadiah.

2. *Mobile Malware*

   Laporan dari European Payment Council pada 2017 menyebutkan bahwa Malware dalam bentuk Trojan mampu memiliki *superuser rights* sebuah perangkat android. Trojan yang memiliki *superuser rights* mampu menyembunyikan dirinya dari deteksi antivirus dan pengguna. Selain itu, Trojan jenis ini juga mampu mengirimkan data tertentu sampai melakukan instalasi perangkat lunak tertentu ke dalam sebuah perangkat android. Hal ini tentu berbaya pada perangkat android yang didalamnya menyimpan data pengguna uang elektronik.

3. Pencurian Melalui Penggunaan Jaringan Nirkabel Publik

   Survei yang dilakukan oleh ISACA pada 2015 menunjukkan bahwa penggunaan jaringan nirkabel publik untuk transaksi uang elektronik memiliki kerentanan. Kerentanan tersebut berupa pencurian data dan informasi tertentu di dalam jaringan nirkabel. Apalagi jika jaringan nirkabel tersebut tidak dilengkapi dengan enkripsi yang ketat sehingga setiap orang yang memiliki akses di dalam jaringan tersebut dapat mengambil data yang ada.

4. Pencurian Perangkat Ponsel Pintar

Bentuk kejahatan uang elektronik yang paling sederhana adalah dengan mencuri ponsel pintar milik orang lain untuk kemudian menggunakan dana yang masih tersisa. Pencurian ponsel pintar selain merugikan pengguna sendiri juga dapat merugikan orang lain. Pencuri ponsel pintar dapat menggunakan daftar kontak di dalam ponsel pintar tersebut untuk dijual kepada pihak lain atau untuk melakukan penipuan.

5. Manipulasi dengan *QR Code*

   Proses bertransaksi yang mudah dilakukan, hanya dengan memindai *QR Code* dengan perangkat ponsel pintar, membuat *QR Code* menjadi cepat diimplementasikan dimanapun. *QR Code* jamak digunakan untuk pembayaran kepada penjual yang menerima pembayaran dengan uang elektronik. Akan tetapi, laporan terakhir menujukkan penyalahgunaan *QR Code* dengan menyusupkan malware tertentu sehingga mengakibatkan kerugian finansial yang tidak sedikit. Jadi, ketika pengguna memindai *QR Code,* maka pengguna terse but akan masuk ke situs tertentu yang mengeksploitasi data pribadi pengguna atau melakukan unduhan *malware*.

6. Penipuan dengan kode *OTP*

   One Time Password atau kode verifikasi dikirimkan melalui layanan pesan singkat dalam tiga situasi. Pertama, pengguna mencoba masuk ke akun miliknya; kedua, pengguna mengganti atau mengeset ulang PIN/sandi miliknya; terakhir, pengguna mengubah nomor telepon atau emailnya dimana keduanya berfungsi sebagai *username*. Pelaku kejahatan OTP biasanya meretas sebuah akun dengan cara masuk menggunakan nomor ponsel calon korban. Kemudian ia menanyakan (pada umumunya melalui telepon) kode OTP yang dikirimkan sistem kepada calon korban melalui SMS dengan berbagai alasan, mulai dari syarat untuk mengambil hadiah undian, meminta bantuan darurat dengan iming-iming imbal jasa, hingga modus salah kirim kode verifikasi. Begitu OTP terkirim, pelaku mendapat akses seluas-luasnya terhadap akun korban dan menggasak rekeningnya. Bila tiba-tiba Anda menerima pesan OTP, padahal tak sedang melakukan satu dari tiga kegiatan di atas, jelas, seseorang tengah mengincar akun Anda. Mengingat manusia merupakan elemen terlemah

dalam sistem keamanan dunia maya, peringatan untuk tidak memberikan kode OTP penting dilakukan.

2.1.4 Panduan Keamanan Transaksi Uang Elektronik

Sebagai mana pada instrumen pembayaran elektronis lainnya, penerbit uang elektronik telah memberikan panduan keamanan untuk dipatuhi pengguna. Panduan keamanan ini selalu diberikan pada pengguna saat proses instalasi aplikasi uang elektronik. Berikut panduan yang umumnya diberikan oleh pengguna uang elektronik:

1. *Login Information*

   Jangan memberikan *login information* berupa nama pengguna (pada umumnya akun surat elektronik atau nomer telepon), kata sandi (*personal identification number*) dan kode OTP (*one time password*) kepada siapapun. *Login information* uang elektronik sebaiknya diketahui hanya oleh pengguna atau pemilik akun tersebut saja. Pengguna juga harus waspada dan tidak memberikan informasi apapun kepada pihak-pihak yang mengaku pihak berotoritas yang meminta *login information*.

2. Keamanan Perangkat Ponsel Pintar

   Ponsel pintar sebaiknya dikunci dengan kata sandi atau dengan *biometric key* (umumya berupa sidik jari). Hal ini untuk mencegah pemakaian uang elektronik oleh sembarang orang.

3. Perlindungan akun

   Penerbit uang elektronik menganjurkan penggunaan nomer telepon dan akun surat elektronik yang masih aktif serta sudah terverifikasi dengan data yang benar. Kata sandi sebaiknya terdiri gabungan dari huruf kapital, huruf kecil, dan karakter. Kata sandi juga sebaiknya diganti secara berkala. Selain itu, akun sebaiknya dibedakan dengan akun-akun yang lain, kata sandi dan alamat surat elektronik menggunakan akun khusus uang elektronik. Prinsip satu akun dan satu kata sandi untuk semua akun harus dihindari.

4. Lakukan pembaruan

   Penerbit uang elektronik secara berkala akan melakukan pembaruan aplikasi uang elektronik. Pembaruan bertujuan untuk menutup celah keamanan yang

ditemukan serta memberikan tambahan informasi. Oleh karena itu, pengguna harus senantiasa melakukan pembaruan aplikasi.

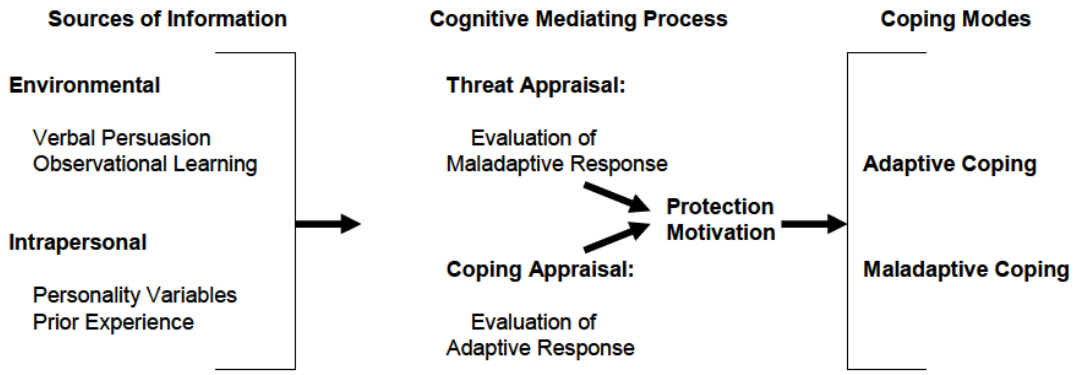
2.2. *Protection Motivation Theory* (PMT)

Pada 2007 *Americas Conference on Information Systems* (AMCIS) mengusulkan agar pendekatan terhadap teori-teori dari disiplin keilmuan lain perlu diuji guna menghadapi tantangan keamanan yang semakin bertambah. Salah satunya adalah *protection motivation theory* (PMT) yang diadaptasi dari keilmuan psikologi social. PMT dapat menjelaskan perilaku keamanan seorang individu, menyediakan penjelasan teoritis mengapa seorang individu melakukan tindakan perlawanan (*countermeasure*) untuk mengenali dan mencegah ancaman yang ada.

Premis dari PMT adalah pertama-tama sebuah informasi diterima (*sources of information*), kemudian individu yang menerimanya akan menilai informasi tersebut (*cognitive mediating process*), dan pada akhirnya individu tersebut mengambil tindakan terhadap informasi yang diterima (*coping mode*). Sumber inforrmasi adalah variabel masukan pada model yang disertai dengan kondisi lingkungan (*environmental*) dan sumber interpersonal (*intrapersonal sources*). Sumber informasi dari lingkungan individu (*environmental sources of information*) termasuk persuasi verbal dan pembelajaran observational. Sedangkan sumber interpersonal (*intrapersonal sources*) termasuk aspek personal umpan balik (*feedback*) dari pengalaman sebelumnya, termasuk pengalaman yang terasosiasi untuk melakukan sebuah perilaku yang diminati (Crossler, 2010).

Menurut konsep PMT, terdapat dua proses kognitif yang menjadi mediasi proses, *threat appraisal process* dan *coping appraisal process* (Crossler, 2010). Proses penilaian ancaman (*threat appraisal process*) terdiri dari persepsi terhadap keparahan (*severity*) dan kerentanan (*vulnerability*) dari tindakan maladaptif. Pada konteks penelitian ini proses penilaian ancaman (*threat appraisal process*) adalah penilaian ancaman keamanan yang terjadi pada saat bertransaksi dengan uang elektronik. Sedangkan proses penilaian penyelesaian (*coping appraisal process*) terdiri dari kepercayaan diri individu pada respon penyelesaian akan mengurangi atau meringankan ancaman keamanan (*response efficacy*) dan individu tersebut percaya bahwa repon tersebut dapat dilakukan (*self efficacy*), hanya jika respon

tersebut tidak memerlukan biaya pencegahan (*prevention cost*) tidak terlalu tinggi. Pada konteks penelitian ini proses penyelesaian (*coping appraisal process*) adalah penilaian kemampuan individu untuk melakukan tindakan pencegahan dan kepercayaan diri bahwa tindakan pencegahan tersebut dapat berhasil mencegah atau menghindari potensi ancaman saat bertransaksi dengan uang elektronik, dengan persepsi biaya pencegahan (*prevention cost*) yang tidak terlalu besar. Hasil yang diharapkan dari proses mediasi kognitif adalah keputusan untuk mengaplikasikan respon yang adaptif dan aplikatif. Terdapat dua tipe perliaku adaptif yaitu perilaku adaptif (untuk melindungi diri) dan maladaptif (tidak melindungi diri). Gambar 2.1 menjelaskan proses tersebut (Crossler, 2010).



Gambar 2.1 Konsep PMT

2.3. *Partial Least Square* (PLS)

Partial Least Square (PLS) dikembangkan pertama kali oleh Herman Wold (1982). Ada beberapa metode yang dikembangkan berkaitan dengan PLS yaitu model *PLS Regression* (PLS-R) dan *PLS Path Modeling* (PLS-PM). PLS *Path Modeling* dikembangkan sebagai alternatif pemodelan persamaan structural (SEM) yang dasar teorinya lemah. PLS-PM berbasis varian. Sedangkan metode SEM menggunakan basis kovarian. Perbedaan analisis PLS dengan model analisis SEM yaitu data pada PLS tidak harus berdistribusi normal, dapat menggunakan sampel kecil, dapat digunakan sebagai konfirmasi teori, dapat digunakan untuk menjelaskan ada atau tidaknya hubungan antar variabel laten. PLS dapat menganalisis konstruk yang dibentuk beserta dengan indikator reflektif dan

formatif sekaligus atau bersifat campuran antara keduanya. PLS mampu mengestimasi model yang besar dan kompleks dengan ratusan variabel laten dan ribuan indikator (Falk and Miller, 1992).

Dalam PLS *path modeling* terdapat dua model yaitu model pengukuran dan model struktural. Kriteria uji dilakukan pada kedua model tersebut. Uji yang dilakukan pada model pengukuran yaitu validitas konvergen dan validitas deskriminan. Konstruk dianggap memenuhi validitas konvergen jika memiliki 3 kriteria sebagai berikut:

1. semua item mempunyai *loading factor* minimal 0.60 dan idealnya 0.70
2. *composite reliability* untuk semua indikator yang digunakan mempunyai nilai lebih dari 0.7
3. nilai *Average Variance Extracted* (AVE) lebih dari 0.5 (Chin, 1998)

Konstruk dianggap memenuhi validitas diskriminan jika nilai *loading* antara variabel laten dengan indikatornya lebih tinggi daripada *loading* indikator tersebut dengan variabel laten lain. Uji yang dilakukan diatas merupakan uji pada model pengukuran untuk indicator reflektif. Untuk indikator formatif dilakukan pengujian yang berbeda. Uji untuk indikator formatif yaitu dengan:

1. s*ignificance of weights* untuk mengetahui nilai weight indikator formatif dengan konstruknya harus signifikan;
2. *multicolliniearity* untuk mengetahui hubungan antar indikator. Indicator formatif mengalami *multicolliniearity* dapat diketahui dari nilai VIF. Nilai VIF antara 5-10 dapat dikatakan bahwa indikator tersebut terjadi *multicolliniearity*.

Uji pada model struktural dilakukan untuk menguji hubungan antara konstruk laten. Ada beberapa uji untuk model struktural yaitu:

1. R^2 pada konstruk endogen, menurut Chin (1998), nilai R2 sebesar 0.67 (kuat), 0.33 (moderat) dan 0.19 (lemah);
2. *Estimate for path coefficients*, merupakan nilai koefisen jalur atau besarnya hubungan/pengaruh konstruk laten dilakukan dengan prosedur bootrapping;
3. *Effect size* (f2) dilakukan untuk mengetahui kebaikan model;

4. *Prediction relevance* (Q2) atau dikenal dengan Stone-Geisser's untuk mengetahui kapabilitas prediksi dengan prosedur blinfolding apabila nilai yang didapatkan 0.02 (kecil), 0.15 (sedang) dan 0.35 (besar).

2.3.1 Konstruk Multidimensi pada PLS

Konstruk berdasarkan kompleksitasnya dibedakan menjadi konstruk unidimensional dan konstruk multideminsional. Konstruk unidiminsional adalah konstruk yang dapat diukur langsung dengan indikatornya. Pengujian konstruk dilakukan langsung melalui *first order construct* dengan indikatonya. Konstruk multidimensional adalah konstruk yang tidak berhubungan langsung dengan indikatornya namun dengan sub-konstruk dari dimensi konstruk. Pengujian konstruk dilakukan melalui dua tahap yaitu, *first order construct* untuk menguji sub-konstruk yang direfleksikan/dibentuk indikatornya, dan kedua *second order construct* untuk menguji konstruk laten yang direfleksikan/dibentuk oleh subkonstraknya. Konstruk multidimensional mendapat perhatian besar dalam jurnal system informasi pada tahun belakang ini namun langkah-langkah bagaimana mengkonsepkan dan mengoperasionalkan konstruk multidimensional dalam SEM masih mendapat perhatian yang sedikit (Wright et al, 2012). Akibatnya perbedaaan dalam mengkonsepkan dan mengoperasionalkan konstruk multidimensional tidak dapat dihindari. Wright et al (2012) telah menyediakan langkah-langkah praktis dalam mengkonsepkan dan mengoperasionalkan konstruk multidimensional untuk membantu peneliti dalam mengevaluasi konstruk multidimensional. Langkah-langkah pengujian konstruk multidimensional pada *covarian based model* (CB-SEM) berbeda dengan *component based model* (PLSSEM). Karena penelitian ini menggunakan PLS maka penulis hanya menjelaskan secara rinci langkah-langkah pengujian konstruk multidimensional pada PLS. Berikut adalah langkah-langkah pengujian konstruk multidimensional pada PLS menurut Wright et al (2012) :

1. Melakukan pengujian model pengukuran *first order*. Sesuai dengan Agarwal & Karahanna (2000), analisa konfirmatori faktor dari *first order* dilakukan untuk mendapatkan *latent variabel score* dari subkonstruk dimensinya yang selanjutnya akan digunakan pada pengujian model pengukuran dan model struktural *second order*.

2. Melakukan pengujian model pengukuran *first order* yang dimulai dari evaluasi reliabilitas data, evaluasi validitas konvergen, dan evaluasi validitas diskriminan. Evaluasi reliabilitas dilakukan dengan memeriksa apakah semua sub-konstruk dimensi memiliki *composite reliability* (CR) > 0.7. Lalu, evaluasi validitas konvergen dilakukan dengan memeriksa apakah semua sub-konstruk dimensi memiliki AVE > 0.5.
3. Terakhir, evaluasi validitas diskriminan dilakukan dengan memeriksa apakah semua sub-konstruk dimensi memiliki akar AVE lebih besar dibandingkan korelasi dengan laten variabel lain.
4. Setelah melakukan pengujian model pengukuran *first order* selanjutnya melakukan pengujian model struktural *second order* dengan membuat file data baru yang diperoleh dari *latent variabel score* dari *first order*.
5. Membuat model *second order* baru dengan menggunakan *latent variabel*
6. *score* sebagai indikator untuk setiap dimensi.
7. Melakukan pengujian model struktural dengan memeriksa signifikasi *path coefficients* (β)
8. Mengevaluasi hasil model struktural secara keselutuhan dengan
9. memeriksa nilai R2, e*ffect size* (f2), dan *Prediction relevance* (Q2).

2.4. *NIST Special Publication 800-50: Building An Information Technology Security Awareness and Training Program*

National Institute of Standards (NIST) adalah badan nonregulator yang merupakan bagian dari Administrasi dan Teknologi Departemen Perdangan Amerika Serikat. NIST mempunyai misi untuk mengembangkan metode pengujian, mengembangkan referensi data, mengimplementasikan konsep, dan melakukan analisis teknis guna mengembangkan produktifitas penggunaan teknologi informasi. NIST bertanggung jawab juga untuk pengembangan teknis dan administratif, standar manajerial yang dilengkapi panduan yang pembiayaan yang efektif dan perlindungan informasi sensitif dari perangkat komputer milik negara. Hasilnya adalah laporan berupa *Special Publication 800-serie*s yang memberikan panduan beserta upaya penjangkauan pada keamanan komputer, dan aktifitas kolaboratif dengan industri, pemerintahan dan organisasi akademis.

Perancangan perilaku kesadaran keamanan informasi dirancang untuk mengubah perilaku atau memperkuat perilaku yang sudah ada. Kesadaran (*awareness*) tidak sama dengan pelatihan. Secara sederhana tujuan yang ingin dicapai adalah untuk memfokuskan perhatian pada resiko keamanan yang ada. Presentasi kesadaran ditujukan untuk mengijinkan individu untuk menyadari potensi ancaman pada keamanan teknologi informasi dan memberikan respon yang tepat. Penyampaian kesadaran yang dikemas dengan lebih menarik akan lebih mudah diterima individu. Selain itu, program keamanan teknologi informasi yang kuat harus dijadikan prioritas. Tanpa prioritas yang kuat potensi kegagalan juga akan semakin besar.

Salah satu hasil seri publikasi NIST adalah NIST 800-50. NIST 800-50 adalah panduan untuk membangun kesadaran keamanan teknologi informasi dan program pelatihan. Publikasi ini menyediakan panduan untuk membangun program kesadaran keamanan teknologi informasi dan program pelatihan dengan lebih efektif. Publikasi ini mengidentifikasi 4 langkah utama pada siklus pelatihan kesadaran dan program pelatihan, yaitu:

1. ***Awareness and Training Program Design***

   Pada tahap ini dilakukan penilaian kebutuhan dan pengembangan strategi. Perencanaan diidentifikasi sebagai sebuah tugas yang harus dijalankan agar tujuan bisa tercapai.

