Analisis Faktor Utama Dalam *Information Security - Personality Threat* Terhadap *Phishing Attacks* Menggunakan Metode *Technology Threat Avoidance Theory (TTAT)*

Kun Saidi
16917211

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Teknik Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2020

Lembar Pengesahan Pembimbing

Analisis Faktor Utama Dalam *Information Security - Personality Threat* Terhadap *Phishing Attacks* Menggunakan Metode *Technology Threat Avoidance Theory (TTAT)*

Kun Saidi
16917211

Yogyakarta, Desember,2020

Pembimbing

Dr. Yudi Prayudi, S.Si., M.Kom

Lembar Pengesahan Penguji

Analisis Faktor Utama Dalam *Information Security - Personality Threat* Terhadap *Phishing Attacks* Menggunakan Metode *Technology Threat Avoidance Theory (TTAT)*

Kun Saodi

16917211

Yogyakarta, Desember,2020

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom

Ketua

Dr. Imam Riadi, M.Kom

Anggota I

Dr. Ir. Bambang Sugiantoro, MT

Anggota II

Mengetahui,

Ketua Program Studi Teknik Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

Analisis Faktor Utama Dalam *Information Security - Personality Threat* Terhadap *Phishing Attacks* Menggunakan Metode *Technology Treat Avoidance Theory (TTAT)*

Social engineering (SE) merupakan kegiatan yang melibatkan *human* ,psikologi manusia, dan teknologi, sehingga menyebabkan kerugian dari *victim* dimana *computer science* dan sosial spikologi digunakan dalam menentukan bahaya SE terhadap masyarakat, serta dapat mengancam di berbagai sektor organisasi/institusi yaitu salah satunya menggunakan SE *attacks.* Masyarakat tersebut merupakan partisipan (dosen/staff/karyawan) yang dipengaruhi oleh faktor meliputi *perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard costs, self-efficacy (security awareness), behavioral intention, avoidance motivation,* dan *avoidance behavior* terhadap *phishing attacks* pada sektor tersebut dengan menggunakan menggunakan model *Technology Threat Avoidance Theory (TTAT).* Analisis faktor tersebut bertujuan untuk mengetahui faktor yang sangat berpengaruh terhadap partisipan tersebut terhadap *phishing attacks* yang terjadi pada organisasi tersebut. Berdasarkan pada hasil analisis MANOVA, *pairwise comparisons* menunjukkan bahwa terdapat keterkaitan antar faktor yang sangat berpengaruh tersebut yaitu faktor *behavioral intention* dengan faktor *self-efficacy – security awareness* berdasarkan pada faktor yang terdapat dalam model tersebut dengan nilai *mean difference* yaitu 12.305.925 (Sig.< 0.05) dan nilai R^2 *(Adjusted R Squared)* yaitu 0.698. Faktor tersebut merupakan keterikatan faktor utama dalam *personality threat*, sehingga individu dapat mencegah menjadi korban *cybercrime* terhadap *phishing attacks.*

Kata Kunci: *social engineering, behavioral intention, self-efficacy – security awareness, Technology Threat Avoidance Theory (TTAT), MANOVA, phishing attacks*.

Abstrack

Analysis of Main Factors in Information Security - Personality Threat Against Phishing Attacks Using the Technology Treat Avoidance Theory (TTAT) Method

Social engineering (SE) is an activity that involves human beings, human psychology, and technology, thus causing losses to the victim where computer science and social psychology are used to determine the dangers of SE to society, and can threaten various organizational / institutional sectors, one of which is using SE. attacks. These communities are participants (lecturers / staff / employees) who are influenced by factors including perceived severity, perceived susceptibility, perceived threats, safeguard effectiveness, safeguard costs, self-efficacy (security awareness), behavioral intention, avoidance motivation, and avoidance behavior towards phishing. attacks on the sector using the Technology Threat Avoidance Theory (TTAT) model. This factor analysis aims to determine the factors that greatly influence the participants against the phishing attacks that occur in the organization. Based on the results of the MANOVA analysis, pairwise comparisons show that there is a relationship between these influencing factors, namely the behavioral intention factor with the self-efficacy - security awareness factor based on the factors contained in the model with avalue mean difference of 12,305,925 (Sig. < 0,05) and R^2 (Adjusted R Squared) is 0,698. This factor is the main factor attached to personality threats, so that individuals can prevent becoming victims of cybercrime against phishing attacks.