2. ***Awareness and Training Material Development***

   Tahapan ini berfokus pada penetapan lingkup materi, pengembangan materi dan pengadaan materi. Pada tahap ini pemilihan topik yang akan disampaikan juga ditentukan. Berikut topik yang dapat dimasukkan :

   a. Pengggunaan dan pengelolaan kata sandi
   b. Perlindungan dari virus, *worms*, dan *trojan horses*
   c. Kebijakan keamanan informasi
   d. Sisipan tautan pada pesan elektronik
   e. Respon terkait insiden

3. ***Program Implementation***

Tahap ini menunjukkan bagaimana menyampaikan pesan yang efektif dan mudah dipahami. Oleh karena itu, teknik penyampaian yang dipakai harus memenuhi unsur-unsur berikut:

a. *Ease of use* mudah diakses dan mudah diperbarui
b. *Scalability* dapat digunakan untuk jumlah audiensi yang besar maupun kecil juga mencakup lokasi besar maupun kecil
c. *Accountability* dapat dipertanggungjawabkan
d. *Broad base of industry support* harus bisa menjangkau berbagai bidang

Pada tahap ini juga dijelaskan pilihan untuk media penyampaian. Berikut teknik penyampaian material yang dapat dipergunakan:

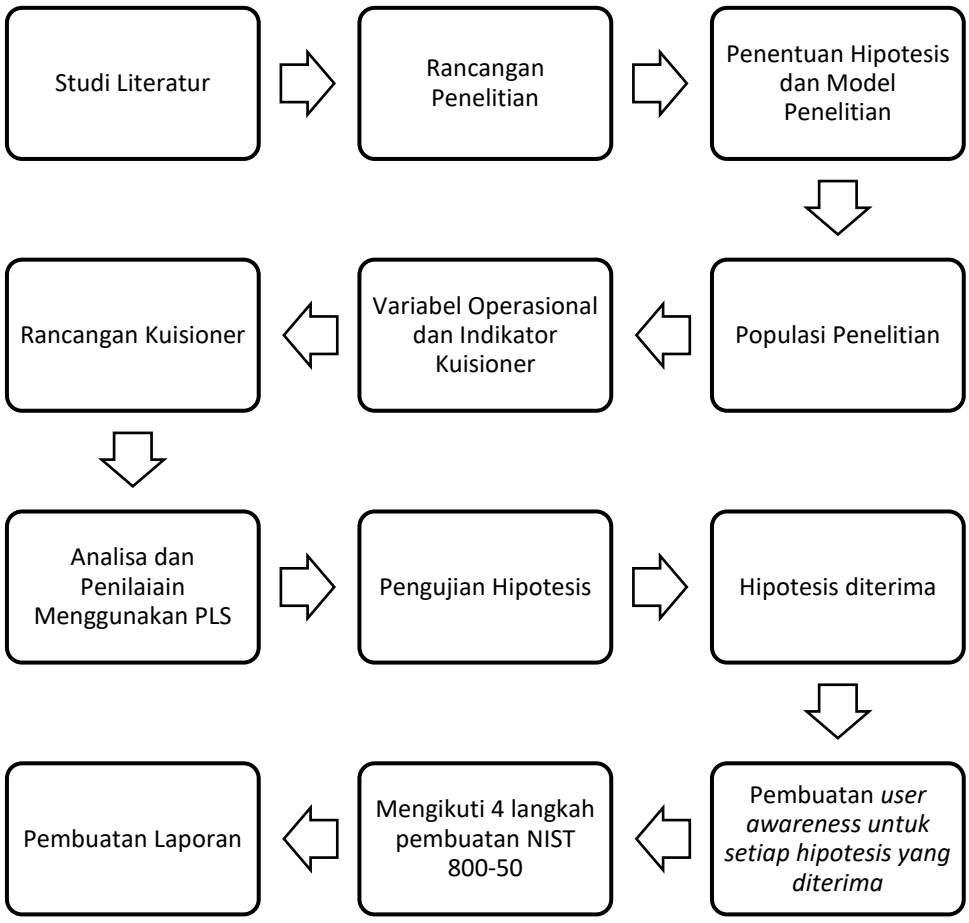
a. Pesan yang dituliskan pada alat disekitar pengguna. Contoh, bolpen, jam, buku catatan kecil, dan lain sebagainya)
b. Menggunakan poster
c. *Newsletter*
d. Sesi khusus dalam sebuah *website*
e. Video

4. *Post Implementation*

Tahap ini memberikan panduan untuk memonitor efektifitas program yang ada serta bagaimana menjaga kontinuitas. Efektifitas dapat diukur dengan mengembangkan survei, diskusi kelompok dan pengukuran kuantitatif pada peserta pelatihan.

BAB 3
METODOLOGI PENELITIAN

Pada bab ini akan diuraikan mengenai metodologi penelitian yang akan dilaksanakan terdiri dari studi literatur, rancangan penelitian, penentuan hipotesis dan model penelitian, populasi penelitian, metode pengumpulan data, variabel operasional dan indikator kuesioner, rancangan kuesioner, analisis dan penilaian menggunakan PLS, pengujian hipotesis, dan pembuatan laporan yang alurnya ditunjukkan pada Gambar 3.1. Selanjutnya disertakan jadwal kegiatan penelitian yang memuat garis waktu dari semua langkah penelitian.



Gambar 3.1 Alur Metodologi Penelitian

3.1. Studi Literatur

Pada tahap ini penulis mengumpulkan referensi yang sesuai dengan penelitian. Pengumpulan referensi dilakukan dengan membaca penelitian terkait dari jurnal ilmiah dan buku. Tahap ini dilakukan untuk memberikan gambaran permasalahan beserta metode yang yang tepat untuk menjawab permasalah penelitian.

3.2. Rancangan Penelitian

Motivasi perlindungan individu pada uang elektronik dapat diketahui melalui model konseptual yang didasari oleh penelitian-penelitan terdahulu dan pada temuan yang diuji secara empiris. Oleh karena itu penelitian dan pengumpulan data mengambil pendekatan secara kuantitatif. Metode kuantitatif adalah pendekatan ilmiah yang memandang suatu realitas itu dapat diklasifikasikan, konkrit, teramati, dan terukur, hubungan variabelnya bersifat sebab akibat dimana data penelitiannya berupa angka-angka dan analisisnya menggunakan statistik (Sugiyono, 2008).

3.3. Penentuan Hipotesis dan Model Penelitian

Hipotesis adalah jawaban sementara terhadap masalah yang masih bersifat praduga karena masih harus dibuktikan kebenarannya. Hipotesis pada dasarnya merupakan suatu proposisi atau anggapan yang mungkin benar dan sering dipergunakan untuk dasar pembuatan keputusan atau pemecahan persoalan atau untuk dasar penelitian yang lebih lanjut.

Teori *protection motivation* terdiri dari 2 proses kognitif yaitu penilaian ancaman (*threat appraisal*) dan penilaian penyelesaian (*coping appraisal*). Pada proses penilaian ancaman individu melakukan evaluasi terhadap kemungkinan akan ancaman dan dampak yang mengikuti. Hal ini diikuti oleh proses penyelesaian di mana individu melakukan evaluasi terhadap cara penyelesaian masalah dan beradaptasi terhadap perubahan untuk menghadapi ancaman. Proses penyelesaian digerakkan oleh efektivitas strategi atau tindakan, dimana pada kondisi tertentu individu tersebut mampu melakukan tindakan yang diperlukan beserta mengetahui akibat yang mengikutinya. Proses kognitif diinisiasi dengan penerimaan informasi yang ada, beserta kondisi lingkungan individu dan relasi antar individu. Proses-proses tersebut memiliki pengaruh pada motivasi perlindungan, yaitu niat untuk

melakukan perilaku tertentu. Pada konteks penelitian ini hasil yang ingin dicapai adalah faktor-faktor yang mempengaruhi individu untuk mengambil tindakan pencegahan. Maka dari itu perlu didefinisikan terlebih dahulu konstruk atau faktor tersebut seperti yang dapat dilihat pada tabel 3.1.

Tabel 3.1 Definisi Konstruk PMT

Konstruk PMT	**Definisi**
Threat Appraisal	Penilaian individu terhadap tingkatan ancaman yang terjadi pada saat bertransaksi dengan uang elektronik
Coping Appraisal	Penilaian individu terhadap kepercayaan diri dan kemampuannya melakukan tindakan pencegahan yang diyakini akan berhasil dengan usaha seminimal mungkin
Perceived Security Vulnerability	Persepsi penilaian terhadap kemungkinan terjadinya ancaman keamanan transaksi uang elektronik
Perceived Security Threat	Persepsi penilaian terhadap dampak atau kerugian sebagai akibat dari ancaman keamanan transaksi uang elektronik
Perceived Security Self Efficacy	Persepsi kepercayaan diri individu terhadap kemampuannya melakukan respon atau tindakan pencegahan yang direkomendasikan
Perceived Response Efficacy	Persepsi kepercayaan diri individu terhadap efektivitas sebuah respon atau tindakan untuk mencegah ancaman keamanan transaksi uang elektronik
Perceived Prevention Cost	Persepsi seorang individu terhadap biaya, waktu, dan usaha yang harus dilakukan untuk melakukan tindakan pencegahan yang disarankan untuk mencegah atau mengurangi dampak ancaman keamanan transaksi uang elektronik

3.3.1 Pengaruh *Security Threat Appraisal* terhadap *Precautionary Behavior*

Security threat appraisal (penilaian ancaman keamanan) adalah proses penilaian individu terhadap ketidakpastian sebagai sebuah kerentanan yang akan dialami jika terpapar ancaman. PMT memosisikan *threat appraisal* sebagai salah satu determinan yang mempengaruhi apakah seseorang mengadopsi respon perilaku yang diberikan. Penelitian yang ada menunjukkan bahwa semakin seseorang memiliki persepsi resiko maka seseorang akan cenderung mengambil tindakan pencegahan untuk melindungi dirinya atau menghindar sama sekali dari resiko (Crossler 2010).

Pada konteks penelitian ini *security threat appraisal* terdiri dari *perceived security vulnerability* dan *perceived security threat*. Keduanya memiliki peranan masing-masing. Pada penelitian terkait kedua konstruk tersebut dapat berpengaruh kuat atau tidak sama sekali bergantung pada subjek yang diteliti (LaRose et all., 2015). Individu akan memiliki respon yang berbeda jika ditunjukkan potensi terjadinya kejahatan. Beberapa akan menganggap hal tersebut sangat mungkin terjadi pada dirinya dan sebagian yang lain menganggap hal tersebut sangat tidak mungkin terjadi pada dirinya.

Perceived security vulnerability mengacu pada persepsi individu terhadap peluang terjadinya kejahatan uang elektronik. Bentuk kejahatan uang elektronik mencakup *phising* memanfaatkan surat elektronik atau kode OTP, pencurian data melalui *mobile malware*, maupun pencurian perangkat ponsel pintar. Ketika individu mempersepsikan bagaimana kejahatan uang elektronik bisa terjadi dan membandingkannya dengan pola perilakunya maka disinilah terjadilah proses penilaian kerentanan (*perceived security vulnerability*). Jika individu menilai dirinya berpeluang kecil menjadi korban kejahatan uang elektronik maka semakin kecil juga peluang perilaku perlindungan dilakukan. Sebaliknya ketika individu mempersepsikan bahwa dirinya rentan dan berpeluang untuk menjadi korban kejahatan uang elektronik maka kencenderungan melakukan tindakan perlindungan semakin besar.

Ketika potensi ancaman dikenali maka individu akan melakukan evaluasi pada perilakunya kemudian menentukan ambang batas sejauh mana dirinya dapat menerima, menghindari atau menolak dampak yang ada. Dampak yang mungkin diterima korban kejahatan uang elektronik diantaranya adalah, kehilangan sejumlah saldo, penangguhan akun, pencurian identitas untuk melakukan kejahatan, dan penjualan data pribadi pada pihak ketiga. Semakin besar dampak dan kerugian yang dipersepsikan individu terhadap dirinya maka akan semakin besar peluang tindakan pencegahan dilakukan dan berlaku sebaliknya. Penilaian ini menentukan sejauh mana orang dapat menerima dampak sebelum menjakankan perilaku penyelesaian. Proses ini didefinisikan sebagai *perceived security threat*. Melalui kedua konstruk tersebut dibangun sebuah hipotesis sebagai berikut:

H1: *Perceived security vulnerability* secara positif mempengaruhi individu melakukan *precautionary behavior*

H2: *Perceived security threat* secara positif mempengaruhi individu melakukan *precautionary behavior*

3.3.2 Pengaruh *Security Coping Appraisal* terhadap *Precautionary Behavior*

Security coping appraisal adalah penilaian kemampuan individu untuk melakukan tindakan pencegahan dan dengan kepercayaan diri meyakini tindakan pencegahan tersebut dapat berhasil mencegah atau menghindarkan potensi ancaman saat bertransaksi dengan uang elektronik dengan biaya pencegahan (*prevention cost*) seminimal mungkin (Crossler 2010). Pada konteks penelitian ini *security coping appraisal* terdiri dari *perceived security self efficacy, perceived response efficacy,*dan *perceived prevention cost*. Ketiga konstruk tersebut berpengaruh kuat atau tidak sama sekali bergantung pada subjek yang diteliti (LaRose et all., 2015).

PMT mendefinisikan *self efficacy* sebagai kepercayaan diri individu pada kemampuannya melakukan perilaku yang disarankan. Individu yang percaya diri dapat melakukan perilaku yang disarankan lebih berpeluang besar melakukan *precautionary behavior* (Ng et all., 2009). Penelitian ini mendefinisikan *self efficacy* sebagai *perceived security self efficacy* yaitu persepsi kepercayaan diri terhadap kemampuannya melakukan tindakan pencegahan yang direkomendasikan.

Semakin tinggi kepercayaan diri maka semakin berpengaruh positif mempengaruhi individu melakukan perilaku pencegahan yang disarankan. Sebagai contoh, penerbit uang elektronik menyarankan pengguna membuat kata sandi yang sulit ditebak. Individu yang memiliki persepsi kepercayaan diri bahwa dirinya bisa membuat kata sandi yang sulit ditebak maka individu tersebut akan melakukan tindakan tersebut.

Response self efficacy pada PMT didefinisikan sebagai kepercayaan individu pada keberhasilan perilaku yang disarankan. Penelitian yang terkait dengan PMT menunjukkan bahwa individu akan cenderung melakukan tindakan pencegahan jika meyakini tindakan tersebut dapat berhasil. Pada konteks penelitian ini *response self efficacy* didefinisikan sebagai *perceived response self efficacy* yaitu persepsi individu terhadap keberhasilan tindakan perlindungan mencegah ancaman keamanan. Semakin tinggi persepsi keyakinan individu pada keberhasilan sebuah tindakan perlindungan maka akan berpengaruh positif mempengaruhi individu melakukan perilaku pencegahan yang disarankan. Contohnya, semakin individu percaya bahwa dengan menginstal antivirus dapat mencegah *malware* mencuri data maka semakin besar peluang individu tersebut melakukannya *precautionary behavior*.

Meskipun individu mungkin meyakini jika perilaku yang diberikan efektif mengurangi ancaman, individu tersebut mungkin saja tidak melakukannya. Hal itu disebabkan dikarenakan tindakan tersebut terlalu sulit atau terlalu membebani. Efek negatif ini didefinisikan sebagai *perceived barriers*. Persepsi ini dapat mencegah individu bertindak karena perilaku pencegahan atau perlindungan menuntut individu melakukan usaha seperti biaya, waktu dan upaya kognitif ekstra (Ng et al., 2009). Dengan kata lain, upaya perlindungan atau pencegahan tidak akan dilakukan pengguna jika usaha untuk melakukan perilaku pencegahan lebih membebani dibandingkan dampak buruk yang akan terjadi. Sebagai contoh, penerbit uang elektronik menyarankan untuk melakukan pergantian kata sandi dan pembaruan aplikasi secara berkala. Jika individu mempersepsikan hal tersebut sebagai sesuatu yang terlalu membebani maka individu akan cenderung mengabaikannya (*precautionary behavior*). Pada penelitian ini, *perceived barriers* didefinisikan

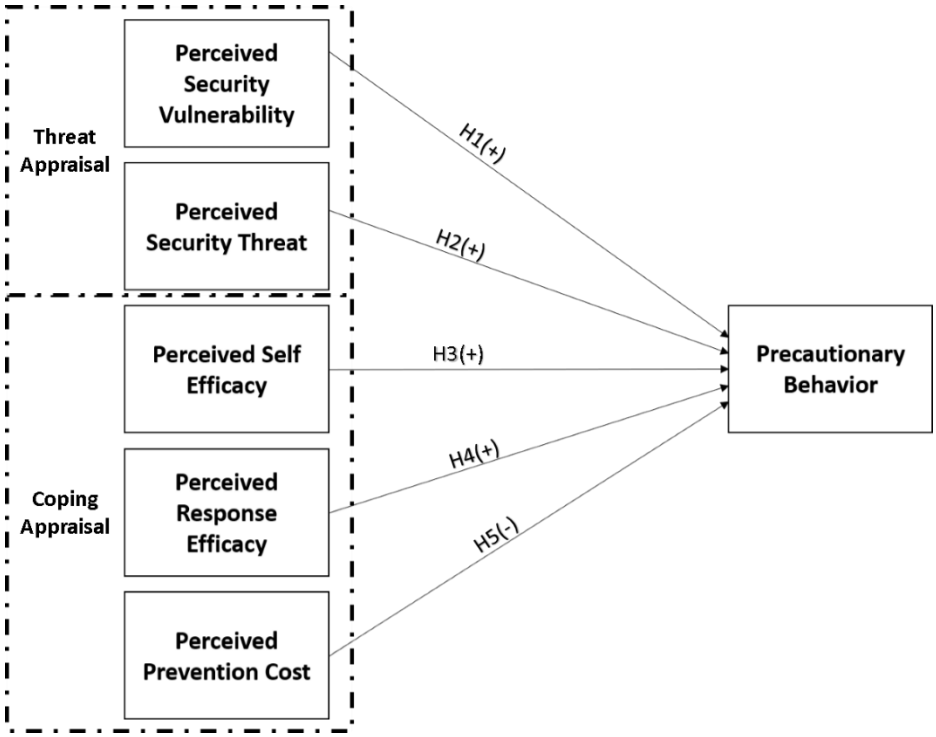
sebagai *perceived prevention cost*. Melalui ketiga konstruk tersebut dibangun hipotesis sebagai berikut:

H3: *Perceived security self efficacy* secara positif mempengaruhi individu melakukan *precautionary behavior*

H4: *Perceived response efficacy* secara positif mempengaruhi individu melakukan *precautionary behavior*

H5: *Perceived prevention cost* secara negatif mempengaruhi individu melakukan *precautionary behavior*

Model penelitian dan hipotesis dijelaskan dalam Gambar 3.2 di bawah ini:



Gambar 3.2 Model Penelitian

3.4. Populasi Penelitian

Populasi penelitian adalah jumlah keseluruhan dari satuan-satuan atau individu-individu yang karakteristiknya hendak diteliti. Satuan-satuan tersebut dinamakan unit analisis, dan dapat berupa orang-orang, institusi-institusi, benda-benda, dst. Target populasi penelitian adalah pengguna uang elektronik. Responden didapatkan dengan menyebarkan tautan kuesioner melalui pesan berantai dan memanfaatkan media sosial. Penelitian ini memakai PLS yang memerlukan jumlah

data paling sedikit berjumlah 30-100 orang. Penelitian ini penulis mengambil data dengan cara menghitung jumlah indikator dikali dengan 10.

3.5. Metode Pengumpulan Data

Pada penelitian ini, pengumpulan data primer dilakukan dengan cara menyebarkan survei yaitu pengumpulan data terstruktur berupa kuesioner. Kuesioner ini akan disebarkan dengan memanfaatkan fasilitas kuesioner digital *Google Forms*. Metode yang digunakan dalam pengisian kuesioner berupa *self-administered survey*, dimana kuesioner diisi sendiri oleh responden dan pertanyaan berupa pertanyaan terstruktur yang alternatif jawabannya dalam bentuk skala (*scale*). Pertanyaan dengan menggunakan skala digunakan untuk mengukur dan mengetahui tanggapan responden mengenai pertanyaan-pertanyaan yang terdapat pada kuesioner. Kuesioner penelitian ini menggunakan metode skala likert dengan 5 poin.

3.6. Variabel Operasional dan Indikator Kuesioner

Pertanyaan dalam kuesioner terbentuk dari informasi-informasi atas variabel-variabel yang akan diteliti. Penelitian ini menggunakan 6 variabel yang terdiri dari:

a. 5 variabel independen/endogen, *perceived security vulnerability*, *perceived security threat, perceived security self efficacy, perceived response efficacy*, dan *perceived prevention cost.*
b. 1 variabel dependen/eksogen, yaitu *precautionary behaviour*.

Untuk semua variabel independen dan variabel dependen diukur dengan menggunakan skala likert (5 poin) dengan rincian sebagai berikut:

a. Sangat tidak setuju (STS) diberi skor 1
b. Tidak Setuju (TS) diberi skor 2
c. Netral (N) diberi skor 3
d. Setuju (S) diberi skor 4
e. Sangat Setuju (SS) diberi skor 5

Tabel 3.2 menunjukkan pertanyaan-pertanyaan yang akan diajukan pada kuesioner ini.

Tabel 3.2 Kuesioner penelitian

Variabel	**Kode**	**Indikator**	**Sumber**
Perceived Security Vulnerabilities (PSV)	PSV1	Saya mungkin saja mengalami *phising* atau ditipu dengan memanfaatkan kode *one time password* (OTP)	(Woon et al, 2005)
	PSV2	Saldo, informasi finansial dan informasi pribadi saya bisa saja menjadi cukup rentan untuk dicuri tanpa saya sadari	
Perceive Security Threat (PST)	PST1	Bagi saya kehilangan akun dan saldo uang elektronik dampaknya akan sangat buruk	(Woon et al, 2005)
	PST2	Pencurian informasi pribadi dan informasi finasial saya adalah masalah yang serius	
	PST3	Pemakaian identitas saya oleh orang yang mencuri akun uang elektronik adalah masalah yang sangat penting	
Perceived Self Efficacy (PSE)	PSE1	Bagi saya menjaga keamanan ponsel pintar adalah cara yang mudah untuk dilakukan	(Martens et all, 2018)
	PSE2	Saya memiliki pengetahuan dan kemampuan untuk menjaga *login information* agar aman dan terlindungi	
	PSE3	Saya merasa nyaman selalu memiliki kehati-hatian dan kewaspadaan setiap saat untuk melindungi akun uang elektronik	

Perceived Response Efficacy (PRE)	PRE1	Menjaga keamanan ponsel pintar adalah cara yang efektif untuk mencegah pencurian saldo dan akun uang elektronik saya	(Woon et al, 2005)
	PRE2	Melindungi *login information* dapat membantu mencegah informasi pribadi dan informasi finasial saya dicuri	
	PRE3	Dengan selalu berhati-hati dan waspada tidak mempercayai informasi selain dari penerbit uang elektronik dapat menghindarkan saya menjadi korban kejahatan uang elektronik	
Perceived Prevention Cost (PPC)	PPC1	Membuat dan melindungi *login information* sesuai yang disarankan mengharuskan saya memulai kebiasaan baru dimana merupakan hal yang sulit	(Ng et al., 2009) (Woon et al, 2005)
	PPC2	Kenyamanan saya berkurang jika harus terus-menerus berhati-hati dan waspada saat bertransaksi menggunakan uang elektronik	
	PPC3	Ada beban biaya, usaha, dan waktu yang besar untuk menjalankan panduan keamanan uang elektronik yang disarankan	

3.7. Rancangan Kuesioner

Kuesioner yang digunakan dalam penelitian ini terbagi ke dalam tiga bagian, yaitu sebagai berikut:

1. Bagian pertama pertanyaan untuk mengetahui data demografi dari responden yaitu usia, jenis kelamin, dan durasi kepemilikan akun.
2. Bagian kedua berisi penjelasan informasi dan pertanyaan *threat appraisal*. Pada bagian ini akan dijelaskan dengan singkat mengenai bagaimana kejahatan uang elektronik dapat terjadi dan dampak yang akan diterima. Selanjutnya pengguna akan diberi pertanyaan-pertanyaan *threat appraisal* sesuai Tabel 3.2.
3. Bagian ketiga berisi penjelasan informasi dan pertanyaan *coping appraisal*. Pada bagian ini akan dijelaskan dengan singkat mengenai bagaimana kejahatan uang elektronik dapat dicegah. Selanjutnya pengguna akan diberi pertanyaan-pertanyaan *coping appraisal* sesuai Tabel 3.1.

Pada bagian kedua dan ketiga responden diberikan informasi terkait *threat* (ancaman) dan *coping* (penyelesaian) terlebih dahulu sebelum menjawab pertanyaan yang merupakan premis PMT, individu mendapat sumber informasi terlebih dahulu. Setelah itu individu melakukan proses mediasi kognitif (*cognitive mediating process*) dan kemudian mengambil tindakan (Crossler, 2010).

3.8. Analisis dan Penilaian Menggunakan PLS

Dalam analisis menggunakan PLS terdapat beberapa langkah umum yang harus dilakukan. Berikut adalah langkah-langkah yang dilakukan:

1. **Analisis Awal**

   Pada tahap ini, dilakukan pemeriksaan terhadap kuesioner yang telah terisi. Melalui pemeriksaan ini diharapkan dapat diketahui kuesioner yang telah diisi oleh responden layak atau tidak digunakan dalam penelitian. Menurut Malhotra (2009), ada beberapa hal yang menyebabkan kuesioner tidak layak digunakan diantaranya : (a) kuesioner diisi atau dijawab oleh orang yang tidak sesuai dengan kualifikasi (bukan pengguna uang elektronik dengan jenis *server based*); (b) responden hanya memilih angka 3 saja pada pertanyaan yang memiliki 5 skala.

2. **Pengolahan Data dengan *Partial Least Square* (PLS)**

   Kuesioner yang telah diisi selanjutnya akan diolah dengan menggunakan PLS. Pada tahap ini akan dilakukan pengujian *outer* model dan *inner* model. Uji *outer*

model digunakan untuk menguji validitas terhadap variabel-variabel pada model dan uji reliabilitas untuk mengetahui apakah konstruk tersebut memiliki reliabilitas yang baik untuk diuji lebih lanjut. Sedangkan uji *inner* model atau uji struktural dilakukan untuk mengetahui seberapa besar *precautionary behaviour* berpengaruh dalam motivasi pengguna melakukan perlindungan menggunakan perhitungan *path coefficients*. Setelah itu dilakukan analisis variabel yang berpengaruh terhadap motivasi perlindungan pengguna dengan analisis *t-value* dengan menggunakan *bootstrapping* pada PLS.

3.9. Pengujian Hipotesis

Pengujian hipotesis dilakukan dengan menghitung *path coefficients*. Setelah data diolah dengan PLS maka akan menampilkan nilai P (P-*value*). Nilai P digunakan untuk memutuskan apakah hipotesis diterima atau tidak dengan membandingkannya dengan nilai alpha (α) = 5%, ketentuannya adalah sebagai berikut:

1. P-*value* ≤ nilai α, maka keputusannya adalah hipotesis diterima. Hipotesis diterima berarti terdapat pengaruh yang signifikan dari variabel independen terhadap variabel dependen.
2. P-*value* > nilai α, maka keputusannya adalah hipotesis ditolak. Hipotesis ditolak berarti tidak terdapat pengaruh variabel independen terhadap variabel dependen.

3.10. Pembuatan Program *User Awareness* dengan NIST 500-80

Tahapan selanjutnya adalah membuat *user awareness*. *User awareness* akan dibuat berdasarkan setiap hipotesis yang diterima. Hipotesis tersebut akan dijadikan masukan pada *scope of the awareness* guna mengembangkan *user awareness*. Setiap hipotesis yang diterima akan dibuatkan *user awareness* masing-masing. Sebagai contoh, hipotesis *perceived security threat* secara positif mempengaruhi individu melakukan *precautionary behaviour* diterima. *Perceived security threat* adalah persepsi penilaian terhadap dampak atau kerugian sebagai akibat dari ancaman keamanan transaksi uang elektronik. Maka *user awareness* akan dibuat dengan *scope of the awareness* yang menekankan pada dampak kejahatan. *User awareness* akan menjelaskan topik terkait dampak buruk yang akan diterima

pengguna. Pembuatan *user awareness* dengan cara seperti ini pernah dilakukan oleh (*source*). Selanjutanya *user awareness* yang dibuat dengan menggunakan PMT dapat dijadikan rujukan untuk penerbit uang elektronik.

User awareness akan dibuat dengan menggunakan kerangka kerja NIST 500-80 dengan mengkikuti 4 langkah utama. Langkah-langkah tersebut meliputi, *awareness program design, awareness material development, program implementation,* dan *post implementation.* Langkah-langkah ini perlu dijalankan untuk membuat sebuah *user awareness* yang terstruktur dengan jelas. Akan tetapi, tidak semua langkah-langkah yang ada akan diikuti karena kerangka kerja ini juga mencakup *training program* untuk organisasi perusahaan. Oleh karena itu, berikut langkah-langkah dari masing-masing tahapan kerangka kerja NIST 500-80 yang akan diikuti guna merancang *user awareness*:

1. *Awarenesss Program Design*

Tahapan ini memberikan poin-poin yang yang dapat menilai kebutuhan dan mendesain pembuatan *user awareness*.

a. *existing*: bentuk *user awareness* yang saat ini sudah ada
b. *scope of the awareness*: ruang lingkup *user awareness* yang akan diambil dari setiap hipotesis yang diterima.
c. *goals to be accomplished*: tujuan yang ingin dicapai dengan menyesuaikan tujuan hipotesis yang diterima.
d. *target audience*: kepada siapa *user awareness* ini ditujukan dalam hal ini terkait usia.
e. *mandatory*: mendesain *user awareness* sebagai sebuah kewajiban
f. *topics to be addressed*: disampaikan sesuai dengan topik terkait setiap hipotesis yang diterima.
g. *frequency* atau jumlah siklus penyampaian *user awareness* dalam satu waktu tertentu.

2. *Developing Awareness Material*

Tahapan ini akan membantu penyusunan *supporting material* dengan tujuan agar target pengguna memiliki kemampuan untuk melakukan perilaku perlindungan yang diharapkan. Pemilihan *supporting material* juga harus spesifik,

personal, menarik dan kekinian sehingga tidak menjadi formalitas belaka. Berikut hal-hal yang perlu diperhatikan:

a. *selecting awareness*: memilih topik spesifik dari setiap hipotesis yang diterima
b. *source of awareness material*: penyertaan referensi ilmiah yang relevan

3. *Implementing The Awareness Program*

Tahapan selanjutnya adalah implementasi. Tahapan ini akan memberikan masukan untuk media penyampaian *user awareness*.

a. techniques for delivering awareness material: adalah teknik memilih media penyampaian materi yang bergantung pada kompleksitas pesan

4. *Post Implementation*

Tahapan selanjutnya adalah evaluasi. Tahapan ini menjelasakan dan mberikan masukan saran terkait metode-metode apa saja yang dapat dipakai.

1. evaluation feedback and success indicator: memilih teknik untuk mengevaluasi dan menentukan indikator keberhasilan.

3.11. Pembuatan Laporan

Langkah selanjutnya adalah membuat laporan dan simpulan dari hasil penelitian yang telah dilakukan. Simpulan ini akan menjawab rumusan-rumusan masalah yang telah ditentukan diawal penelitian. Dari hasil simpulan tersebut bisa digunakan untuk rekomendasi pembuatan program *user awareness* pengguna uang elektronik. Pembuatan laporan dilakukan agar semua langkah yang telah dilakukan terdokumentasi dengan baik sehingga bisa memberikan informasi yang berguna bagi pembacanya.

BAB 4
HASIL DAN PEMBAHASAN

Pada Bab ini membahas pengolahan data dan penjelasan tahapan-tahapan dan hasil analisis data dan pengujian hipotesis menggunakan metode PLS-PM. Hasil dari pengujian hipotesis yang diterima akan dipergunakan untuk membuat user awareness.

4.1. Pengumpulan Data

Pengumpulan data menggunakan kuesioner dengan menggunakan aplikasi Google Forms. Aplikasi Google Forms terdiri dari 7 bagian yaitu pertanyaan demografi responden dan pertanyaan validasi yaitu "Apakah anda pernah bertransaksi menggunakan uang elektronik ?" untuk memastikan responden pernah menggunakan uang elektronik. Bagian selanjutnya berturut-turut adalah informasi *threat appraisal*, pernyataan *threat appraisal* yang dijawab responden, informasi *coping appraisal*, pernyataan *threat appraisal* yang dijawab responden, dan pernyataan *precautionary behavior* yang dijawab responden. Keuntungan menggunakan Aplikasi Google Forms adalah pengaturan untuk memaksa responden menjawab semua pertanyaan sebelum melanjutkan ke bagian selanjutnya. Hal ini diperlukan guna memastikan responden menjawab semua pertanyaan dan menghindari *missing value*.

Target responden adalah para pengguna uang elektronik. Target jumlah responden adalah 170 orang yang didapatkan dengan menghitung jumlah indikator penelitian (17) dikali dengan 10. Responden didapatkan dengan menyebarkan tautan kuesioner Google Forms melalui pesan berantai dan memanfaatkan media sosial. Kuesioner disebar selama 7 hari pada 21 Mei 2019 sampai dengan 27 Mei 2019 dengan jumlah responden yang berhasil didapatkan sebanyak 196 orang.

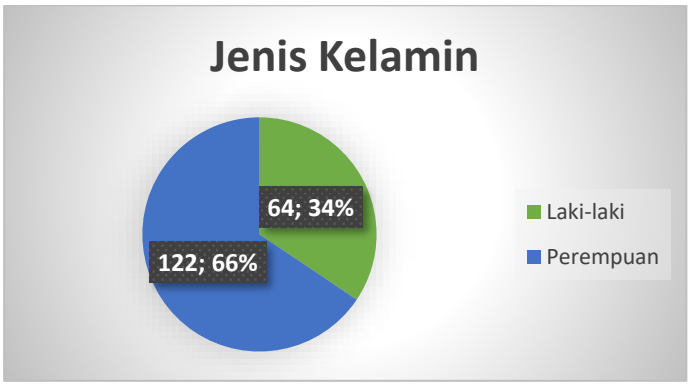
Data kuesioner diunduh dan diolah terlebih dahulu melalui Microsoft Excel. Format dokumen adalah *.csv file*. Proses pengolahan data awal adalah sebagai berikut:

1. Data demografi dihapus sehingga hanya menyisakan data penelitian berupa jawaban angka kuesioner yang bernilai 1 sampai dengan 5.
2. Data responden kemudian dipilah berdasarkan jawaban pertanyaan validasi, jika jawaban tidak maka tidak dipergunakan.
3. Setelah dilakukan pemilahan validasi maka didapatkan jumlah responden sebanyak 186 orang. Data ini merupakan data akhir yang akan diolah Smart PLS dan merupakan populasi penelitian.

4.2. Data Demografi Responden

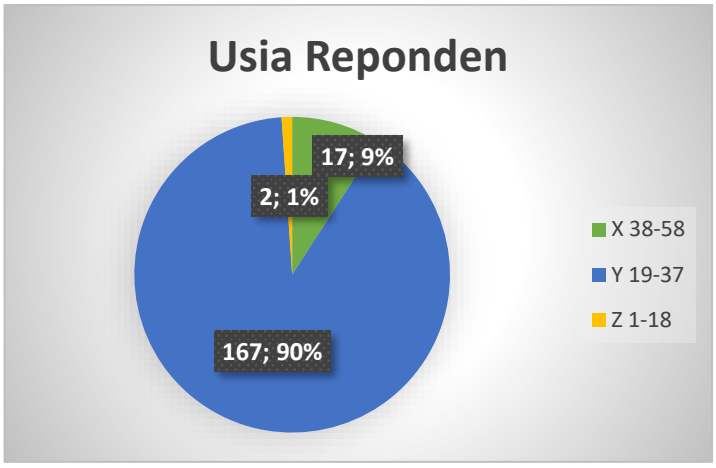
Responden penelitian merupakan pengguna uang elektronik. Pengguna adalah orang yang pernah menggunakan uang elektronik berbasis aplikasi. Data demografi responden yang berhasil dikumpulkan adalah jenis kelamin, usia, uang elektronik yang dipakai dan usia akun uang elektronik.

Data demografi jenis kelamin 186 responden menujukkan 64 orang (34%) adalah laki-laki dan 122 orang (66%) adalah perempuan seperti yang dijelaskan pada Gambar 4.1.



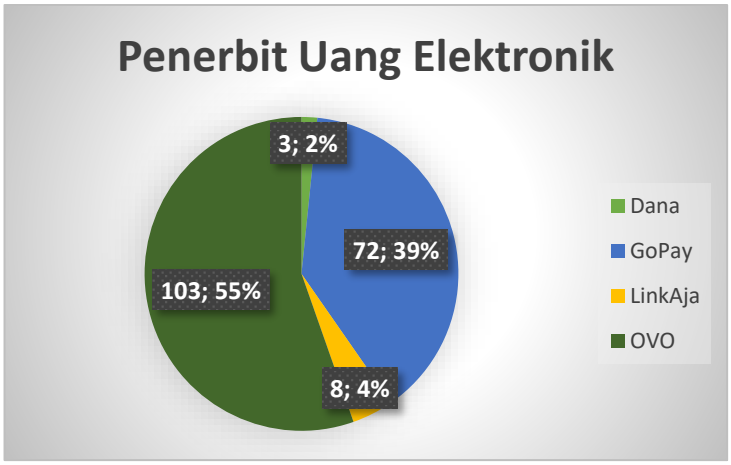
Gambar 4.1 Data Demografi Jenis Kelamin Responden

Data demografi usia 186 responden menujukkan 17 orang (9%) adalah generasi X dengan rentang usia 38-54 tahun, 167 orang (90%) adalah generasi Y dengan rentang usia 19-37 tahun dan 2 orang (1%) adalah generasi Z dengan usia kurang dari 18 tahun seperti yang dijelaskan pada Gambar 4.2.



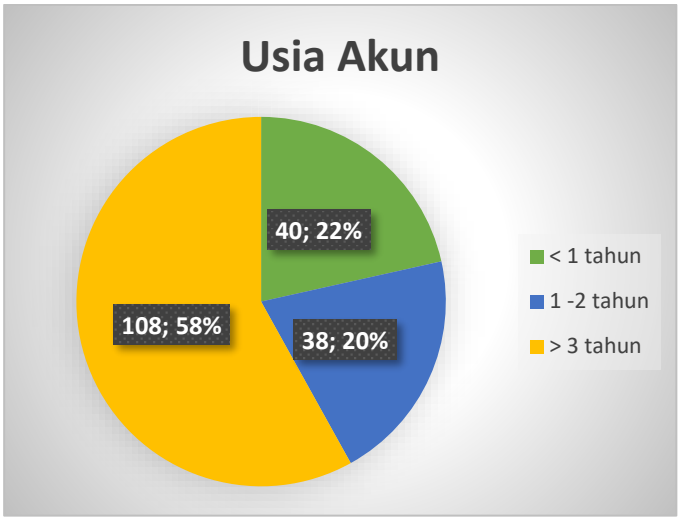
Gambar 4.2 Data Demografi Usia Responden

Data demografi jenis uang elektronik 186 responden menujukkan 3 orang (2%) adalah pengguna DANA, 8 orang (4%) adalah pengguna LinkAja, 72 orang (39%) adalah pengguna GoPay dan 103 orang (55%) adalah pengguna OVO seperti yang dijelaskan pada Gambar 4.3.



Gambar 4.3 Data Demografi Penerbit Uang Elektronik Responden

Data demografi usia akun uang elektronik 186 responden menujukkan 40 orang (22%) sudah memiliki akun selama kurang dari 1 tahun, 38 orang (20%) sudah memiliki akun selama 1 – 2 tahun, dan 108 orang (58%) sudah memiliki akun selama lebih dari 3 tahun seperti yang dijelaskan pada Gambar 4.4.



Gambar 4.4 Data Demografi Usia Akun Uang Elektronik Responden

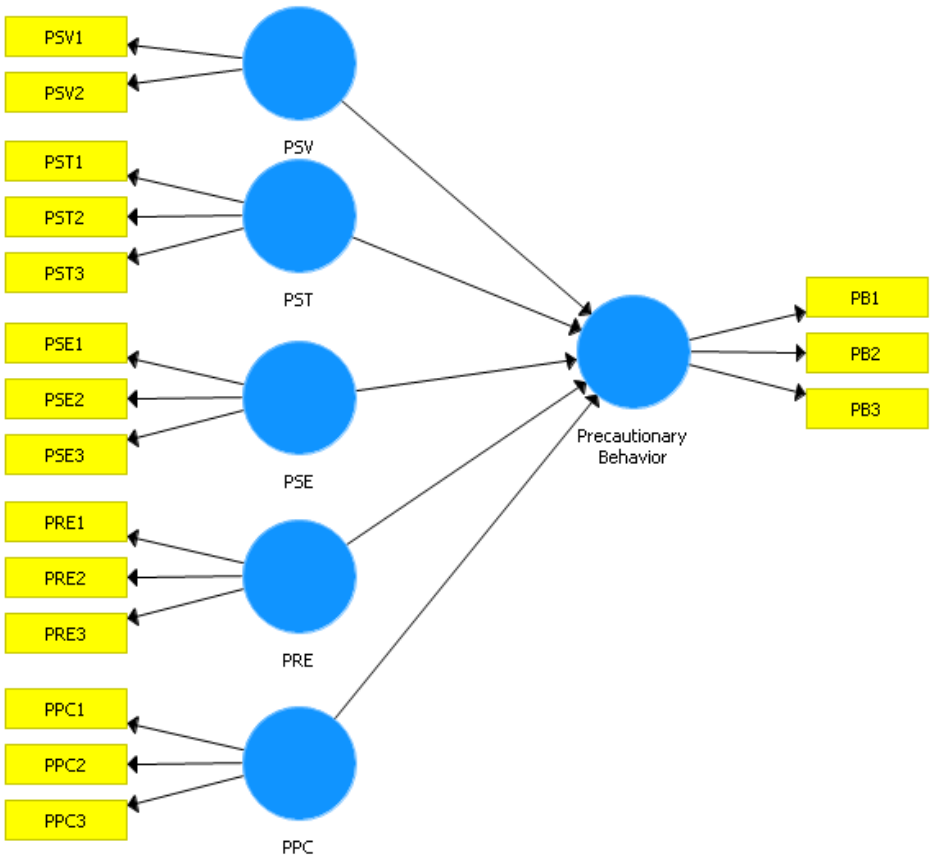
Rangkuman data demografi responden penelitian ini dapat dilihat pada Tabel 4.1 di bawah ini:

Tabel 4.1 Data Demografi Responden

No.	Karakteristik		Jumlah	Presentase
1.	Jenis Kelamin	Laki-laki	64	34%
		Perempuan	122	66%
	Total		186	100%
2.	Usia	< 18 tahun	2	1%
		19 – 37 tahun	167	90%
		38 – 58 tahun	17	9%
	Total		186	100 %
3.	Penerbit Uang Elektronik	Dana	3	2%
		LinkAja	8	4%
		GoPay	72	39%
		OVO	103	55%
	Total		186	100 %
4.	Usia Akun	< 1 tahun	40	22%
		1 – 2 tahun	38	20%
		> 3 tahun	108	58%
	Total		186	100 %

4.3. Analisis Data

Analisis dan pengolahan data responden menggunakan *Structural Equation Model* (SEM) berbasis *Partial Least Square* (PLS). Analisis data menggunakan aplikasi SmartPLS versi 3. Analisis PLS-SEM dilakukan dengan cara melakukan pengujian model pengukuran (*outer model*), model struktural (*inner model*) dan pengujian hipotesis. Gambar 4.5 menjelaskan diagram jalur dari model penelitian yang diestimasi. Diagram jalur dibuat sesuai dengan hipotesis dan model penelitian yang telah dibuat. Diagram jalur terdiri dari 6 variabel laten dan 17 indikator. Variabel laten digambarkan dengan bentuk lingkaran atau bulatan elips sedangkan indikator digambarkan dengan bentuk persegi. Variabel laten tersebut adalah PB (*precautionary behaviour*), PSV (*perceived securiy vulnerabilities*), PST (*perceived security threat*), PSE (*perceived self efficacy*), PRE (*perceived response efficacy*), dan PPC (*perceived prevention cost*).