Keywords: *social engineering, behavioral intention, self-efficacy – security awareness, Technology Threat Avoidance Theory (TTAT), MANOVA, phishing attacks*

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bawah tesis ini merupakan tulisan asli dari penulis, dan tidak berisi yang tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survey, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Desember 2020

Kun Saidi

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dalam penulisan tesis ini

Kontributor	Jenis Kontribusi
Kun Saidi	Mendesain eksperimen (70%) Menulis *paper* (70%)
Dr. Yudi Prayudi, S.Si., M.Kom	Mendesain eksperimen (30%) Menulis dan mengedit *paper* (30%)

Daftar Isi

Daftar Gambar

Daftar Tabel

Halaman Persembahan

Dengan mengucapkan syukur Alhamdulillah, Penelitian ini saya persembahkan pada orang-orang yang selama ini telah mendukung, memberikan semangat dan motivasi dalam menyelesaikan pendidikan magister komputer saya ini, secara khususnya kepada :

1. Ayahanda tercinta Imam Bisri yang telah wafat yang memberikan dukungan untuk melanjutkan studi dan Ibu saya tercinta Jaziroh yang selalu berdo'a dan mendukung setiap langkah saya. Tiada banyak kata yang dapat saya tuliskan untuk menggambarkan segala pengorbanan dan kasih sayang bapak dan ibu. Namun hanya doa yang dapat selalu kupersembahkan untuk bapak dan ibu. Terimakasih bapak, terimaksih ibu.
2. Kakak saya tercinta (Hidayati, Fitriani, dan Mawardinata). Terima kasih atas semua bantuan dan doa yang telah diberikan kepada saya selama menempu perkuliahan mulai dari jenjang strata satu hingga strata dua ini.

Semua penulis terpaksa lakukan untuk masa depan penulis.

Semua penulis lakukan untuk membanggakan keluarga.

Kata Pengantar

بِسْـــــــــــــمِ اللهِ الرَّحْمَنِ الرَّحِيْمِ

Assalamu'alaikum Wr. Wb.

Puji syukur penulis panjatkan kepada Allah SWT atas limpahan dan karunia yang diberikan kepada penulis sehingga dapat menyelesaikan laporan proposal penelitian tesis dengan judul "Analisis faktor utama dalam *information security - personality threat* terhadap *phishing attacks*" menggunakan metode *Technology Threat Avoidance Theory (TTAT)*. Adapun maksud dari penulisan laporan proposal penelitian ini adalah sebagai prasyarat dalam mencapai jenjang pendidikan Magister Teknik Informatika konsentrasi Forensika Digital di Fakultas Teknologi Industri, Universitas Islam Indonesia.

Dalam proses penyelesaian laporan proposal tesis ini, penulis tidak dapat menyelesaikan bila tidak ada turut serta dan membantu baik secara langsung maupun tidak langsung dalam menyelesaikan proposal penelitian ini, maka daripada itu penulis ingin menyampaikan rasa terimakasih kepada beberapa pihak yang telah mendukung dalam penyusunan tesis ini, antara lain:

1. Bapak Prof. Fathul Wahid, ST., M.SC., Ph.D, selaku rektor Universitas Islam Indonesia yang memberikan kesempatan kepada penulis untuk menima ilmu di Univeristas Islam Indonesia.
2. Bapak Prof. Hari Purnomo, M.T selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan bantuan untuk belajar.
3. Ibu Izzati Muhimmah, ST., M.Sc., Ph.D, selaku Ketua Program Studi Teknik Informatika Program Magister Fakultas Teknologi Industri, Universitas Islam Indonesia, yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Dr, Yudi Prayudi, S.Si., M.Kom selaku dosen pembimbing yang telah banyak meluangkan waktunya dalam memberikan berbagai saran selama proses bimbingan.
5. Seluruh dosen, staff administrasi dan civitas Magister Teknik Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung yang telah membantu penulis selama masa studi penulis.
6. Alm ayahanda tercinta yang telah membesarkan dan mendidik saya, semoga beliau bangga meliahat anak tercinta dapat menyelesaikan laporan proposal penelitian ini.

7. Seluruh keluarga baik ibu, kakak, dan keponakan tercinta yang telah mencurahkan segenap cinta, kasih sayang, perhatian dan dukugan baik moril maupun materiil.
8. Rekan – rekan mahasiswa MTI khususnya kosentrasi Forensika Digital angkatan XV yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain.
9. Pihak – pihak lain yang turut membantu dalam menyelesaikan laporan proposal penelitian ini yang tidak dapat disebutkan satu persatu oleh penulis.

Penulis menyadari bahwa laporan proposal penelitian ini masih memiliki kekurangan. Oleh karena itu dengan senang hati meneriam setiap saran atau komentar serta kritikan dari para dosen penguji guna menyempurnakan proses penelitian saya kedepannya. Akhir kata penulis mengucapkan terima kasih, semoga penyusunan laporan proposal penelitian ini dapat memberikan gambaran mengenai proses penelitian saya kedepannya.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, Desember 2020

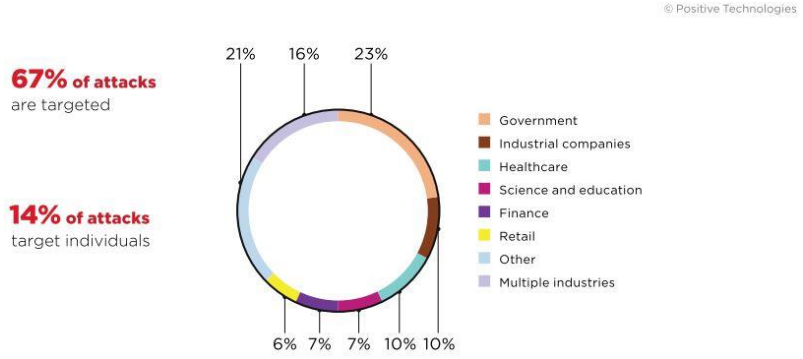
Penulis

BAB 1
Pendahuluan

1.1 Latar Belakang

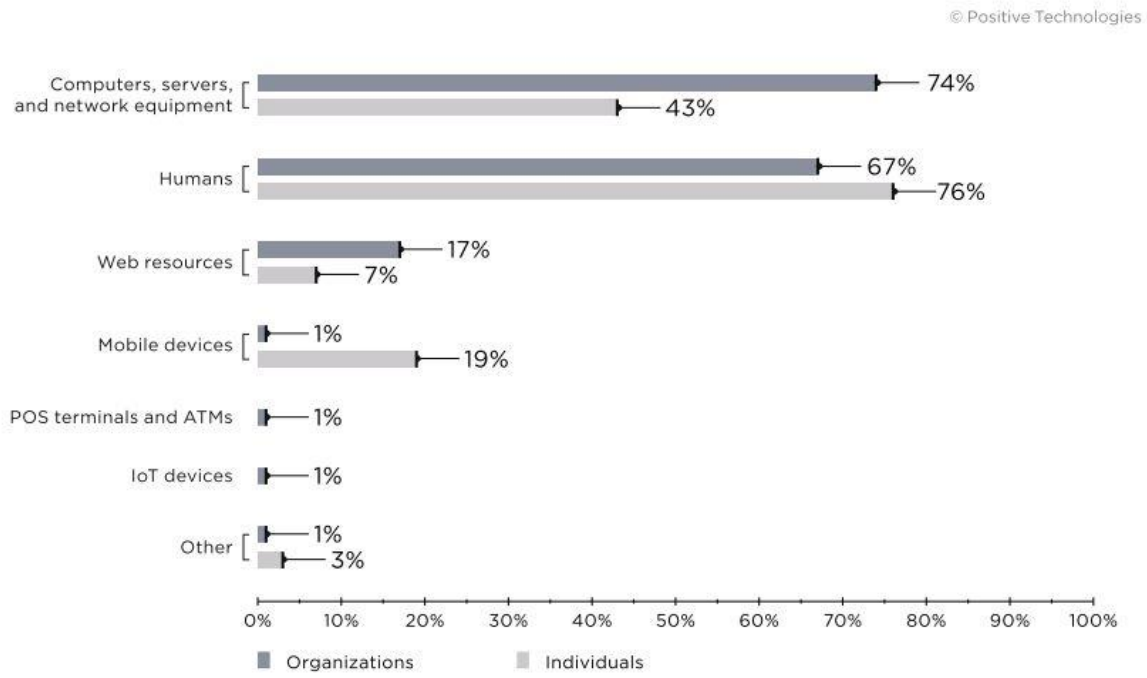
Seiring dengan berkembangnya teknologi yang semakin pesat, menyebabkan aktivitas masyarakat dengan menggunakan teknologi tersebut semakin tidak terkendali. Masyarakat dapat melakukan aktivitas yang berdampak pasitif maupun negatif dengan menggunakan teknologi. Dampak positif dari penggunaan teknologi tersebut yaitu sangat beragam seperti pada kegiatan akademik, sosial, kesehatan, dan lain sebagainya. Peningkatkan *Information and communication Technologies (ICT)* memberikan dukungan dan integrasi secara vital dalam setiap efek kehidupan dari keseharian mereka menjadi *electrical power system* yang merupakan bagian yang sangat penting (Jimada-Ojuolape & Teh, 2020). Namun demikian, penggunaan dari teknologi tersebut mempunyai dampak negatif seperti pada kejahatan dengan menggunakan alat bantu teknologi *(social engineering)* yang menyebabkan kerugian baik mental maupun finansial dari victim.