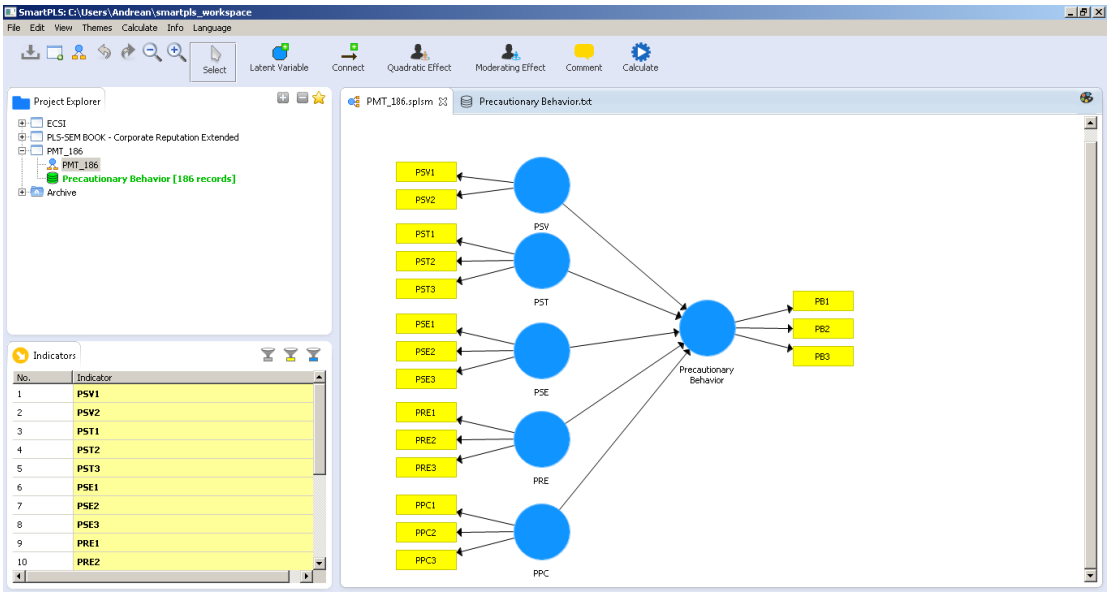


Gambar 4.5 Diagram Jalur

4.3.1. Pengujian model pengukuran (*outer model*)

Pengujian model pengukuran (*outer model*) dilakukan untuk mengukur hubungan antara indikator-indikator dengan variabel laten. Pengujian model pengukuran (outer model) dilakukan dengan melakukan uji validitas dan uji reabilitas. Setelelah pengujian ini baru dilakukan pengujian model struktural (*inner model*). Pengujian model pengukuran (*outer model*) pada Smart PLS 3 dengan langkah-langkah sebagai berikut:

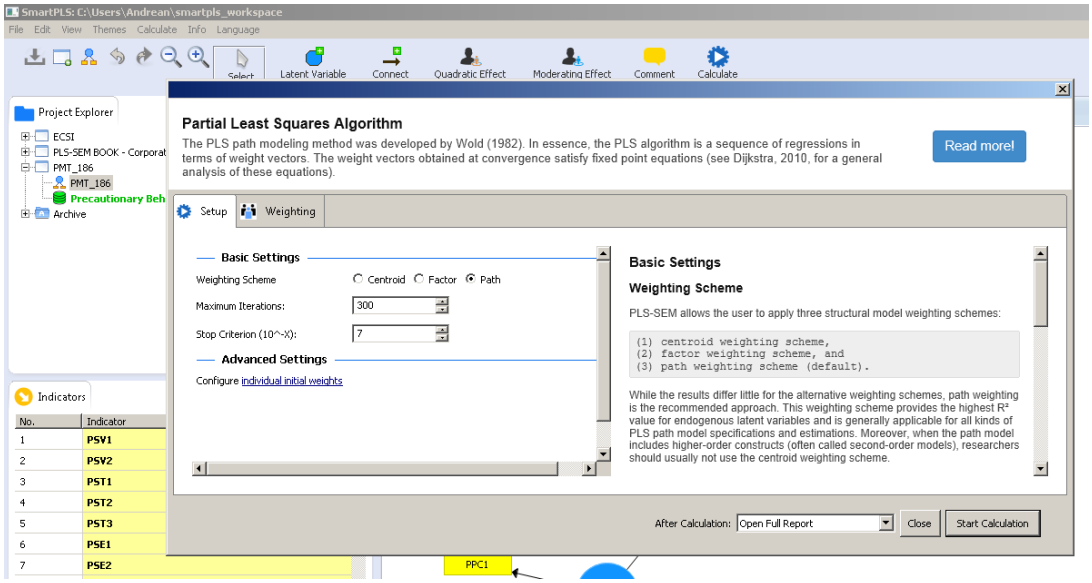
1. Pada *Main Window* Smart PLS 3 yang ditunjukkan Gambar 4.6 pilih *Calculate* kemudian *PLS Algorithm*.



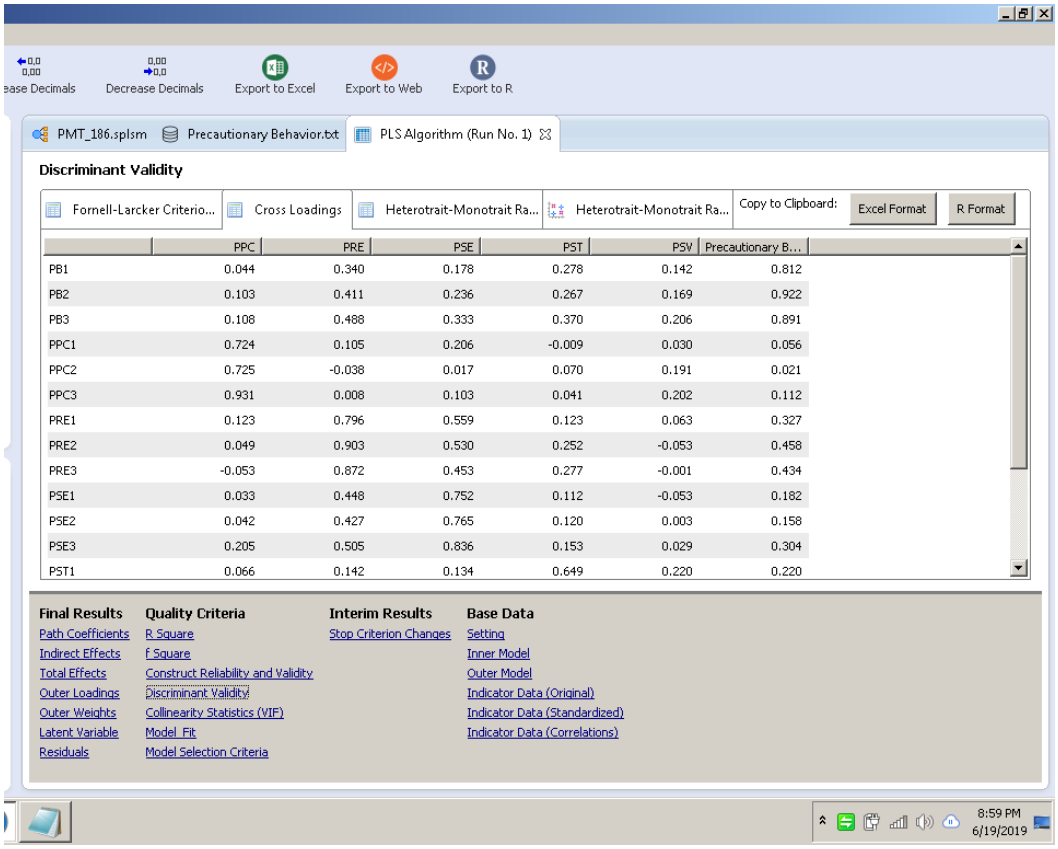
Gambar 4.6 *Main Window* Smart PLS

2. Gambar 4.7 menunjukkan *Window* baru *Partial Least Square Start Calculate*. Pada *Basic Setting* diatur sesuai dengan Gambar 4.7. *Weighting Scheme* merupakan pilihan default yang biasanya dipakai untuk pemodelan Smart PLS standar. *Maximum Iterations* merupakan jumlah iterasi maksimal, sedangkan *Stop Criterion* merupakan nilai kriteria agar iterasi berhenti dengan nilai yang disarankan Smart PLS adalah 7.
3. Setelah semua kriteria ditentukan maka dapat dimulai penghitungan dengan memilih *Start Calculation*.

4. Smart PLS akan melakukan penghitungan dan jika sudah selesai hasilnya dapat dilihat seperti pada Gambar 4.8. Hasil Pengujian model pengukuran (*outer model*) ada pada bagian *outer loadings*, *construct reliability* and *validity* (nilai AVE, *Cronbach's Alpha*, dan *Composite Reliability*), *discriminat validity* (*cross loadings*).



Gambar 4.7 Jendela Menu *PLS Alorithm*



Gambar 4.8 Hasil Penghitungan *Smart PLS Alorithm*

4.3.1.1. Uji Validitas

Uji validitas dilakukan dengan menguji *convergent validity* dan *discriminant validity*. Pengujian tersebut disebabkan model penelitan indikator bersifat reflektif (indikator disebabkan oleh konstruk). *Convergent validity* diuji dengan melihat nilai *loading factor* dan *average variance extracted* sedangkan *discriminant validity* diuji dengan menggunakan *cross loading*. Nilai ketiganya didapatkan dengan melalui Smart PLS pada bagian *outer loadings*, *construct reliability and validity* dan *discriminant validity*.

a. *Loading factor* (*Outer Loading*)

   Uji validitas *convergent* indikator reflektif dengan Smart PLS 3 diketahui dari nilai *loading factor* untuk setiap indikator konstruk. Nilai *loading factor* harus lebih besar dari 0,7 (Chin, 1998). Jika terdapat nilai kurang dari 0.7 maka indikator tersebut dianggap tidak valid sehingga harus dihapus dan dilakukan analisis ulang.

Tabel 4.2 Nilai *Outer Loadings*

	PPC	PRE	PSE	PST	PSV	Precautionary Behavior
PB1						0.812
PB2						0.922
PB3						0.891
PPC1	0.724					
PPC2	0.725					
PPC3	0.931					
PRE1		0.796				
PRE2		0.903				
PRE3		0.872				
PSE1			0.752			
PSE2			0.765			
PSE3			0.836			
PST1				0.649		
PST2				0.83		
PST3				0.891		
PSV1					0.878	
PSV2					0.858	

Tabel 4.2 merupakan keluaran hasil uji validitas *convergent* indikator reflektif dengan Smart PLS 3. Nilai *loading factor* indikator PST1 Tabel 4.2 kurang dari 0,7. Oleh karena itu indikator PST1 perlu dihapus. Setelah itu dilakukan analisis ulang melalui Smart PLS 3 dengan cara yang sama. Tabel 4.3 menjelaskan hasil uji validitas nilai *loading factor* menggunakan Smart PLS 3 setelah indikator PST1 dihapus. Semua indikator berhasil memenuhi syarat yaitu memiliki nilai *outer loadings* lebih dari 0,7.

Tabel 4.3 Nilai *Outer Loadings* tanpa PST1

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

b. *Average Variance Extracted* (*AVE*)

Validitas konvergen adalah seperangkat indikator yang mewakili satu variabel laten dan mendasari variabel laten tersebut. Perwakilan tersebut dijelaskan dengan menggunakan nilai rata-rata varian yang diekstrasi (AVE). Nilai AVE minimal sebesar 0,5. Nilai AVE menggambarkan validitas konvergen memadai dan satu variabel laten mampu menjelaskan lebih dari setengah varian dari indikator-indikatornya dalam rata-rata. Nilainya didapatkan dari Smart PLS 3 pada *construct reability and validity*. Hasilnya ditampilkan pada tabel 4.4 dimana semua konstruk memiliki nilai lebih besar dari 0,5 sehingga dinyatakan memenuhi syarat.

Tabel 4.4 Nilai AVE

	Average Variance Extracted (AVE)
PPC	0.64
PRE	0.737
PSE	0.617
PST	0.817
PSV	0.753
Precautionary Behavior	0.767

c. *Cross Loadings*

Cross loadings merupakan metode yang dipakai untuk mengukur *discriminat validity*. Indikator dinyatakan valid jika nilai *loading factor* yang dimilikinya sendiri lebih tinggi dibandingkan dengan nilai *loading factor* konstruk yang lain. Tabel 4.5 merupakan hasil *cross loading* dari Smart PLS 3 yang dinyatakan valid karena memenuhi syarat.

Tabel 4.5 Nilai *Cross Loadings*

	PPC	PRE	PSE	PST	PSV	Precautionary Behavior
PB1	0.044	0.34	0.178	0.248	0.142	0.808
PB2	0.103	0.411	0.236	0.246	0.169	0.921
PB3	0.108	0.488	0.333	0.381	0.206	0.894
PPC1	0.725	0.105	0.206	-0.024	0.03	0.056
PPC2	0.727	-0.038	0.017	0.051	0.191	0.022
PPC3	0.93	0.008	0.103	0.025	0.202	0.112
PRE1	0.123	0.796	0.559	0.115	0.063	0.327
PRE2	0.049	0.903	0.53	0.254	-0.053	0.459
PRE3	-0.053	0.872	0.453	0.278	-0.001	0.435
PSE1	0.033	0.448	0.753	0.104	-0.053	0.183
PSE2	0.042	0.427	0.765	0.138	0.003	0.159
PSE3	0.205	0.505	0.835	0.12	0.029	0.304
PST2	-0.001	0.196	0.136	0.893	0.168	0.293
PST3	0.028	0.272	0.136	0.914	0.125	0.325
PSV1	0.172	0.004	0.003	0.116	0.877	0.18
PSV2	0.135	-0.011	-0.004	0.164	0.858	0.168

4.3.1.2. Uji Reliabilitas

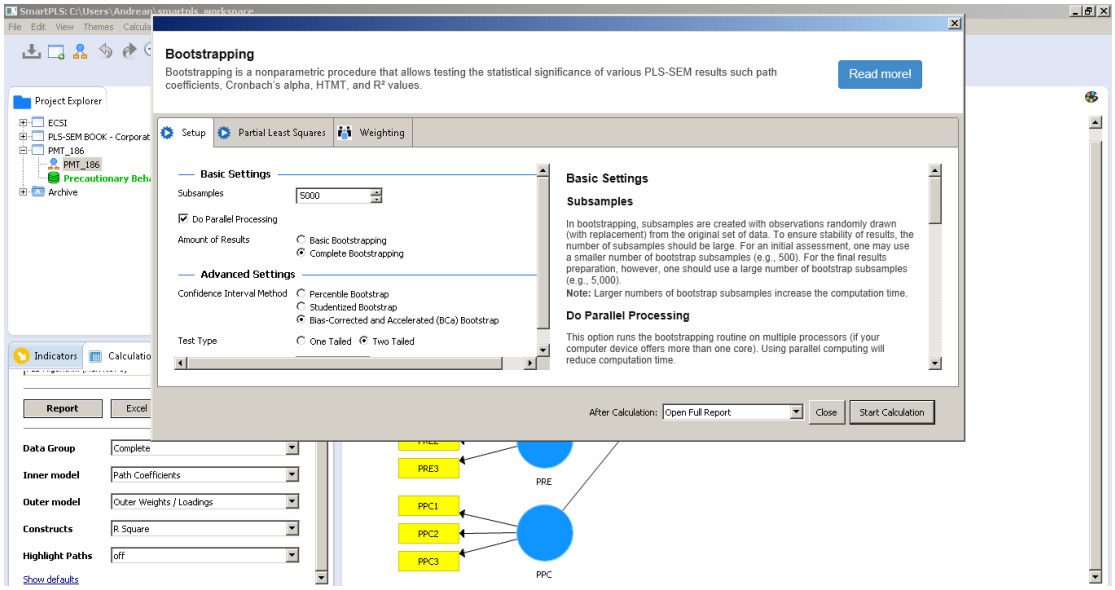
Suatu indikator dinyatakan reliabel atau andal jika jawaban yang diberikan reponden konsisten dan menghasilkan jawaban yang konsisten jika digunakan pada populasi yang berbeda. Tingkat konsistensi data terhadap indikator penelitian didapatkan melalui uji reliabilitas. Uji reliabilitas dilakukan oleh Smart PLS 3 dan dapat diketahui pada *composite reliability* dan *cronbach's alpha*. Suatu *outer model* dapat dianggap reliabel jika nilai *composite reliability* dan *cronbach's alpha* yang dimilinya lebih besar dari 0,6. Pada Tabel 4.6 merupakan keluaran dari Smart PLS 3 pada bagian *construct reliability and validity*. Pada Tabel 4.6 diketahui masing-masing *composite reliability* dan *cronbach's alpha* memiliki diatas 0,7. Hal ini dapat disimpulkan bahwa setiap indikator dapat diandalkan atau reliabel.

Tabel 4.6 Nilai *Composite Reliability dan Cronbach's Alpha*

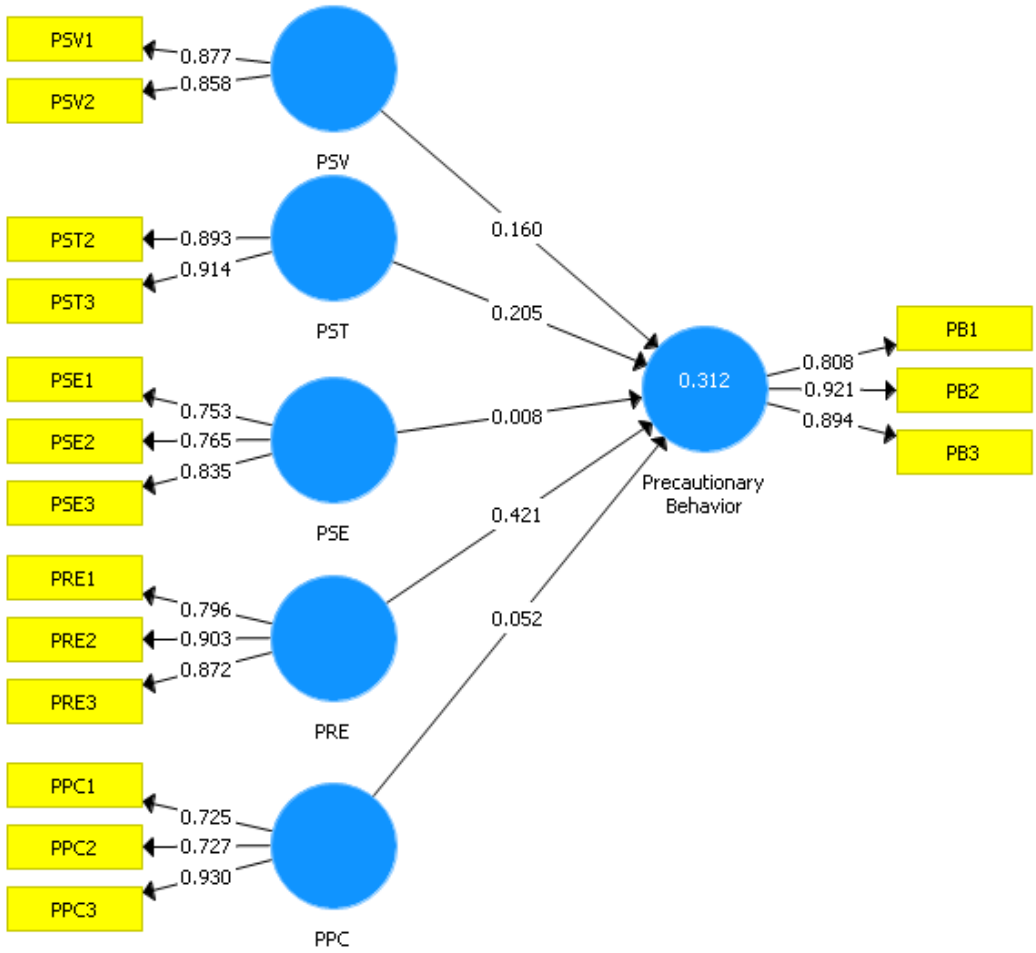
	Composite Reliability	Cronbach's Alpha
PPC	0.84	0.761
PRE	0.893	0.822
PSE	0.828	0.714
PST	0.899	0.776
PSV	0.859	0.672
Precautionary Behavior	0.908	0.85

4.3.2. Pengujian model struktural (*inner model*)

Model struktural adalah model yang menghubungkan antar variabel laten. Evaluasi model struktural dapat memprediksi hubungan kausal antar variabel laten. Pada Smart PLS untuk dapat melakukan pengujian model struktural perlu dilakukan *bootsrapping* dengan mengambil jumlah subsampel sebesar 5000 untuk menilai *significance of path coefficients* dengan test type yaitu *two tailed*. Kemudian akan diketahui nilai koefisiensi determinasi (R^2) untuk variabel dependen dan nilai *coefficient path* untuk variabel independen. Nilai signifikansinya kemudian dinilai berdasarkan nilai *t-statistics* setiap *path*. Prosedur tersebut dilakukan dengan cara memilih *Calculate* kemudian *Bootstrapping*. Gambar 4.9 merupakan jendela pengaturan *bootsrapping* yang diatur sesuai pengaturan yang sudah ditentukan sebelumnya. Hasil *bootstrapping* dapat dilihat pada Gambar 4.10.



Gambar 4.9 Pengaturan *Bootstrapping*



Gambar 4.10 Diagram Jalur Hasil *Bootstrapping*

a. *Path Coefficients*

Uji *path coefficients* dilakukan guna melihat hubungan antar variabel laten. Hubungan antar variabel laten dianggap signifikan jika memiliki *t-statistics* lebih besar dari 1,96 dengan *significance level* = 5% (Ghozali, 2008). Hasil uji *path coefficients* pada Smart PLS ditunjukkan Tabel 4.7. Pada Tabel 4.7 diketahui terdapat 3 jalur yang memenuhi syarat signifikansi yaitu PRE, PST, dan PSV sedangkan 2 jalur yang tidak memenuhi syarat yaitu PPC dan PSE.

Tabel 4.7 Hasil Uji Path Coefficients

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Value	Significance (p < 0,05)
PSV -> Precautionary Behavior	0.16	0.164	0.073	2.207	0.027	Ya
PST -> Precautionary Behavior	0.205	0.207	0.061	3.367	0.001	Ya
PSE -> Precautionary Behavior	0.008	0.025	0.088	0.086	0.932	Tidak
PRE -> Precautionary Behavior	0.421	0.413	0.088	4.767	0	Ya
PPC -> Precautionary Behavior	0.052	0.055	0.086	0.61	0.542	Tidak

b. *R Square*

Tabel 4.8 menjelaskan nilai R^2 adalah 0,312. Nilai *R square* atau R^2 digunakan untuk mengukur tingkat variasi perubahan variabel independen terhadap variabel dependen. Jika nilai R^2 semakin tinggi maka semakin baik model prediksi yang diuji. Nilai R^2 dianggap lemah jika nilainya 0,19, dianggap moderat jika nilainya 0,33, dan dianggap kuat jika nilainya 0,67 (Ghozali dan Latan, 2012). Pada penelitian ini nilai R^2 atau koefesien determinasi tergolong

lemah dengan nilai yang didapatkan adalah 0,312. Oleh karena itu dapat disimpulkan bahwa kelima variabel tersebut hanya mampu menjelaskan 31,2% variabel dependen dan sisanya dijelaskan oleh variabel lain yang tidak ada dalam penelitian ini.

Tabel 4.8 Hasil Uji *R Square*

	Original Sample (O)
Precautionary Behavior	0.312

4.3.3. Pengujian hipotesis

Pengujian Hipotesis dilakukan dengan melihat nilai *t-statistics* dan *significance level* atau juga dengan melihat nilai probabilitas *p-value*. Nilai *t-statistics* yang diharapkan harus lebih besar dari 1,96 dengan *significance level* = 5%. Sedangkan, nilai probabilitas *p-value* dengan *alpha* 5% (0,05) adalah kurang dari 0,05. Sehingga kriteria penerimaan Hipotesis adalah ketika *t-statistics* > *t table* (1,96) dan p-value kurang dari *alpha* 5% (0,05). Tabel 4.9 menunjukkan hasil pengujian hipotesis Smart PLS 3, dimana terdapat 3 hipotesis diterima yaitu, PSV, PST, PRE dan 2 hipotesis ditolak yaitu PSE dan PPC.

Tabel 4.9 Hasil Pengujian Hipotesis

Hipotesis	PATH	Path Coefficients	T Statistics (|O/STDEV|)	P Values	Kesimpulan
H1	PSV -> PB	0.16	2.207	0.027	Diterima
H2	PST -> PB	0.205	3.367	0.001	Diterima
H3	PSE -> PB	0.008	0.086	0.932	Ditolak
H4	PRE -> PB	0.421	4.767	0	Diterima
H5	PPC -> PB	0.052	0.61	0.542	Ditolak

Pada Tabel 4.9 menunjukkan hipotesis H1 diterima. Hipotesis diterima berdasarkan hasil pengujian *path coeffecients* pada Smart PLS 3 dimana nilai *t statistics* > 1,96 dan *p value* < 0,05. Dengan demikian, *perceived security vulnerabilites* secara positif mempengaruhi individu melakukan *precautionary behavior*. Hipotesis ini didukung juga oleh penelitian lain yaitu Woon et all (2005), Boerman et all (2018), dan Ophoff et all (2019). Hal ini menyiratkan jika individu

dipaparkan bagaimana ancaman keamanan informasi dilakukan maka individu tersebut akan semakin memiliki kecenderungan untuk melakukan tindakan perlindungan.

Pada Tabel 4.9 menunjukkan hipotesis H2 diterima. Hipotesis diterima berdasarkan hasil pengujian *path coeffecients* pada Smart PLS 3 dimana nilai *t statistics* > 1,96 dan *p value* < 0,05. Dengan demikian, *perceived security threat* secara positif mempengaruhi individu melakukan *precautionary behavior*. Hipotesis ini didukung juga oleh penelitian lain yaitu Yoon et all (2012) dan Ophoff et all (2019). Hal ini menyiratkan jika individu dipaparkan bagaimana dampak kejahatan keamanan informasi dilakukan maka individu tersebut akan semakin memiliki kecenderungan untuk melakukan tindakan perlindungan.

Pada Tabel 4.9 menunjukkan hipotesis H3 ditolak. Hipotesis ditolak berdasarkan hasil pengujian *path coeffecients* pada Smart PLS 3 dimana nilai *t statistics* < 1,96 dan *p value* > 0,05. Dengan demikian, *perceived security self efficacy* secara positif tidak mempengaruhi individu melakukan *precautionary behavior*. Hal ini menyiratkan bahwa individu tidak yakin pada kemampuan dirinya sendiri untuk menjalankan panduan keamanan. Penelitian Boerman et all (2018) juga menemukan hal yang sama, yang menurutnya dikarenakan karena individu tidak benar-benar memahami bagaimana menjalankan perilaku perlindungan harus dilakukan. Sedikitnya pemahaman nampaknya mempengaruhi kepercayaan diri individu untuk melakukan perilaku perlindungan.

Pada Tabel 4.9 menunjukkan hipotesis H4 diterima. Hipotesis diterima berdasarkan hasil pengujian *path coeffecients* pada Smart PLS 3 dimana nilai *t statistics* > 1,96 dan *p value*. Dengan demikian, *perceived response efficacy* secara positif mempengaruhi individu melakukan *precautionary behavior*. Hipotesis ini didukung juga oleh penelitian lain yaitu Woon et all (2005) dan Tsai et all (2010). Hal ini menyiratkan jika individu meyakini perilaku perlindungan dapat berhasil melindungi individu dari kejahatan keamanan informasi, maka individu tersebut akan semakin memiliki kecenderungan untuk melakukan tindakan perlindungan.

Pada Tabel 4.9 dapat diketahui bahwa hipotesis H5 ditolak. Hipotesis ditolak berdasarkan hasil pengujian *path coeffecients* pada Smart PLS 3 dimana

nilai *t statistics* < 1,96 dan *p value* > 0,05. Dengan demikian, *perceived prevention cost* tidak mempengaruhi individu melakukan *precautionary behavior*. Hasil yang sama dengan Crossler (2010) ini menyiratkan bahwa persepsi beban pada usaha untuk melakukan *precautionary behavior* memang tidak memiliki dampak signifikan. Hal ini merupakan hal yang positif karena tidak ditemukan persepsi beban terhadap respon pencegahan sehingga kemungkinan besar pengguna akan melakukannya.

4.4. Pembuatan *User Awareness*

Tujuan utama dari pembuatan *awareness program* adalah mengedukasi pengguna agar dapar menghindari atau melaporkan ancaman, bukan menjadi ahli atau profesional. Tujuan tersebut dapat dipenuhi pertama-tama dengan memastikan pengguna mengenali ancaman yang dihadapi, beserta pelaku dan motif kejahatan. Selain itu juga memastikan pengguna memahami nilai dari informasi pribadinya. Hal ini dapat dicapai melalui proses dan perubahan perilaku (Gardner & Thomas 2014).

Penelitian ini merancang *user awareness* menggunakan kerangka kerja NIST 800-50 dengan memakai pendekatan faktor-faktor yang ada pada *precautionary behavior*. Faktor-faktor tersebut merupakan variabel pada pengujian hipotesis yang dilakukan sebelumnya. Hasil pengujian tersebut mendapatkan *perceived security vulnerabilities, perceived security threat,* dan *perceived response efficacy* yang walaupun memiliki pengaruh positif pada pengujian hipotesis namun hanya menjelaskan 31,2% *precautionary behavior*. Sisanya dijelaskan oleh variabel lain yang tidak ada pada penelitian ini.

Perancangan *user awareness* menggunakan tahapan-tahapan kerangka kerja NIST 800-50. Akan tetapi tidak semua tahapan pada NIST 800-50 dilakukan sepenuhnya. Hal ini dikarenakan penelitian ini hanya mencakup *user awareness*. Adapun kerangka kerja NIST 800-50 juga menjelaskan pembuatan pelatihan (*user training*). Kerangka kerja NIST 800-50 dipergunakan agar *user awareness* dapat dibuat secara optimal, terstruktur, dapat dengan mudah diintegrasikan dengan *protection motivation theory*, dapat dipertanggungjawabkan karena dibuat menggunakan kerangka kerja yang disusun oleh para ahli, dan mempunyai manfaat

di masa mendatang karena dapat diulang untuk untuk topik lain yang berbeda (*replicabilitiy*). *User awareness* dibuat dengan menggunakan referensi berupa data demografi responden penelitian sebagai populasi sasaran. Hasil penelitian ini diharapkan dapat dipertimbangkan dan dipakai oleh penerbit uang elektronik menyusun *user awareness* keamanan informasi untuk pengguna uang elektronik.

4.4.1. *Awarenesss Program Design*

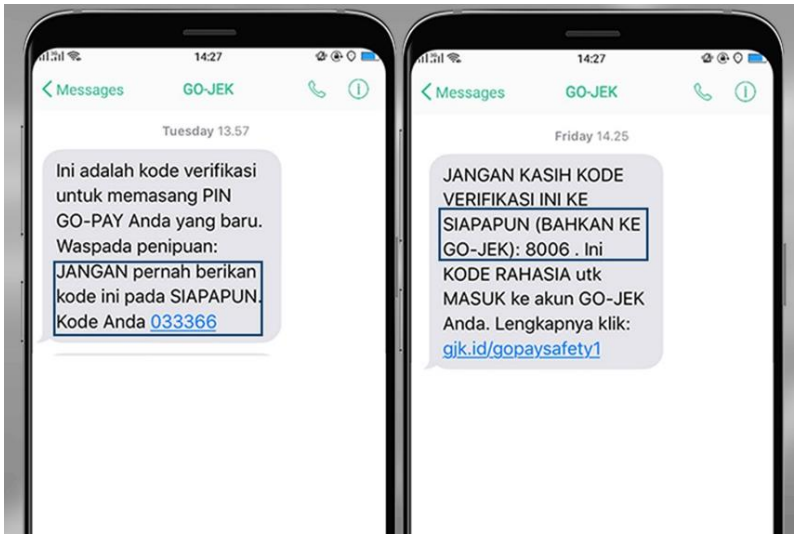
Awareness program design adalah proses perancangan awal. Proses perancangan harus dapat menjawab tujuan *user awareness*, mengalihkan fokus *audience* kepada masalah keamanan dan membuat respon yang sesuai. Proses desain juga harus dapat menilai kebutuhan dan menjawab pertanyaan-pertanyaan mendasar pembuatan *user awareness*.

4.4.1.1. *Existing*

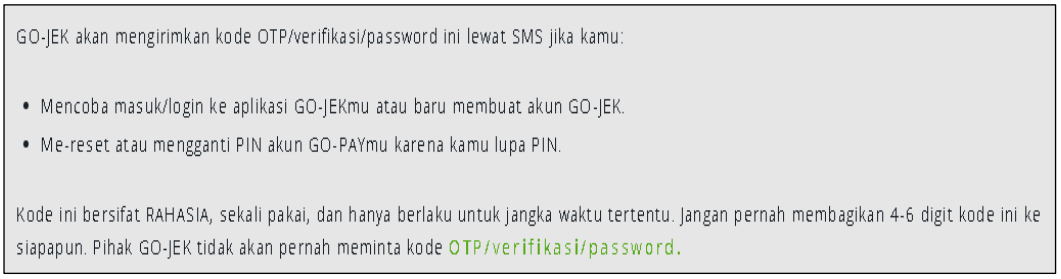
Existing atau bentuk *user awareness* yang sudah dibuat oleh penerbit uang elektronik. Gambar 4.7 sampai dengan 4.9 menjelaskan contoh *user awareness* yang sudah dibuat OVO dan GoPay. *User awareness* yang dibuat oleh OVO pada Gambar 4.7 menjelaskan 2 langkah keamanan dan tips penggunaan. Gambar ini didapatkan dari iklan, sosial media OVO serta *pop up messsage* pada aplikasi OVO. Gambar 4.7 menjelaskan aplikasi OVO yang dilindungi fungsi keamanan 2 langkah yaitu *security code* untuk masuk dan bertransaksi serta *One Time Password* (OTP) yang dikirim melalui SMS. Kedua langkah keamanan tersebut merupakan bentuk perlindungan data pengguna. Gambar 4.7 juga menjelaskan tips menggunakan OVO. Gambar 4.7 juga menjelaskan panduan pencegahan agar pengguna terhindar dari penipuan (*phising*).

Gambar 4.11 Contoh *User Awareness* OVO

Pada situs www.go-jek.com/go-pay terdapat artikel keamaanan transaksi GoPaY yang diberi judul *ALWAYS KEEP YOUR GO-PAY SAFE*. Judul tersebut memiliki 3 artikel yang berisi *Lima Cara Mudah Melindungi Akun GO-PAY*, *Lindungi akun GO-JEK kamu, jangan berikan kode verifikasi ke siapa pun!* dan *Pasang PIN untuk Keamanan GO-PAY*. Pada ketiga artikel tersebut dijelaskan dengan detail langkah keamanan untuk melindungi pengguna. Gambar 4.8 dan 4.9 contoh *user awareness* yang sudah dibuat oleh GoPay. Ketiga artikel tersebut memiliki isi yang kurang lebih sama yaitu memberikan langkah-langkah kepada pengguna untuk melindungi akunnya serta memberikan panduan pencegahan agar pengguna terhindar dari penipuan (*phising*).



Gambar 4.12 Contoh *User Awareness* GoPay (1)


GO-JEK akan mengirimkan kode OTP/verifikasi/password ini lewat SMS jika kamu:

- Mencoba masuk/login ke aplikasi GO-JEKmu atau baru membuat akun GO-JEK.
- Me-reset atau mengganti PIN akun GO-PAYmu karena kamu lupa PIN.

Kode ini bersifat RAHASIA, sekali pakai, dan hanya berlaku untuk jangka waktu tertentu. Jangan pernah membagikan 4-6 digit kode ini ke siapapun. Pihak GO-JEK tidak akan pernah meminta kode OTP/verifikasi/password.

Gambar 4.13 Contoh *User Awareness* GoPay (2)

4.4.1.2. *Scope of the awareness*

Scope of the awareness atau ruang lingkup *user awareness* dimana akan dilandaskan pada *protection motivation theory*. Pendekatan *protection motivation theory* sebagai landasan pembuatan *user awareness* pernah dicontohkan sebelumnya oleh LaRose et all (2008). Pada bagian sebelumnya telah dilakukan pengujian pada faktor-faktor yang mempengaruhi pengguna melakukan *precautionary behavior* pengguna uang elektronik. Pengujian pada responden menghasilkan penerimaan hipotesis faktor-faktor yang mempengaruhi pengguna melakukan *precautionary behavior* pengguna uang elektronik yaitu *perceived security vulnerabilities, perceived security threat,* dan *perceived response efficacy*. Ruang lingkup *perceived security vulnerabilities* yaitu bagaimana kejahatan uang elektronik untuk dapat melakukan penilaian kerentanan. Ruang lingkup *perceived security threat* yaitu menjelaskan dampak kejahatan uang elektronik. Ruang lingkup *perceived response efficacy* adalah keberhasilan *precautionary behavior* yaitu menjalankan panduan keamanan uang elektronik.

4.4.1.3. *Goals to be accomplished*

Goals to be accomplished atau tujuan yang ingin dicapai. Tujuan yang ingin dicapai harus dapat menjawab *scope of the awareness* yang disesuaikan dengan setiap hipotesis yang diterima. Hipotesis yang diterima adalah *perceived security vulnerabilities, perceived security threat,* dan *perceived response efficacy*. Tujuan *perceived security vulnerabilities* adalah menjelaskan bagaimana kejahatan uang elektronik dilakukan untuk menekankan pesan kerentanan sehingga pengguna memiliki persepsi kerentanan dengan cara menilai seberapa rentan dirinya jika dihadapkan pada ancaman. Tujuan *perceived security threat* adalah menekankan pesan dampak kejahatan uang elektronik sehingga pengguna memiliki persepsi keparahan (*severity*). Tujuan *perceived response efficacy* adalah menekankan pesan keberhasilan *precautionary behavior* yaitu panduan keamanan. Pesan tersebut membantu pengguna memiliki persepsi bahwa dengan menjalankan panduan keamanan akan dapat melindungi dirinya dari kejahatan uang elektronik.

4.4.1.4. *Target audience*

Target audience atau kepada siapa *user awareness* ditujukan. *Target audience* dari *user awareness* adalah pengguna uang elektronik. Data demografis

penelitian ini menunjukkan bahwa populasi berusia 19-37 tahun, 90% dari total populasi. Klasifikasi umur tersebut menurut Brosdahl and Carpenter's (2011) merupakan *Gen Y* atau *The Millennials* yang lahir diantara 1982-2000, memiliki rentan usia 19-37 tahun pada 2019. Generasi Y memiliki karakteristik tersendiri dalam menerima dan memproses informasi. Bolton, et all (2013) menyatakan bahwa generasi Y adalah generasi yang lahir dimana teknologi sudah berada di lingkungannya (*digital natives*). Generasi Y bukan merupakan generasi yang lahir dimana teknologi belum berkembang (*digital imigrants*). Penerbit uang elektronik dalam membuat *user awareness* perlu melakukan penyesuaian pada bagaimana *user awareness* disampaikan dan dibahasakan agar sesuai target *audience*. Hal tersebut dikarenakan perihal keamanan informasi adalah perihal manusia dibanding perihal teknis.

Data demografis lain penelitian ini menunjukkan bahwa 58% populasi (108 orang) dari populasi sudah lebih dari 3 tahun memakai uang elektronik dan 42 % (78 orang) dibawah 3 tahun. Secara tersirat hal ini menunjukkan terdapat kenaikan jumlah pengguna pada 2 tahun terakhir. Kenaikan ini menunjukkan adanya pengguna baru atau pengguna pemula. Pengguna pemula dengan usia akun dibawah 3 tahun inilah yang dapat juga dijadikan *target audience* utama. Hal ini perlu dilakukan karena menurut laporan dari *European Payment Council*, target utama pelaku kejahatan keamanan informasi adalah pengguna pemula.