Social engineering (SE) merupakan kegiatan yang melibatkan *human* ,psikologi manusia, dan teknologi, sehingga menyebabkan kerugian dari victim tersebut dimana *computer science* dan sosial spikologi digunakan dalam menentukan bahaya *social engineering* terhadap partisipan (F. Mouton et al., 2013). Berdasarkan pada literatur (Positive Technologies, 2020) yang menerangkan bahwa metode *attackss* dapat mengancam berbagai macam institusi dimana *goverment, industrial companies, healthcare, science and education,* dan *finance* merupakan institusi terentan yaitu salah satunya dengan menggunakan SE *attackss*. Berikut merupakan info grafis mengenai beberapa institusi yang mengalami SE *attackss* dan terdapat pada Gambar 1.1



Gambar 1.1 Kategori Tingkat *Attacks* Terhadap Institusi 2020

Berdasarkan pada (Positive Technologies, 2020) mengenai metode kategori tujuan *attacks* yang digunakan oleh para *hacker* dalam memperoleh informasi di berbagai sektor organisasi/institusi, dimana metode yang digunakan oleh *hacker* tersebut berdasarkan pada tujuan *attacks* yaitu *computer, server and network* merupakan metode paling sering digunakan oleh para *hacker* tersebut, diikuti oleh *human* dan *web resources*. Berikut merupakan detail dari metode kategori *attacks target* digunakan *hacker* dalam *attackss* terhadap institusi tersebut yang tertuang pada Gambar 1.2



Gambar 1.2 Kategori *Attacks* Target 2020

Pada penelitian sebelumnya yang dilakukan oleh (Rege et al., 2019) mengenai edukasi dan keterbatasan kurikulum pendidikan khususnya strata-1 (sarjana) terhadap SE dengan objek siswa dan pengajar. Tujuan penelitian ini adalah meningkatkan kemampuan dalam pembuatan aplikasi *cybersecurity* yang baru dengan menggabungkan faktor dari *human*, aspek sosial, spikologi dan teknik interaksi social. Hasil penelitian ini adalah dapat memberikan solusi terhadap dampak dari *cybercriminal* dengan mempertimbangkan waktu yang dibutuhkan dalam pembuatan projek SE kurikulum pendidikan *cybersecurity* tersebut.