4.4.1.5.*Mandatory*

Mandatory atau kebijakan untuk merancang *user awareness* sebagai sebuah kewajiban. Kondisi saat ini, belum ada *user awareness* penerbit uang elektonik yang bersifat *mandatory*. *User awareness* tidak bersifat wajib untuk dilihat, seperti milik OVO, pengguna punya pilihan untuk melihat *user awareness* lebih lanjut atau mengabaikannya. Hal ini tentu kurang efektif. Sebaiknya *user awareness* bersifat *mandatory* atau wajib namun tetap disampaikan dengan tepat dan wajar. Hal ini guna menghindari pengguna terkena *privacy fatigue*. Jika bersifat *mandatory*, frekuensi pelaksanaanya setiap 6 bulan atau 1 tahun sekali. Pelaksanaanya dapat sebaiknya dilakukan dalam momen tertentu misalnya, *awareness security month*.

Sementara yang sifatnya rutin bisa berbentuk *pop up message* atau juga dengan menggunakan *newsletter*.

4.4.1.6. Topics to be addressed

Topics to be addressed atau topik *user awareness* yang akan disampaikan sesuai dengan setiap hipotesis yang diterima. Topik *perceived security vulnerabilities* menjelaskan bagaimana kejahatan uang elektronik dilakukan. Topik *perceived security threat* menjelaskan dampak jika menjadi korban kejahatan uang elektronik. Topik *perceived response efficacy* menjelaskan panduan keamanan dapat melindungi pengguna dari kejahatan uang elektronik.

4.4.1.7. *Frequency*

Frequency atau jumlah siklus *user awareness* disampaikan dalam satu waktu tertentu. *User awareness* memiliki sifat berkelanjutan, artinya harus dilakukan terus-menerus. Akan tetapi perlu diperhatikan frekuensi *user awareness* diberikan kepada pengguna uang elektronik. Pengguna dapat dengan mudah merasa lelah pada prosedur keamanan dan proses didalamnya. Prosedur keamanan dan *user awareness* yang disampaikan terus-menerus dapat menimbulkan persepsi jika menjalankan prosedur keamanan adalah beban (Bada dan Sasse, 2014). Frekuensi yang berlebihan menjadikan *user awareness* sampah informasi serta menyebabkan pengguna apatis karena terus-menerus disampaikan. Akan tetapi, di lain sisi frekuensi penyampaian yang terlalu jarang akan mengakibatkan *user awareness* tidak efektif. Jarak waktu penyampaian *user awareness* yang terlalu jauh akan membuat pengguna mudah melupakannya. Selain itu, pemilihan waktu yang tepat juga perlu menjadi perhatian dan bahan pertimbangan.

4.4.2. Developing Awareness Material

Tahapan ini membantu penyusunan *supporting material* dengan tujuan pengguna memiliki kemampuan untuk melakukan perilaku perlindungan yang diharapkan. Pemilihan *supporting material* juga harus spesifik, personal, menarik dan kekinian sehingga tidak menjadi formalitas belaka.

4.4.2.1. *Selecting awareness*

Selecting awareness atau memilih topik spesifik dari setiap hipotesis yang diterima. Proses pemilihan topik yang spesifik berguna untuk menggugah pengguna

merasa terhubung dengan permasalahan. Topik yang dapat membuat pengguna merasa terhubung lebih mudah menarik perhatian pengguna untuk menyimak *user awareness*.

Topik spesifik *perceived security vulnerabilities* adalah *social engineering* yaitu *phising* dan *malware*. Pemilihan *social engineering* dan *mobile malware* didasarkan pada laporan yang diterbitkan oleh European Payments Council yaitu *2018 Payment Threats And Fraud Trends Report*. European Payments Council setiap tahunnya melaporkan tren ancaman keamanan terkini. Laporan European Payments Council menyatakan ancaman keamanan informasi melalui *social engineering* dan *malware* masih berkontribusi besar pada sejumlah kerugian bahkan semakin signifikan.

a. *Social engineering*

Social engineering merupakan metode penyusupan non teknis yang digunakan untuk mengelabui pengguna agar menyerahkan informasi kredensial dari perangkat atau sistem yang dimiliki atau bahkan menginfeksi *malware*. *Social engineering* memanfaatkan berbagai media seperti surel, pesan singkat, panggilan telepon, dan media sosial. Pelaku memakai *social engineering* dikarenakan lebih mudah untuk mengeksploitasi kecenderungan alami manusia untuk mempercayai dibandingkan menemukan celah keamanan sebuah perangkat lunak. Contoh serangan *social engineering* yang umumnya dilakukan adalah *phishing* melalui surel, media sosial, dan pesan singkat serta *vishing* (*voice and phishing*) melalui panggilan telepon langsung. Skenario umum *phishing* dilakukan pelaku dengan mengirim surel kemudian berpura-pura sebagai pihak resmi / penerbit uang elektronik. Pelaku kemudian meminta calon korbannya untuk memverifikasi informasi dengan cara mengeklik tautan yang berisi formulir informasi pengguna. Jika calon korban tidak teliti dan mengisi formulir pada tautan tersebut maka pelaku akan mendapatkan informasi pribadi pengguna. Modus serupa berupa pesan yang menyatakan bahwa penerima surel adalah pemenang kuis atau undian dan harus memverifikasi data dengan mengeklik sebuah tautan. *Vishing* pada umumnya juga memakai modus yang sama dengan phising namun dengan media telepon. Pelaku menyamar sebagai

pihak resmi yang meminta pengguna memberikan kode OTP yang dikirim melalui pesan singkat. Pada umumnya kode OTP dikirimkan kepada pengguna oleh sistem saat mencoba masuk ke akun aplikasi uang elektronik atau mengganti PIN akun uang elektronik.

b. *Mobile malware*

Malware atau *malicious software* adalah istilah yang dipakai untuk perangkat lunak yang menyusup pada sebuah sistem operasi atau perangkat lunak. Pelaku kejahatan merancang malware untuk merusak fungsi tertentu sebuah perangkat, memotong kontrol akses keamanan serta mencuri data dan mengirimkannya tanpa diketahui pemilik perangkat. *Mobile malware* adalah *malware* yang menyerang perangkat seperti ponsel pintar. *Mobile malware* biasanya disusupkan pada sebuah tautan yang otomatis terunduh jika diklik oleh pengguna. Sebuah laporan dari China menunjukkan bahwa *mobile malware* disusupkan pada QR Code, saat pengguna memindai QR Code maka secara otomatis juga mengunduh *mobile malware* yang kemudian menginfeksi ponsel pintar pengguna.

Topik terkait dampak kejahatan uang elektronik belum diteliti dan dilaporkan secara empiris. Selain karena jumlah kasus yang belum banyak juga karenakan keengganan korban untuk melapor. Laporan yang paling mendekati adalah catatan Lembaga Studi dan Advokasi Masyarakat (ELSAM) pada 2017. ELSAM melaporkan 33 kasus penyalahgunaan data pribadi sepanjang 2013 sampai 2017. Akan tetapi bukan berarti kemungkinan kejahatan uang elektronik kecil dan bisa diabaikan.

Topik *perceived security threat* yang dibahas adalah dampak yang akan diterima jika menjadi korban kejahatan uang elektronik. Secara umum ada dua dampak yang mengakibatkan kerugian oleh pengguna uang elektronik. Kedua dampak tersebut terkait dengan akun uang elektronik, data dan informasi pribadi pengguna.

a. Kehilangan Akun uang elektronik

Tujuan pelaku kejahatan melakukan *phising* adalah mendapakatkan *login information* dari akun uang elektronik. *Phising* dilakukan dengan

memanfaatkan kode OTP (*One Time Password*) untuk mengubah kata sandi pengguna. Begitu OTP didapatkan, pelaku dapat mengganti *login information* pengguna yaitu *username* dan *password*. Setelah itu pelaku akan mendapat akses seluas-luasnya terhadap akun uang elektronik korban beserta saldo dan semua keuntungan finansial yang ada pada akun uang elektronik tersebut.

b. Pencurian Data dan Informasi Pribadi Pengguna

Ponsel pintar pada umumnya memiliki data dan informasi pribadi pengguna. Ponsel pintar yang terinfeksi *mobile malware* tanpa diketahui dapat mengirim data dan informasi pribadi pengguna melalui internet. Data dan informasi pribadi pengguna tersebut dapat dijual kepada pihak ketiga atau dipakai untuk melakukan kejahatan. Selain itu informasi kredensial perbankan yang mungkin ada pada ponsel pintar juga terancam kerahasiannya.

Topik *perceived response efficacy* adalah penjelasan keberhasilan panduan keamanan uang elektronik menghindarkan pengguna menjadi korban kejahatan uang elektronik. *Perceived response efficacy* adalah persepsi pengguna terhadap penilaian respon (*coping appraisal*), bagaimana perilaku yang disarankan dapat berhasil menghindarkan pengguna dari ancaman kejahatan uang elektronik. Oleh karena itu topik pembahasan adalah cara-cara yang dapat dipakai pengguna untuk melindungi dirinya dari kejahatan uang elektronik. Topik pembahasan tersebut harus menekankan pesan keberhasilan sehingga pengguna dapat mempercayainya kemudian mempengaruhi pengguna melakukan melakukan *precautionary behavior*. Laporan European Payments Council yaitu *2018 Payment Threats And Fraud Trends Report* memberikan topik panduan keamanan.

a. Menjaga Login Information

Secara umum *login information* biasanya didapatkan dengan menipu pengguna (*phising*). *Login information* adalah informasi yang digunakan pengguna untuk masuk ke dalam akun miliknya. *Login information* uang elektronik berupa nomer telepon, alamat surat elektronik (surel), kata sandi (PIN), dan kode OTP tidak boleh diberitahukan kepada siapapun termasuk kepada pihak-pihak yang berusaha meminta dan mengaku sebagai petugas resmi penerbit uang elektronik.

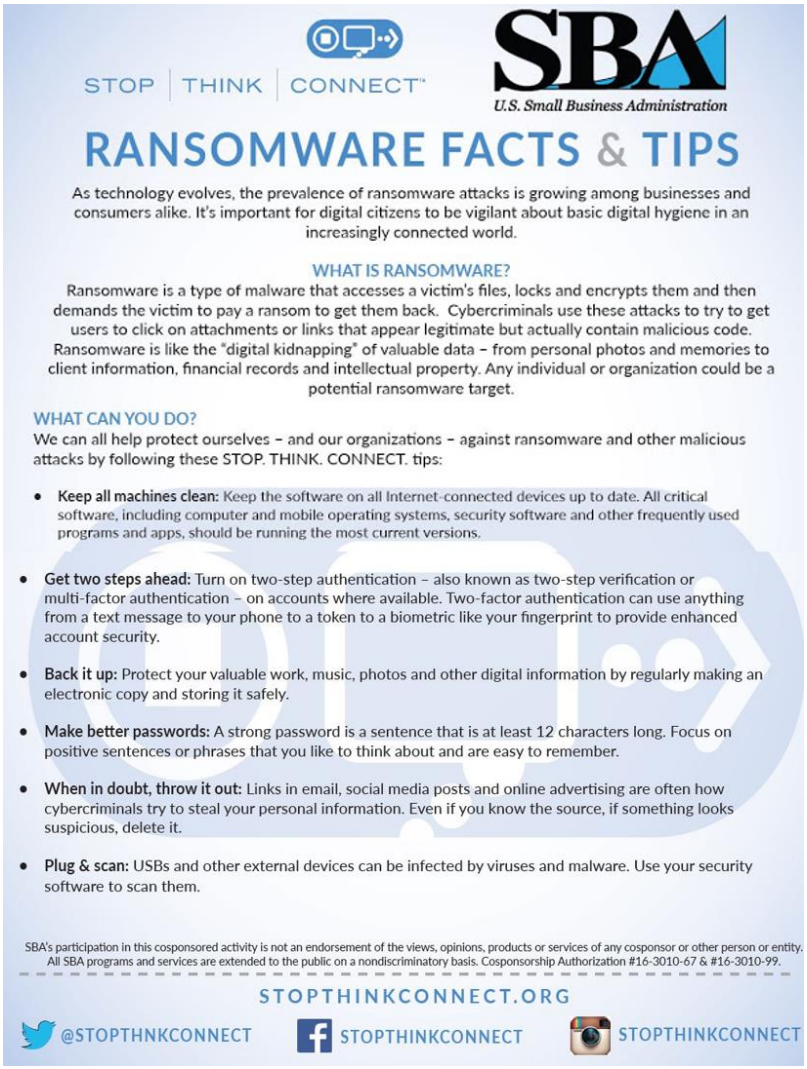
b. Menjaga Keamanan Ponsel Pintar

Keamanan ponsel pintar merupakan kunci utama perlindungan karena merupakan media yang berperan layaknya dompet bagi uang elekronik. Secara fisik, keamanan ponsel pintar dapat dilakukan dengan mengunci ponsel pintar dengan sandi angka, pola atau sidik jari agar tidak sembarang orang dapat memakai ponsel pintar tersebut. Sedangkan untuk dapat melindungi ponsel pintar dari acaman *malware* adalah dengan selalu melakukan pembaruan aplikasi uang elektronik untuk mendapatkan *security patches* terbaru. Kemudian selalu memasang aplikasi resmi yang sudah terverifikasi *App Store* dan *Play Store* serta memiliki antivirus yang selalu diperbarui juga adalah sebuah keharusan.

4.4.2.2.*Source of awareness material*

Source of awareness material atau penyertaan referensi tambahan yang relevan. Ada banyak sumber material *security awareness* yang dapat dihubungkan pada program *user awareness*. Materi pendukung harus dapat mendukung penjelasan isu spesifik dan memberikan panduan penyusunan *user awareness*.

Materi pendukung dapat juga diambil dari situs-situs keamanan informasi seperti, www.staysafeonline.info dan www.isafe.org. Kedua situs tersebut adalah menyediakan materi, infografis dan panduan untuk mempromosikan kesadaran keamanan informasi. Kedua situs tersebut dikelola masing-masing oleh *National Cyber Security Alliance* dan *U.S. Department of Justice*. Gambar 4.10 adalah contoh *user awareness* yang dibuat oleh situs *staysafe.org* melalui kampanye *Stop Think Connect*.. *User awareness* Gambar 4.10 menjelaskan *ransomware*, dampak jika terinfeksi *ransomware*, serta bagaimana pengguna dapat melindungi dirinya.



Gambar 4.14 Contoh *User Awareness* oleh *National Cyber Security Alliance*

Referensi pembuatan *user awareness* pada penelitian ini ditambahkan dari hasil penelitian ilmiah yaitu, *2018 Payment Threats and Fraud Trends Report* oleh European Payment Council yang pada penelitian ini dipakai untuk menentukan topik spesifik. Penelitian *Promoting Personal Responsibility For Internet Safety* oleh Robert LaRose, Nora J. Rifon, dan Richard Enbody (2008) dipakai sebagai referensi pembuatan *user awareness* yang memakai *protection motivation theory*, penelitian ini memberikan contoh kalimat *user awareness* yang menekankan pesan pada variabel-variabel *protection motivation theory*. *Cyber Security Awareness Campaigns: Why do they fail to change behaviour*? oleh Maria Bada & Angela Sasse (2014) memberikan referensi teknik persuasif untuk menyampaikan *user*

awareness dan *User preference of cyber security awareness delivery* (Abawajy Jemal, 2014) yang memberikan contoh teknik penyampaian *user awareness*.

4.4.3. Implementing The Awareness Program

Tahapan selanjutnya adalah implementasi. Tahapan ini akan menjelaskan teknik penyampaian materi. *Techniques for delivering awareness material* atau bagaimana memilih media untuk menyampaikan materi. Media penyampaian materi bergantung pada kompleksitas pesan. NIST 800-50 memberikan beberapa alternatif media untuk menyampaikan pesan. Pesan pada *user awareness* dapat berbentuk secara fisik seperti spanduk, kalender, suvenir dan iklan pada media cetak. Sedangkan dalam bentuk digital diantaranya adalah, pesan imbauan melalui surel, iklan melalui sosial media, *computer based session* dan gambar dalam bentuk *pop up message* untuk ponsel pintar.

Penelitian *user awareness* banyak dilakukan di dalam organisasi formal seperti perusahaan untuk para karyawan. Akan tetapi tidak menutup kemungkinan *user awareness* tersebut diterapkan untuk umum atau konsumen karena menyangkut topik yang sama. Perbedaan utama terdapat *reward and punishment* dan keharusan. Penelitian dari Abawajy et al (2014) memberikan beberapa teknik untuk menyampaikan *user awareness*.

a. *Conventional delivery methods*

   Metode konvensional meliputi sumber berupa kertas (*paper based*). Metode kertas biasanya berbentuk selebaran dan poster, disampaikan berupa slogan singkat, menyoroti satu topik spesifik, dan bersifat memberikan anjuran yang harus dilakukan. Selebaran atau poster ada di tempat umum yang bisa dilihat banyak orang. Selebaran atau poster biasanya digunakan untuk memperkuat suatu pesan tertentu. Kekurangan selebaran atau poster adalah pesan *user awareness* menjadi terabaikan karena terus-menerus dilihat. Selebaran atau poster dapat juga berbentuk digital dan muncul berupa *pop up message*. Bentuk lain metode konvensional adalah buletin. Buletin diterbitkan periodic bulanan, triwulan atau waktu tertentu lain dan bisa berbentuk cetak atau digital. Buletin pada umumnya digunakan untuk memperkuat atau menindaklanjuti program

user awareness yang sudah ada. Keunggulan buletin dibanding poster adalah buletin bisa menyampaikan beberapa pesan dibandingkan poster.

b. *Instructor-led delivery methods*

   Instructor-led delivery methods adalah metode penyampaian dengan bentuk presentasi yang dipimpin oleh satu atau beberapa orang yang biasanya merupakan ahli. Metode ini merupakan metode *top-down* dengan tujuan untuk memberikan *user awareness* dari kacamata ahli.

c. *Web-based delivery methods*

   User awareness disampaikan melalui website. Metode ini ramah pengguna sekaligus menawarkan fleksibilitas waktu. Pengguna bisa mengakses user awareness melalui sesi website. Metode ini bisa sekaligus dipakai menawarkan pelatihan keamanan informasi interaktif jika dilengkapi dengan aktivitas.

d. *Game-based delivery methods*

   User awareness bisa disampaikan dalam bentuk permainan yang menggabungkan konsep grafis, permainan dan user awareness. Keuntungan metode ini adalah dapat mendorong pengguna untuk berpartisipasi. Selain itu metode ini dapat dipakai sebagai alat ukur keberhasilan user awareness melalui nilai permainan yang didapatkan pengguna.

e. *Video-based delivery methods*

   Video edukatif dapat memainkan peran penting sebagai bagian dari user awareness. Video dapat menjadi media yang menyediakan user awareness dalam suara dan gambar. Video dapat dilihat berkali-kali, kapanpun, dimanapun, membuat user awareness sangat efektif.

Hasil penelitian Abawajy et al (2012) sekaligus melakukan evaluasi teknik penyampaian *user awareness*. Metode menggunakan *purposive random sampling* pada 60 orang partisipan. Hasil yang didapatkan adalah sebanyak 50% partisipan lebih memilih *user awareness* dalam bentuk *video-based*. Hal ini tentu dapat menjadi pertimbangan penerbit uang elektronik untuk mengembangkan *user awareness* dalam bentuk *video-based* berdurasi pendek.

Selain media untuk menyampaian materi ada hal lain terkait *techniques for delivering awareness material* yang perlu dibahas. Bada & Sasse (2014) pada

penelitiannya menjelaskan penggunaan pendekatan dengan teknik persuasif. Teknik persuasif dipakai untuk mendapatkan atensi dan mempengaruhi *audience*. Contoh teknik-teknik persuasif diantaranya dengan menggunakan *fear message*, memakai asosiasi (menghubungkan dengan hal lain yang setara), menggunakan penggunaan bukti ilmiah yang didukung ahli bidang tertentu (*experts*), humor, testimoni dan repetisi. Teknik persuasif lain seperti analogi dan teknik penempatan waktu (*timing*).

Teknik persuasif yang dipakai pada penelitian ini adalah penggunaan *fear message* dan penggunaan bukti ilmiah. Pada bagian sebelumnya penelitian ini diketahui bahwa *threat appraisal* yaitu *perceived security vulnerabilities* dan *perceived security threat* mempengaruhi pengguna uang elektronik untuk melindungi dirinya dari ancaman kejahatan informasi. Hal ini dapat disimpulkan bahwa pengguna uang elektronik akan dapat terpengaruh pada *user awareness* jika pesan yang disampaikan adalah kerentanan, bagaimana kejahatan keamanan informasi dilakukan dan dampak atau akibat yang akan diterima pengguna uang elektronik. Oleh karena itu guna memperkuat pesan *threat appraisal* teknik persuasif yang tepat untuk mempengaruhi pengguna adalah dengan menggunakan *fear message* yang didukung penelitian ilmiah para ahli.

Sedangkan pada *coping* appraisal hanya perceived *response efficacy* yang dinyatakan mempengaruhi pengguna uang elektronik untuk melindungi dirinya dari ancaman kejahatan informasi. Hal ini berarti kepercayaan individu terhadap keberhasilan dan efektifitas suatu tindakan perlindunganlah yang mempengaruhi individu melakukan tindakan perlindungan, bukan kepercayaan dirinya atau persepsi terhadap beban usaha yang harus dilakukan. Oleh karena itu, pengguna uang elektronik akan dapat terpengaruh pada *user awareness* melalui sudut pandang *coping appraisal* jika pesan yang disampaikan adalah keberhasilan dan efektifitas suatu tindakan perlindungan untuk mencegah kejahatan uang elektronik. Oleh karena itu, teknik penyampaian persuasif yang tepat adalah dengan menggunakan bukti ilmiah untuk memperkuat dan mendukung pendekatan koping atau penyelesaian pada *user awareness*.

4.4.4. *Post Implementation*

Tahapan selanjutnya adalah evaluasi. Tahapan ini menjelasakan dan memberikan masukan saran terkait metode-metode apa saja yang dapat dipakai. *Evaluation feedback and success indicator* atau memilih teknik untuk mengevaluasi dan menentukan indikator keberhasilan. Pemilihan teknik evaluasi harus didahului dengan pemahaman bahwa user security awareness program adalah proses berkelanjutan. Hal yang paling utama adalah memulai proses kemudian menyelesaikannya. Penerbit uang elektronik dapat menggunakan cara-cara yang disarankan oleh Gardner & Thomas (2014) berikut ini:

a. Number of hits on the security awareness

Jumlah klik atau kunjungan pengguna pada *pop up message* yang berhubungan dengan *user awareness*. Penerbit uang elektronik dapat mengetahui apakah *user awareness* menarik perhatian pengguna melalui jumlah klik, semakin banyak jumlah klik semakin menunjukkan ketertarikan pengguna pada topik keamanan informasi.

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

Jumlah pertanyaan, laporan dan keluhan yang masuk berhubungan dengan keamanan informasi kepada *call center*. Semakin banyaknya pertanyaan, laporan atau keluhan menunjukkan semakin meningkatnya kesadaran pengguna untuk melindungi dirinya. Hal ini berarti *user awareness* dapat dikatakan berhasil meningkatkan kesadaran pengguna.

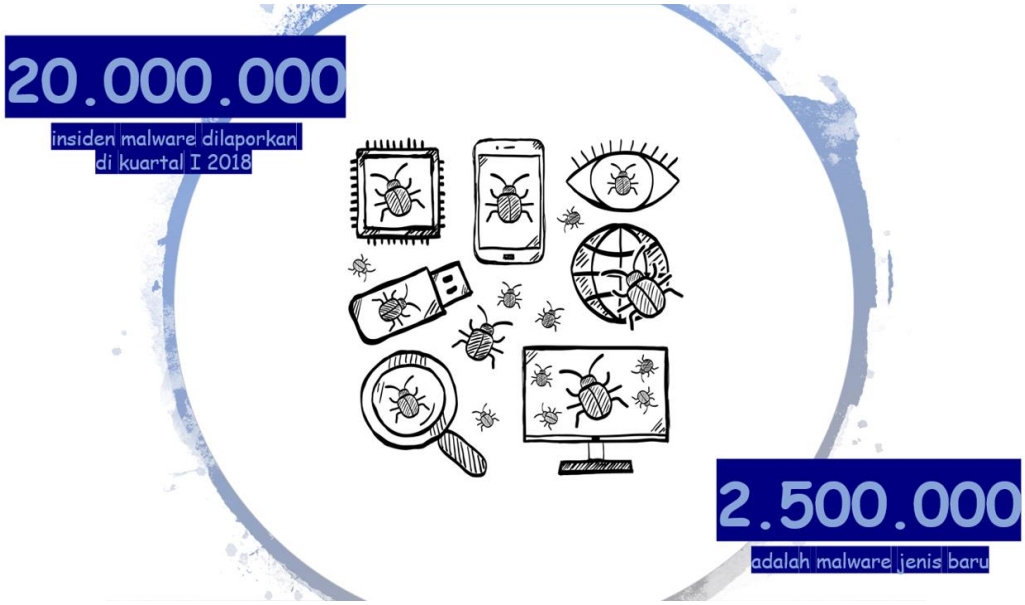
4.5. *User Awareness*

Penelitian ini menggunakan kerangka kerja NIST 800-50 untuk merancang *user awareness*. *User awareness* dirancang menggunakan pendekatan *protection motivation theory*. *User awareness* penelitian ini berfokus untuk membangun kesadaran terhadap ancaman dengan cara mengenali bagaimana kejahatan uang elektronik dilakukan (PSV), dampak yang bisa terjadi (PST) dan respon koping atau penyelesaian (PRE). Bentuk *user awareness* penelitian ini mengacu pada penelitian LaRose et all (2008) yang berupa *short fact* pendek yang bisa dibaca dalam waktu singkat, mudah dimengerti pengguna dan memuat informasi yang diperlukan. *Short fact* pendek tersebut memakai strategi penekanan pesan dengan *protection*

motivation theory. Topik dari setiap *user awareness* yang dibuat dengan PSV, PST dan PRE saling terkait satu sama lain yaitu *phishing* dan *malware*.

Gambar 4.15 dan 4.16 adalah *user awareness* yang dibuat menggunakan kerangka kerja NIST 800-50. Gambar 4.15 dan Gambar 4.16 memiliki pendekatan dan bentuk yang berbeda jika dibandingkan dengan *user awareness* milik GoPay dan OVO yang ada (*existing*). *User awareness* penelitian ini dibuat untuk (*target*) generasi Y yang merupakan *digital natives* sehingga berbentuk (*techniques*) poster digital berupa *pop up message.* Pesan pada *pop up messange* sifatnya persuasif, singkat, padat dan jelas agar pesan yang ruang lingkupnya (*scope*) yaitu *perceived security vulnerabilities* dapat diterima. *User awareness* penelitian ini bebentuk *short fact* yang diharapkan mampu memicu keingintahuan dan membangkitkan kesadaran pengguna uang elektronik. Pada *short fact* diberikan sebuah pesan singkat. Pesan singkat teresebut berbentuk *fear message* (*techniques*) yang disertai dengan mencantumkan (*source*) hasil penelitian dari para ahli yaitu ENISA dan Symantec. Hasil penelitian dari para ahli dicantumkan guna mendukung *fear message*. Hal ini diperlukan guna menghindari *fear message* menjadi opini tidak berdasar yang sekadar menakut-nakuti pengguna. Pada tujuan *user awareness* (*goals*) dijelaskan bagaimana kejahatan uang elektronik dilakukan sehingga pengguna dapat menilai seberapa rentan dirinya jika dihadapkan pada ancaman dengan topik (*selecting*) terkait *phishing* (Gambar 4.15) dan *mobile malware* (Gambar 4.16).

Gambar 4.15 *User Awareness* dengan PSV (1)



Gambar 4.16 *User Awareness* dengan PSV (2)

Gambar 4.17 dan 4.18 adalah *user awareness* yang dibuat menggunakan kerangka kerja NIST 800-50. *User awareness* memiliki pendekatan dan bentuk yang berbeda jika dibandingkan dengan *user awareness* milik GoPay dan OVO yang ada (*existing*). *User awareness* penelitian ini dibuat dengan sasaran (*target*) generasi Y yang merupakan *digital natives* sehingga bentuknya (*techniques*) adalah poster digital berupa *pop up message* yang persuasif, singkat, padat dan jelas agar pesan yang ruang lingkupnya (*scope*) adalah *perceived security threat* dapat diterima. *User awareness* Gambar 4.17 dan Gambar 4.18 mencantumkan (*source*) laporan dari European Payment Council guna memperkuat pesan persuasif *fear message* yang diterima pengguna. Perbedaan lainnya adalah pada tujuan (*goals*) yang menjelaskan akibat kejahatan uang elektronik sehingga pengguna memiliki persepsi terhadap dampak kejahatan uang elektronik dengan topik (*selecting*) dampak *phising* (Gambar 4.17) dan *malware* (Gambar 4.18) yang akan diterima pengguna. *User awareness* penelitian ini merupakan *short fact* yang menjelaskan akibat atau kerugian yang akan diterima pengguna. Berbeda dengan *user awareness* pada PSV, *short fact* yang dibuat tidak mencantumkan angka atau statistik penelitian. Sebagai gantinya *short fact* langsung menjelaskan dampak-dampak dari *phishing* dan *malware*.Hal ini dibuat agar *fear message* lebih dekat dan relevan

dengan pengguna uang elektronik sehingga pengguna uang elektronik dapat langsung memahami dampak atau akibat kejahatan uang elektronik.

Gambar 4.17 Contoh *User Awareness* dengan PST (1)

Gambar 4.18 Contoh *User Awareness* dengan PST (2)

Gambar 4.19 dan Gambar 4.20 adalah *user awareness* yang dibuat dengan menggunakan kerangka kerja NIST 800-50. Pada gambar tersebut jika kita bandingkan dengan *user awareness* milik GoPay dan OVO yang ada (*existing*) maka terdapat perbedaan. *User awareness* OVO misalnya, memberikan tips dan langkah-langkah untuk bertransaksi aman tanpa menjelaskan tujuannya dan dengan sengaja tidak secara gamblang menjelaskan sebuah resiko atau akibat. Gambar 4.19 dan Gambar 4.20 adalah *user awareness* yang dibuat dengan tujuan (*goals*) untuk menjelaskan keberhasilan sebuah respon penyelesaian atau koping sehingga pengguna memiliki persepsi terhadap urgensi sebuah respon untuk mencegah kejahatan uang elektronik. Kedua gambar tersebut memiliki topik (*selecting*) yaitu respon yang dapat dipakai untuk melindungi dari *phising* (Gambar 4.19) dan mencegah *malware* (Gambar 4.20). *User awareness* penelitian ini dibuat untuk (*target*) generasi Y yang merupakan *digital natives* sehingga berbentuk (*techniques*) poster digital berupa *pop up message* yang persuasif, singkat, padat dan jelas agar pesan yang ruang lingkupnya (*scope*) adalah *perceived response efficacy* dapat diterima oleh pengguna. *User awareness* Gambar 4.19 dan 4.20 mencantumkan laporan (*source*) dari European Payment Council guna

menyampaikan pesan persuasif (*techniques*) berupa *fear message* disertai referensi ilmiah guna meyakinkan pengguna pada keberhasilan tindakan respon atau koping. *User awareness* penelitian ini merupakan *short fact*, dibandingkan tips-tips dan langkah-langkah seperti *user awareness* yang sebelumnya ada. Hal ini diharapkan mampu memicu keingintahuan dan membangkitkan kesadaran pengguna uang elektronik.

Gambar 4.19 Contoh *User Awareness* dengan PRE (1)

Gambar 4.20 Contoh *User Awareness* dengan PRE (2)

BAB 5
KESIMPULAN DAN SARAN

Bab ini akan menjelaskan mengenai kesimpulan yang dapat ditarik dari seluruh proses penelitian untuk memastikan apakah hasil yang diperoleh mampu menjawab pertanyaan penelitian serta memenuhi tujuan penelitian.

5.1 Kesimpulan

Penelitian ini bertujuan untuk melakukan pendekatan melalui *protection motivation theory* untuk mendapatkan faktor-faktor yang mempengaruhi pengguna melakukan *precautionary behavior*. Faktor-faktor tersebut kemudian digunakan sebagai landasan untuk merancang *user awareness*. *User awareness* ditujukan untuk pengguna uang elektronik.

1. Penelitian mengidentifikasi faktor-faktor yang mempengaruhi pengguna melakukan *precautionary behavior* yang diujikan pada populasi pengguna uang elektronik dengan jumlah populasi sebanyak 186 orang.
2. Penelitian ini tidak mendukung *protection motivation theory*. Hasil Pengujian dengan R^2 menunjukkan bahwa kelima variabel independen penelitian hanya mampu menjelaskan 31,2% variabel dependen dan sisanya dijelaskan oleh variabel lain yang tidak ada di dalam penelitian ini.
3. Kerangka kerja NIST 800-50 dapat dipakai untuk merancang *user awarenes* pengguna uang elektronik dengan melakukan pendekatan teori *protection motivation*.

5.2 Saran

Berdasarkan keseluruhan tahap penelitian hingga kesimpulan diperoleh saran yang dapat digunakan untuk pengembangan penelitian selanjutnya yaitu:

1. Penelitian selanjutnya dapat melakukan evaluasi terhadap *user awareness* dengan pendekatan *protection motivation theory*, apakah lebih memiliki dampak dibanding *user awareness* yang sudah ada.

2. Penelitian selanjutnya dapat menambahkan *context-specific variables* (keamanan transaksi pengguna uang elektronik) lainnya yang dapat menjelaskan *precautionary behavior*.
3. Penelitian selanjutnya dapat meneliti *actual behavior* dibanding *intention* pengguna uang elektronik terkait keamanan informasi.
4. Penerbit uang elektronik dapat mengembangkan *user awareness* dengan melakukan pendekatan *cognitive behavioral*.
5. Penerbit uang elektronik dapat mengembangkan *user awareness* dengan kerangka kerja NIST 800-50.

Daftar Pustaka

Bada, Maria & Sasse, Angela & Nurse, Jason. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. 118-131.

Bank Indonesia. (2018). PERATURAN BANK INDONESIA NOMOR 20/6/PBI/2018 TENTANG UANG ELEKTRONIK.Jakarta

Boerman, Sophie & Kruikemeier, Sanne & J. Zuiderveen Borgesius, Frederik. (2018). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. Communication Research.

Chin, Wynne & Marcoulides, G. (1998). The Partial Least Squares Approach to Structural Equation Modeling. Modern Methods for Business Research. 8.

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. In Proceedings of the 43rd Hawaii international conference on system sciences (pp. 1-10).

European Payment Council. (2018). Payment Threats and Fraud Trends Report. [online] Available at:https://www.europeanpaymentscouncil.eu [Accessed 24 Apr. 2019].

Falk, R.F. and Miller, N.B. (1992). A Primer for Soft Modeling. University of Akron Press, Akron.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407-429.

Gardner, Bill & Thomas, Valerie. (2014). Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats 1st Edition.

Grabner-Kr€auter, S., & Faullant, R. (2008). Consumer acceptance of internet banking: The influence of internet trust. International Journal of Bank Marketing, 26(7), 483-504.

Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). Multivariate Data Analysis 6th ed. Prentice Hall.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

Hidayati, Siti. (2006). Kajian Operasional E-Money. Bank Indonesia.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

Jemal, Abawajy (2014) User preference of cyber security awareness delivery methods, Behaviour & Information Technology, 33:3, 237-248.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly, 34(3), 549-566.

Jansen, Jurjen & Schaik, Paul. (2017). Testing a model of precautionary online behaviour: The case of online banking. Computers in Human Behavior. 87.

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. Decision Support Systems, 52(2), 353e363.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. Communications of the ACM, 51(3), 71–76.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Associationfor Information Systems, 11(7), 394-413.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469-479.

Malhotra, N. (2009). Riset Pemasaran Pendekatan Terapan Jilid 1. Jakarta: PT Index.

Marijn Martens, & De Wolf, Ralf & Marez, Lieven (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Computer in Human Behavior 92. 139-150.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health related behavior: A meta-analytic review of protection motivation theory.

Journal of Applied Social Psychology, 30(1), 106-143.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.

Ophoff, Jacques & Lakay, Mcguigan. (2019). Mitigating the Ransomware Threat: A Protection Motivation Theory Approach: 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018.

Tsai, H., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49, 190-198.

Wilson, M., & Hash, J. (2003). SP 800-50. Building an Information Technology Security Awareness and Training Program.

Woon, Irene; Tan, Gek-Woo; and Low, R., "A Protection Motivation Theory Approach to Home Wireless Security" (2005). *ICIS 2005 Proceedings*. 31.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in human behavior, 24(6), 2799-2816.

Wright, Ryan T.; Campbell, Damon E.; Tatcher, Jason Bennet; and Roberts, Nicholas (2012) "Operationalizing MultidimensionalConstructs in Structural Equation Modeling: Recommendations for IS Research," Communications of the Association for InformationSystems: Vol. 30, Article 23.

Wu, Cynthia & Ting Wong, Ho & Chou, Lai & Pak Wai To, Bobby & Lee, Wai Lok & Loke, Alice Yuen. (2014). Correlates of Protective Motivation Theory (PMT) to Adolescents' Drug Use Intention. International journal of environmental research and public health. 11. 671-84.

Yoon, C & Hwang, J.-W & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. Journal of Information Systems Education. 23. 407-416.

BIODATA PENULIS

Penulis lahir di Surabaya pada 15 Oktober 1990 dan merupakan anak kedua dari tiga bersaudara. Penulis telah menempuh studi formal di SMAN 9 Surabaya pada tahun 2006-2009, dan mengambil gelar Sarjana di Institut Bisnis dan Informatika Stikom Surabaya pada tahun 2009-2013. Kemudian Penulis melanjutkan pendidikan Pasca Sarjana di Magister Manajemen Teknologi ITS Surabaya pada 2017-2019. Penulis juga mengikuti seminar internasonal pada *International Conference on Business and Management of Technology* yang diselenggarakan di Surabaya, Indonesia yang berjudul USER AWARENESS DESIGN FOR ELECTRONIC MONEY USER USING PROTECTION MOTIVATION THEORY AND NIST 800-50 FRAMEWORK. Adapun pertanyaan dapat disampaikan langsung pada email andrean.christian@live.com.

(Halaman ini sengaja dikosongkan)

Lampiran 1

Tabel Hasil Kuesioner

PSV1	PSV2	PST1	PST2	PST3	PSE1	PSE2	PSE3	PRE1	PRE2	PRE3	PPC1	PPC2	PPC3	PB1	PB2	PB3
5	5	5	5	5	4	4	5	4	4	4	4	3	3	5	5	5
4	4	3	5	3	3	3	5	5	3	3	4	4	4	3	4	3
3	4	5	5	5	4	4	4	4	4	4	4	4	4	4	4	4
4	4	5	4	5	5	2	4	5	5	5	4	4	4	5	5	5
5	5	5	5	5	5	5	5	5	5	5	3	5	4	5	5	5
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
4	4	5	5	5	3	3	4	4	4	4	2	2	2	4	4	4
2	2	1	5	4	5	5	5	5	5	5	5	5	5	3	5	5
1	5	5	5	5	4	3	5	5	5	5	5	4	4	5	5	5
5	5	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5
1	1	5	5	5	5	3	5	3	5	3	5	5	3	3	3	3
5	5	5	5	5	3	3	3	3	4	4	1	3	2	5	5	5
4	4	3	4	4	4	4	4	4	4	4	5	4	3	4	4	4
3	5	5	5	5	5	4	5	5	4	5	4	3	4	4	4	4
3	4	5	5	5	5	5	5	5	5	5	3	4	2	4	4	4
4	3	4	3	4	5	4	3	5	4	4	4	3	4	4	4	3
4	4	2	4	4	5	5	4	5	4	5	2	4	2	4	4	4
2	3	5	4	5	5	5	4	5	5	5	5	4	3	5	5	5
3	3	3	3	3	4	2	4	4	4	4	4	3	3	3	3	4
5	4	5	5	5	4	4	3	5	5	5	3	4	3	5	5	5
3	3	5	3	5	5	5	5	5	5	5	2	3	3	4	3	4
3	2	5	5	5	4	4	5	5	5	5	2	1	3	5	5	5
4	3	5	5	5	3	3	5	5	5	5	4	3	3	5	5	5
2	3	2	4	5	2	3	4	4	4	4	4	4	4	4	4	4
4	4	5	5	5	4	4	4	5	5	4	4	4	3	5	5	5
2	2	5	2	5	3	3	5	5	5	5	5	5	5	5	5	5
2	2	3	4	4	4	3	4	4	4	4	4	3	3	3	4	4
5	5	5	5	5	2	4	4	4	3	3	4	5	4	2	2	4
3	3	5	5	5	4	4	4	4	4	4	3	3	3	4	4	4
2	2	5	5	5	4	4	4	4	4	4	3	3	3	5	5	5
4	2	2	4	4	3	4	4	4	4	4	2	2	3	4	4	4
4	2	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5
4	2	5	5	5	2	2	5	5	5	4	3	4	5	4	4	4
4	4	4	5	5	2	2	3	2	3	3	3	3	3	4	4	4
3	3	3	5	5	4	4	5	4	5	5	3	4	2	4	4	5