Dalam penelitian yang dilakukan oleh (Arachchilage & Love, 2014) mengenai pengujian *conceptual knowledge* atau *procedural knowledge* memiliki dampak positif pada *computer user's self-efficacy* terhadap *phishing attacks* dan melakukan evaluasi teori model yang berdasarkan pada (Liang & Xue, 2010) yaitu *Technology Threat Avoidance Theory (TTAT)*. Pengumpulan data berdasarkan pada 161 pengguna komputer yang aktif yang berdasarkan pada tanggapan pengguna melalui kuesioner *online*. Hasil dari penelitian ini

yaitu terdapat efek interaksi dari *conceptual* dan *procedural knowledge* mempunyai dampak positif terhadap *computer users' self-efficacy*, meningkatkan *avoidance behavior* terhadap ancaman *phishing*, dan berkontribusi terhadap edukasi keamanan terhadap *end-user* dengan baik.

Pada penelitian lainnya mengenai *phishing* dalam identifikasi ancaman *online,* dimana kesadaran akan bahaya *phishing* perlu untuk dipertimbangkan. Penelitian ini bertujuan untuk membuat desain *game framework* yang dapat digunakan untuk meningkatkan *avoidance behaviour* melalui *motivation to protect* pengguna dari *phishing attacks* dengan menggunakan model *Technology Threat Avoidance Theory (TTAT).* Pada penelitian ini menggunakan 150 pengguna komputer dalam mengisi kuesioner. Hasil dari penelitian ini menjelaskan bahwa elemen *perceived theat, safeguard effectiveness, safeguard costs, self-efficacy, perceived severity,* dan *perceived susceptibility* dapat digunakan dalam desain *game framework* pada pengguna komputer terhadap *phishing attacks* dan tidak hanya dapat digunakan dalam pencegahan *phishing attacks*, tetapi juga dapat mencegah serangan *malicious IT* yang lainnya seperti *virus, malware, botnets* dan *spyware* (Arachchilage & Love, 2013).

Penelitian yang lainnya mengenai pembuatan laporan berdasarkan pada desain dan pembuatan *game mobile prototype* sebagai perangkat *(tools)* edukasi. Perangkat *(tools)* tersebut menggunakan elemen dari pembuatan *framework game* yang digunakan dalam membantu melindungi pengguna komputer terhadap *phishing attacks* bedasarkan pada *pre-test* dan *post-test* yang terdapat pada *framework* tersebut. Tujuan dari desain *framework game mobile* yaitu meningkatkan *avoidance behavior* pengguna melalui *motivation to protect* pengguna dari *phishing attacks*. Hasil dari penelitian ini yaitu adanya perbaikan yang signifikan dari *phishing avoidance behavior* dari setiap partisipan pada pengujian *post-test.* Penelitian ini menerangkan bahwa *threat perception, safeguard effectiveness, self-efficacy, perceived severity* dan *perceived susceptibility* merupakan efek element positif terhadap *avoidance bahviour*, sedangkan *safeguard* memiliki efek negatif (Arachchilage et al., 2016)

Dalam penelitian yang lainnya mengenai kebutuhan kenyamanan pengguna *smartphone* dalam memilih pengaman kemananan yang berbeda terhadap ancaman *mobile phishing*. *Anti phishing self-efficacy* merupakan instrument dalam menjelaskan *mobile phishing avoidance behavior*. Penelitian ini bertujuan untuk membuat sebuah model yang menjelaskan bagaimana *anti-phishing self-efficacy* dengan *anticipated regret* dan *gender* mempengaruhi pengguna *smartphone* terhadap *phishing avoidance behavior.* Dengan menggunakan data dari 231 responden, penelitian menunjukkan bahwa pengaruh positif

yang secara langsung pada kedua yaitu *anti-phishing self-efficacy* dan *anticipated regret* pada *mobile phishing avoidance motivation* dan *behavior*. Sebagai tambahan, *gender* dengan signifikan mempengaruhi *anti-phishing self-efficacy* yaitu pada *avoidance behavior* dan *motivation* dengan hubungan yang terjadi lebih tinggi untuk wanita dibandingkan dengan pria. Hasil penelitian menunjukkan bahwa terdapat interaksi antara *anti-phishing self-efficacy* dengan *anticipated regret* dan *gender* dengan *mobile phishing avoidance behavior* (Verkijika, 2019)

Dari apa yang telah diterangkan sebelumnya mengenai *phishing attacks* yang terjadi di berbagai sektor organisasi/institusi dengan objek (mahasiswa dan dosen/staff/karyawan) dengan menggunakan faktor yang berpengaruh terhadap objek tersebut, maka diperlukan penelitian lebih lanjut mengenai analisis faktor yang mempengaruhi objek tersebut yaitu *perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard costs, self-efficacy (security awareness), behavioral intention, avoidance motivation,* dan *avoidance behavior* terhadap *phishing attacks* di sektor tersebut. Analisis faktor tersebut menggunakan metode MANOVA digunakan dalam proses data, sedangkan model *Technology Threat Avidance Theory (TTAT)* digunakan dalam analisis faktor *personality threat.* Analisis faktor tersebut bertujuan mengetahui keterikatan faktor yang sangat berpengaruh terhadap objek tersebut terhadap *phishing attacks* yang terjadi di sektor tersebut.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang yang telah dijelaskan sebelumnya mengenai berbagai macam SE *attacks* di berbagai sektor organisasi/institusi dengan objek (mahasiswa dan dosen/staff/karyawan) serta analisis faktor yang mempengaruhi objek (mahasiswa dan dosen/staff/karyawan), maka dapat dirumuskan rumasan masalah sebagai berikut.

- Bagaimana penerapan model penelitian kualitatif dan kuantitatif dalam analisis faktor *information security – personality threat* berdasarkan pada model *Technology Threat Avoidance Theory (TTAT)* terhadap terjadinya *phishing attacks* di berbagai sektor organisasi dan institusi ?
- Faktor apa yang memiliki keterkaitan dan sangat berpengaruh terhadap objek (mahasiswa dan dosen/staff/karyawan) terhadap terjadinya *phishing attacks* di berbagai sektor organisasi dan institusi berdasarkan pada analisis faktor berdasarkan pada model *Technology Threat Avoidance Theory (TTAT)*? *(perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard costs,*

self-efficacy (security awareness), behavioral intention, avoidance motivation, dan *avoidance behavior).*

1.3 Tujuan Penelitian

Berdasarkan pada rumusan masalah yang telah dijelaskan sebelumnya mengenai analisis faktor yang mempengaruhi objek (mahasiswa dan dosen/staff/karyawan) terhadap terjadinya *phishing attacks* yang terjadi di berbagai sektor organisasi/institusi dengan menggunakan model *Technology Treat Avoidance Theory (TTAT)*, maka didapatkan tujuan penelitian sebagai berikut.

- Menerapkan model penelitian kualitatif dan kuantitatif berdasarkan pada hasil pengumpulan data kuesioner model faktor TTAT. Model penelitian kualitatif digunakan dalam pengumpulan data berdasarkan pada pertanyaan kuesioner model faktor TTAT dan model penelitian kuantitatif digunakan dalam perhitungan data kuesioner tersebut dengan menggunakan metode MANOVA.
- Untuk dapat memahami dan analisa pada keterikatan antar faktor *(perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard costs, self-efficacy (security awareness), behavioral intention, avoidance motivation,* dan *avoidance behavior)* apa berdasarkan pada model tersebut yang sangat berpengaruh terhadap objek (mahasiswa dan dosen/staff/karyawan) terhadap terjadinya *phishing attacks* di berbagai sektor organisasi/institusi tersebut