2	4	5	5	5	2	4	4	4	4	4	1	3	3	5	4	4
3	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
3	4	4	4	4	3	4	4	4	4	4	2	2	2	4	4	4
3	4	3	4	4	4	4	4	4	4	4	2	3	2	4	4	4
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
5	5	5	5	5	5	4	5	5	5	5	5	4	5	5	5	5
5	4	5	5	5	2	2	5	4	5	5	2	2	1	5	5	5
5	5	3	5	5	5	5	5	5	5	5	5	3	3	1	1	5
4	4	4	4	5	4	3	3	4	5	4	4	3	4	4	4	4
4	4	4	5	5	3	3	4	5	5	5	4	3	2	5	5	5
2	4	3	5	5	3	3	3	3	5	5	5	2	3	5	5	5
3	3	2	4	4	4	4	3	4	4	3	4	2	2	4	4	4
3	4	5	5	5	5	5	5	5	5	5	5	4	1	5	5	5
3	4	4	5	5	5	5	5	5	5	5	5	2	2	5	5	5
5	4	5	5	5	2	4	4	2	4	5	3	3	2	3	4	4
1	1	5	5	5	5	5	5	5	5	5	1	1	1	5	5	5
2	3	5	5	5	5	4	4	5	5	5	1	3	3	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
3	4	4	5	5	5	5	5	5	5	5	5	5	4	5	5	5
4	3	3	4	5	4	4	4	5	5	5	2	2	2	4	5	5
5	2	5	5	5	5	5	5	5	5	5	1	1	4	5	5	5
1	2	2	5	5	4	3	4	5	5	5	1	2	1	4	5	5
3	4	5	5	5	5	5	5	5	5	5	2	2	2	5	5	5
3	4	4	5	5	3	4	3	4	4	5	4	4	4	5	5	5
4	4	5	5	4	4	4	5	5	5	5	3	2	4	4	4	4
3	4	3	5	5	4	4	4	4	4	4	3	2	3	4	4	4
4	3	5	5	5	4	4	4	4	4	4	4	2	3	4	4	4
1	3	1	5	4	4	4	4	4	4	4	4	2	3	4	4	4
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
4	2	4	5	5	5	4	4	5	5	5	4	4	3	4	4	4
5	5	5	5	5	5	5	5	5	5	4	4	5	4	5	5	5
4	3	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4
3	1	5	5	5	5	4	5	3	5	4	5	5	4	4	4	5
4	4	5	5	5	4	4	4	4	4	4	4	4	5	4	5	4
2	5	5	5	5	5	4	5	5	5	5	4	3	3	4	4	4
4	3	5	5	5	5	3	5	5	5	5	3	3	3	4	3	3
4	4	5	5	5	4	4	5	5	5	5	5	5	1	4	3	4
5	5	4	5	5	3	4	3	5	5	5	2	4	4	3	3	3
2	3	3	4	5	5	5	5	4	4	5	5	1	2	4	3	3
4	4	4	5	5	3	4	5	4	4	4	4	4	3	5	4	4
5	5	5	5	5	5	4	4	5	5	5	5	2	3	5	5	5
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
2	3	4	3	5	4	4	4	4	4	5	4	3	2	5	3	3

5	5	3	5	5	5	4	4	5	4	4	4	4	5	5	5	5
3	3	5	5	5	5	4	2	4	3	4	5	5	2	4	4	5
4	4	5	4	5	5	5	5	4	5	4	5	5	5	4	4	5
3	4	5	5	5	5	4	4	3	4	5	2	5	2	3	4	4
2	4	4	4	4	4	4	4	4	4	4	4	4	2	4	4	4
4	4	4	5	4	5	5	4	5	5	5	5	3	3	3	4	4
4	5	4	5	5	5	4	3	3	4	3	4	5	3	4	4	5
1	5	5	5	5	5	3	4	5	4	4	4	4	3	4	4	4
4	2	5	5	5	5	3	4	5	5	4	2	1	2	4	4	4
4	4	5	5	5	4	4	5	5	5	4	3	1	1	5	5	5
5	5	5	5	5	2	2	2	2	3	3	5	5	5	5	5	5
4	4	5	5	5	3	4	4	4	4	4	3	3	3	4	4	4
4	4	5	5	5	5	5	5	5	5	5	1	1	2	5	5	5
4	2	4	4	4	5	4	4	5	5	5	3	4	2	5	5	5
4	5	5	4	5	3	3	5	5	3	4	5	4	4	4	4	4
3	3	5	5	5	4	2	4	5	5	5	1	2	2	5	5	5
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
5	4	5	4	5	4	3	5	4	2	2	3	4	5	4	3	4
4	5	5	5	5	5	5	5	3	4	5	3	5	5	2	5	5
4	5	5	5	5	3	4	4	4	4	5	2	3	3	5	5	5
2	3	2	5	4	4	5	4	4	5	4	2	4	4	5	4	5
3	4	5	3	3	2	2	4	4	4	4	4	3	2	4	5	4
4	3	5	5	5	5	5	5	5	5	5	5	5	3	3	4	5
4	4	4	5	5	5	4	4	5	5	5	2	4	2	4	4	4
4	2	3	5	5	4	5	5	5	5	5	5	5	5	4	5	5
4	5	4	5	4	5	5	4	5	4	5	4	3	4	5	4	4
3	5	5	4	5	4	4	5	5	5	5	2	1	4	3	5	5
2	4	5	5	4	5	5	5	4	5	4	4	3	3	4	4	4
4	4	5	5	5	4	4	4	5	5	5	3	3	3	4	4	4
1	4	4	5	5	5	4	3	4	5	5	2	4	3	3	4	5
3	4	5	5	4	4	3	4	5	5	4	4	4	4	5	4	4
4	4	5	5	5	4	4	4	4	4	5	2	3	2	5	5	5
2	3	4	5	5	4	3	5	4	4	4	4	4	5	5	5	5
4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
5	5	5	5	5	4	4	4	4	4	4	3	3	2	5	5	5
5	5	5	5	5	2	2	4	5	5	5	5	5	5	5	5	5
1	1	5	5	5	5	5	5	5	5	5	5	1	4	5	5	5
4	4	5	5	5	5	5	5	5	5	5	5	2	1	5	5	5
5	5	5	5	5	2	2	5	5	5	5	5	5	5	5	5	5
3	3	4	5	5	4	4	3	5	5	5	4	4	3	5	4	4
4	4	5	5	5	4	3	3	4	4	4	3	3	3	3	3	3
1	1	4	5	5	4	5	5	5	5	5	4	3	4	4	4	4
2	3	3	5	5	5	5	5	5	5	5	5	1	1	5	4	5

4	4	5	5	5	5	4	5	5	4	5	4	3	3	5	5	5
4	4	4	5	5	4	3	4	4	5	4	2	1	3	4	5	5
4	4	4	4	5	5	5	5	5	5	4	5	5	5	4	5	4
3	3	5	5	5	4	4	4	5	5	5	4	3	3	4	4	4
3	2	4	4	4	4	4	4	4	4	4	4	2	3	4	4	4
3	4	5	5	5	3	4	4	2	5	5	3	4	2	4	4	4
3	4	4	5	5	3	3	5	5	5	5	5	5	3	5	5	5
3	4	5	5	5	5	4	4	5	5	5	5	4	4	5	5	5
4	4	5	5	5	5	5	5	5	5	5	2	2	2	5	5	5
4	4	4	4	4	3	3	4	4	4	4	4	3	3	4	4	4
3	3	5	5	5	4	4	4	4	4	4	4	4	4	4	4	4
4	5	3	5	5	2	2	5	4	4	5	5	5	5	5	5	5
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	5	5	5	5	5	5	4	4	5	2	2	4	4	4	4
4	3	3	5	5	4	4	4	4	5	4	4	4	4	4	4	4
3	3	2	5	5	3	4	4	4	4	4	3	3	3	4	4	4
3	4	4	5	5	5	5	5	5	5	5	1	2	2	5	5	5
3	5	5	5	5	4	5	5	5	5	5	4	5	4	4	5	5
4	4	5	5	5	3	4	5	5	5	4	5	3	3	5	5	5
4	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5
3	5	3	5	5	5	4	4	5	5	4	3	3	3	4	4	4
4	4	5	5	5	5	5	4	5	5	5	1	1	2	5	5	5
4	4	4	5	5	5	3	5	5	5	5	5	3	4	5	5	5
5	5	5	5	5	5	3	5	4	4	4	4	5	5	5	5	5
5	5	5	5	5	5	5	5	5	5	5	3	2	3	4	4	5
5	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
1	3	4	5	5	3	3	3	3	3	4	3	3	3	3	3	3
4	4	5	5	5	4	3	2	4	3	5	2	3	2	3	4	4
5	4	2	5	5	5	5	5	5	5	5	1	1	1	5	5	5
3	3	5	5	5	5	4	4	4	4	4	3	3	3	4	4	4
3	3	3	4	5	4	3	4	5	5	5	3	4	3	3	3	5
3	4	5	5	5	3	4	3	4	4	4	5	5	4	3	3	4
4	4	5	5	5	3	3	5	4	4	4	4	2	2	4	4	4
3	3	5	5	5	5	3	4	3	4	5	3	2	2	5	5	5
5	4	5	5	5	4	4	5	5	5	5	5	4	3	5	5	5
1	4	5	5	5	5	5	5	5	5	5	3	4	4	5	5	5
4	4	4	5	5	4	4	4	4	4	4	4	4	4	4	4	4
4	5	4	5	4	5	5	5	5	5	4	4	4	4	5	5	5
5	4	5	5	5	5	5	5	5	5	5	5	3	3	4	4	4
4	4	5	5	5	4	4	4	4	5	5	4	4	3	5	5	5
4	5	5	5	5	5	5	5	5	4	4	4	3	3	4	4	4
4	4	3	5	5	3	3	2	4	4	4	2	2	3	4	4	4
4	4	4	4	4	4	4	4	4	4	4	2	4	3	4	4	4
3	1	3	3	3	3	3	4	4	4	4	4	4	4	4	3	3

3	3	4	5	5	4	4	3	4	4	4	3	3	3	4	4	4
4	4	4	4	4	5	3	5	5	5	5	3	3	5	5	5	5
5	4	4	4	4	4	3	4	4	4	4	3	5	4	3	5	4
4	4	5	4	5	4	4	4	5	5	5	4	3	5	5	5	5
5	5	5	5	5	5	5	5	5	5	5	2	2	3	5	5	5
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
4	4	4	4	4	4	4	4	4	4	4	3	2	2	4	4	4
3	3	3	4	5	4	3	4	4	3	4	2	1	3	4	4	4
1	1	5	5	5	5	5	5	5	5	5	5	2	2	4	4	4
4	5	5	5	5	5	4	4	5	5	5	3	2	3	5	5	5
4	4	4	4	5	5	3	4	4	4	4	4	2	2	4	4	4
2	4	2	1	2	5	5	5	5	5	5	5	2	2	3	4	4
4	5	5	4	5	4	4	5	5	5	4	5	3	4	5	4	4
3	3	4	4	4	3	3	3	3	3	3	3	4	3	4	3	3
4	4	4	4	4	4	4	4	4	4	4	2	2	2	4	4	4
4	4	4	4	4	4	4	4	4	4	4	2	2	2	4	4	4
2	2	5	5	5	5	5	5	5	5	5	5	3	3	3	5	5
4	4	4	4	4	4	3	4	3	4	4	2	2	2	5	5	5
4	4	5	5	5	3	4	4	5	5	5	2	2	2	5	5	5

(Halaman ini sengaja dikosongkan)

Lampiran 2

KUESIONER GOOGLE FORM

Precautionary Behavior Pengguna Uang Elektronik

Halo! Saya Christian Andrean mahasiswa Magister Manajemen Teknologi - Institut Teknologi Sepuluh November yang sedang melakukan penelitian terkait precautionary behaviour pengguna uang elektronik.

Bacalah informasi yang diberikan terlebih dahulu sebelum memberi respon atas pernyataan-pernyataan di halaman selanjutnya.

Jawablah dengan sebenar-benarnya sesuai dengan persepsi Anda. Segala informasi yang diberikan akan dirahasiakan dan hanya akan digunakan pada penelitian ini.

Saya sangat mengapresiasi bantuan Anda. Terima kasih banyak!

* Required

1. **Email address** *

2. **Apakah anda pernah bertransaksi menggunakan uang elektronik ?** *
   Mark only one oval.
   - ◯ Pernah
   - ◯ Tidak Pernah *Stop filling out this form.*

Data Demografis Responden

3. **Usia (contoh: 27)** *

4. **Jenis Kelamin** *
   Mark only one oval.
   - ◯ Laki-laki
   - ◯ Perempuan

5. **Sudah berapa lama anda memakai Uang Elektronik?** *
Mark only one oval.

- ◯ < 1 tahun
- ◯ 1 -2 tahun
- ◯ > 3 tahun

6. **Uang Elektronik mana yang paling sering anda gunakan?** *
Mark only one oval.

- ◯ GoPay
- ◯ OVO
- ◯ LinkAja / T-Cash
- ◯ Other: _____

Threat Appraisal

Melakukan transaksi dengan uang elektronik tidak sepenuhnya terbebas dari RISIKO KEJAHATAN yang menyebabkan terjadinya KERUGIAN tertentu. Berikut adalah informasi terkait kejahatan uang elektronik.

Bagaimana Kejahatan Uang Elektronik dilakukan?

1. Mencuri Ponsel Pintar

Jika seseorang mencuri ponsel dan memiliki akses sepenuhnya pada semua aplikasi, maka akun uang elektronik dapat diambil alih dan dimanfaatkan dengan mengganti kata sandi melalui fitur “lupa password” yang mengirim kode verifikasi ke ponsel tersebut.

2. Malware

Malware mencatat aktivitas ponsel pintar yang diinjeksinya kemudian mengirimkannya melalui internet tanpa sepengetahuan anda. Malware bisa disusupkan melalui cara-cara berikut:
· QR Code palsu yang dipindai saat transaksi
· Link yang mengarah ke situs tertentu yang mengunduh malware secara otomatis
· Saat anda memakai WiFi publik yang datanya tidak tersandikan maka malware dapat membaca dan mengirimkannya melalui internet

3. Phishing

Teknik menipu dengan menyamar sebagai pihak resmi. Pada umumnya dilakukan dengan 2 cara:

· Pelaku mengirim tautan pada surel pengguna.
Alamat surel dibuat sangat meyakinkan sehingga mungkin sulit dibedakan.
Tautan tersebut berisi kode program yang mengirimkan data pribadi dan informasi
finansial tanpa sepengetahuan pengguna.
· Pelaku menelepon pengguna dan mengaku dari pihak resmi uang elektronik.
Pelaku selanjutnya akan meminta pengguna mengirimkan kode OTP (one time password)
yang dikirimkan sistem lewat SMS.
Kode OTP ini dapat dipakai pelaku untuk mengganti kata sandi akun pengguna. Jika
berhasil maka pelaku akan mendapat akses seluas-luasnya pada akun pengguna.

Apa Dampak Kejahatan Uang Elektronik

1. Kerugian finasial

Kerugian berupa hilangnya saldo uang elektronik yang ditransfer atau dibelanjakan pelaku.

2. Pencurian infomasi pribadi

Informasi pribadi mengacu pada identitas berupa nama lengkap, nomer KTP, tanggal lahir dan lain sebagainya. Identitas korban digunakan untuk melakukan penipuan dengan mengaku sebagai korban dan meminta sejumlah uang.

3. Akun Uang Elektronik dan Informasi Finansial

Akun menyimpan catatan nama pengguna, kata sandi, alamat surel, dan informasi perbankan (nomer kartu ATM) pengguna. Sedangkan informasi finansial menyimpan sekumpulan informasi transaksi yang dilakukan dengan menggunakan uang elektronik. Data akun dan informasi finansial tersebut dapat dijual kepada pihak ketiga yang memanfaatkannya untuk kepentingan tertentu atau digunakan untuk membobol akun perbankan korban.

PSV dan PST

Sesudah membaca informasi-informasi tersebut, silahkan menjawab pernyataan-pernyataan berikut sesuai dengan apa yang anda persepsikan. Tidak ada jawaban benar atau salah.

1=Sangat Tidak Setuju
2=Tidak Setuju
3=Netral
4=Setuju
5=Sangat Setuju

7. **Saya mungkin saja menjadi korban kejahatan phising melalui surat elektronik atau melalui telepon secara langsung** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

8. **Saldo, informasi finansial dan informasi pribadi saya bisa saja menjadi cukup rentan untuk dicuri tanpa saya sadari** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

9. **Bagi saya kehilangan akun dan saldo uang elektronik dampaknya akan sangat buruk** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

10. **Pencurian informasi pribadi dan informasi finasial saya adalah masalah yang serius** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

11. **Pemakaian identitas saya oleh orang yang mencuri akun uang elektronik adalah masalah yang sangat penting** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

Coping Appraisal

Kejahatan uang elektronk dapat dicegah. Penerbit uang elektronik memberikan PANDUAN KEAMANAN yang bisa dilakukan pengguna.

Bagaimana Mencegah Kejahatan Uang Elektronik?

1. Menjaga Keamanan Ponsel Pintar

· Kunci Ponsel Pintar anda dengan sandi angka, pola atau sidik jari agar tidak sembarang
orang dapat memakai ponsel pintar tersebut
· Selalu lakukan pembaruan aplikasi uang elektronik
· Pasang antivirus pada ponsel pintar anda

2. Menjaga Login Information

a) Jangan memberitahukan login information berupa nomer telepon, alamat surat elektronik
(surel), dan kata sandi akun uang elektronik kepada siapapun.
b) Lakukan verifikasi alamat surel. Sebisa mungkin gunakan surel tersebut hanya untuk
akun uang elektronik saja untuk mencegah masuknya pesan spam dan phishing jika anda
menggunakan alamat surel tersebut untuk berbagai akun.
c) Ubah PIN secara berkala

3. Selalu Berhati-hati dan Waspada

a) Selalu waspada pada pihak yang mengatasnamakan penerbit uang elektronik. Penerbit
uang elektronik tidak pernah meminta informasi pribadi anda seperti PIN atau kode OTP.
Perhatikan baik-baik alamat pengirim surel jika anda menerima surel yang
mengatasnamakan penerbit uang elektronik.
b) Segera lakukan pemblokiran melalui penerbit uang elektronik jika nomer telepon atau
ponsel pintar anda hilang.

PSE, PRE, dan PPC

Sesudah membaca informasi-informasi tersebut, silahkan menjawab pertanyaan-pertanyaan berikut sesuai dengan apa yang anda persepsikan. Tidak ada jawaban benar atau salah.

1=Sangat Tidak Setuju
2=Tidak Setuju
3=Netral
4=Setuju
5=Sangat Setuju

12. **Bagi saya menjaga keamanan ponsel pintar adalah cara yang mudah untuk dilakukan** *
Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

13. **Saya memiliki pengetahuan dan kemampuan menjaga login information agar aman dan terlindungi** *
Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

14. **Selalu memiliki kehati-hatian dan kewaspadaan setiap saat untuk melindungi akun uang elektronik membuat saya merasa nyaman** *
Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

15. **Menjaga keamanan ponsel pintar adalah cara yang efektif untuk mencegah pencurian akun dan saldo uang elektronik saya** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

16. **Melindungi login information dapat membantu mencegah informasi pribadi dan informasi finasial saya dicuri** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

17. **Selalu berhati-hati dan waspada tidak mempercayai informasi selain dari penerbit uang elektronik dapat menghindarkan saya menjadi korban kejahatan uang elektronik** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

18. **Membuat dan melindungi login information sesuai yang disarankan mengharuskan saya memulai kebiasaan baru dimana merupakan hal yang sulit** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

19. **Kenyamanan saya berkurang jika harus terus-menerus berhati-hati dan waspada saat bertransaksi menggunakan uang elektronik** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

20. **Ada beban biaya, usaha, dan waktu yang besar untuk menjalankan panduan keamanan uang elektronik yang disarankan** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

Precautionary Behavior

Sesudah membaca informasi-informasi tersebut, silahkan menjawab pernyataan-pernyataan berikut sesuai dengan apa yang anda persepsikan. Tidak ada jawaban benar atau salah.

1=Sangat Tidak Setuju
2=Tidak Setuju
3=Netral
4=Setuju
5=Sangat Setuju

21. **Setelah mendapat informasi kejahatan uang elektronik dan panduan perlindungan keamanan yang ada, mungkin saya akan melakukan perilaku pencegahan dengan menjalankan panduan keamanan** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

22. **Setelah mendapat informasi kejahatan uang elektronik dan panduan perindungan keamanan yang ada, semestinya saya akan melakukan perilaku pencegahan dengan menjalankan panduan keamanan** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju

23. **Setelah mendapat informasi kejahatan uang elektronik dan panduan perlindungan keamanan yang ada, sepatutnya saya melakukan perilaku pencegahan dengan menjalankan panduan keamanan** *

Mark only one oval.

	1	2	3	4	5	
Sangat Tidak Setuju	◯	◯	◯	◯	◯	Sangat Setuju