1.4 Batasan Masalah

Setelah melakukan perumusan masalah, maka akan ditentukan batasan masalah dari penelitian ini, maka didapatkan batasan masalah. Batasan penelitian dilakukan agar penelitian ini lebih terarah yaitu sebagai berikut:

a. Responden/objek adalah mahasiswa, dosen/staff/karyawan di berbagai sektor orgnasasi/institusi yang mempunyai latar belakang pendidikan D3, S1, S2, dan S3
b. Menggunakan metode MANOVA digunakan dalam proses data, sedangkan model *Technology Treat Avoidance Theory (TTAT)* digunakan sebagai model yang digunakan dalam analisis faktor *personality threat.*

1.5 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan dapat memberikan kontribusi terhadap perkembangan ilmu pengetahuan dan para peneliti pada umumnya. Manfaat dari penelitian ini yaitu pada bidang keamanan informasi mengenai analisis keterikatan faktor model

Technology Treat Avoidance Theory (TTAT) meliputi faktor *perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard costs, self-efficacy (security awareness), behavioral intention, avoidance motivation,* dan *avoidance behavior* yang sangat berpengaruh terhadap objek (mahasiswa dan dosen/staff/karyawan) terhadap *phishing attacks* yang terjadi di berbagai sektor organisasi/institusi.

1.6 Literatur Review

Pada penelitian sebelumnya mengenai hubungan antara *the big five personality traits (Neuroticism, Extroversion, Openness, Agreeableness,* dan *Conscientiousness)* dengan 100 mahasiswa dari *Notheastern Engineering College* yang terdiri dari 83 laki – laki dan 17 wanita dan berusia 18 sampai 31 tahun terhadap serangan *phishing e-mail*. Tujuan dari penelitian ini adalah pengujian terhadap *the big five personality traits* tersebut yang merupakan faktor kerentanan tertinggi terhadap terjadinya *phishing attacks* dan *neuroticism traits* merupakan faktor yang paling berpengaruh diantara *the big five personality traits* tersebut berdasarkan pada 100 mahasiswa dari *Notheastern Engineering College*. Hasil penelitian tersebut, dimana wanita memiliki kencenderungan menjadi korban terhadap *attacks* yaitu sebesar 53% dibandingkan laki – laki yaitu sebesar 41%. Pada bagian yang lainnya, *attacks* dilakukan melalui *phising* akun *facebook*, dimana dengan mudah *user* menambahkan demografi dan melakukan *posting* (pesan dan foto) mereka yang menyebabkan mereka lebih rentan terhadap *attacks* tersebut. (Halevi et al., 2013).

Penelitian yang lainnya mengenai pembuatan laporan berdasarkan pada desain dan pembuatan *game mobile prototype* sebagai perangkat *(tools)* edukasi. Perangkat *(tools)* tersebut menggunakan elemen dari pembuatan *framework game* yang digunakan dalam membantu melindungi pengguna komputer terhadap *phishing attacks* berdasarkan pada *pre-test* dan *post-test* yang terdapat pada *framework* tersebut. Tujuan dari desain *framework game mobile* yaitu meningkatkan *avoidance behavior* pengguna melalui *motivation to protect* pengguna dari *phishing attacks*. Hasil dari penelitian ini yaitu adanya perbaikan yang signifikan dari *phishing avoidance behavior* dari setiap partisipan pada pengujian *post-test.* Penelitian ini menerangkan bahwa *threat perception, safeguard effectiveness, self-efficacy, perceived severity* dan *perceived susceptibility* merupakan efek element positif terhadap *avoidance bahviour*, sedangkan *safeguard* memiliki efek negatif (Arachchilage et al., 2016)

Pada penelitian lainnya mengenai *phishing* dalam identifikasi ancaman *online,* dimana kesadaran akan bahaya *phishing* perlu untuk dipertimbangkan. Penelitian ini bertujuan untuk membuat desain *game framework* yang dapat digunakan untuk meningkatkan *avoidance behavior* melalui *motivation to protect* pengguna dari *phishing*

attacks dengan menggunakan model *Technology Threat Avoidance Theory (TTAT).* Pada penelitian ini menggunakan 150 pengguna komputer dalam mengisi kuesioner. Hasil dari penelitian ini menjelaskan bahwa elemen *perceived theat, safeguard effectiveness, safeguard costs, self-efficacy, perceived severity,* dan *perceived susceptibility* dapat digunakan dalam desain *game framework* pada pengguna komputer terhadap *phishing attacks* dan tidak hanya dapat digunakan dalam pencegahan *phishing attacks*, tetapi juga dapat mencegah serangan *malicious IT* yang lainnya seperti *virus, malware, botnets* dan *spyware* (Arachchilage & Love, 2013).

Penelitian yang lainnya mengenai *Information Security (Isec) Training Effectiveness* yaitu dengan menguji dampak terhadap koordinasi pembelajaran dari setiap organisasi yang mulai mengerti akan pentingnya pendidikan dan pelatihan keamanan *(security)* dan upaya *(efforts).* Penelitian ini memiliki *gap* yang harus dikerjakan antara lain identifikasi karakteristik yang sesuai dalam mendesain *training programs* dengan menggunakan karakteristik tersebut sebagai petunjuk dalam mendesain sebuah *web-based information security training*, evaluasi keefektivan berdasarkan pada percobaan *training* dengan menggunakan *critical* sebagai *outcome* seperti *training satisfaction, security training performance, self-efficacy, perceived threat sevetiry* dan *susceptibility*. Hasil dari penelitian ini bahwa *web-based Isec training* dapat menggabungkan koordinasi dari setiap pembelajaran dengan positif berdasarkan pada hasil *training* dan pembelajaran tersebut (Abraham & Chengalur-Smith, 2019)

Dalam penelitian yang lainnya yaitu dalam mengatasi dampak *anti-phishing self-efficacy* terhadap mahasiswa dari universitas (*internet self-efficacy, anti phishing behavior*, dan *gender* sebagai variable). Penelitian menggunakan survey berdasarkan pada *convenience sampling* 434 mahasiswa dari universitas sebagai partisipan yang memiliki pengalaman menggunakan internet dan 411 partisipan dapat merespon dengan valid dari seluruh responden tersebut. Berdasarkan pada perhitungan statistik *(SEM analisys),* terdapat perbedaan yang signifikan antara *anti-phishing behavior indicator* dan *anti-phishing self-efficacy indicator* antara mahasiswa laki – laki dan perempuan, dan *internet self-efficacy faktor* memiliki kecenderungan yang positif terhadap *anti-phishing behavior faktor*. Hasil penelitian ini yaitu faktor tersebut dapat memperbaiki *internet self-efficacy indicator* dan *anti-phishing self-efficacy indicator* dalam meningkatkan *learning motivation* dan *anti-phishing experience*, sehingga dapat digunakan sebagai referensi dalam bahan pembelajaran yang adaptif (Sun et al., 2016)

Dalam peneltian yang lainnya mengenai kebutuhan kenyamanan pengguna *smartphone* dalam memilih pengaman kemananan yang berbeda terhadap ancaman *mobile phishing*. *Anti phishing self-efficacy* merupakan instrument dalam menjelaskan *mobile phishing avoidance behavior*. Penelitian ini bertujuan untuk membuat sebuah model yang menjelaskan bagaimana *anti-phishing self-efficacy* dengan *anticipated regret* dan *gender* mempengaruhi pengguna *smartphone* terhadap *phishing avoidance behavior.* Dengan menggunakan data dari 231 responden, penelitian menunjukkan bahwa pengaruh positif yang secara langsung pada kedua yaitu *anti-phishing self-efficacy* dan *anticipated regret* pada *mobile phishing avoidance motivation* dan *behavior*. Sebagai tambahan, *gender* dengan signifikan mempengaruhi *anti-phishing self-efficacy* yaitu pada *avoidance behavior* dan *motivation* dengan hubungan yang terjadi lebih tinggi untuk wanita dibandingkan dengan pria. Hasil penelitian menunjukkan bahwa pemahaman yang tinggi mengenai *mobile phishing avoidance behavior* yaitu terdapat Hasil penelitian menunjukkan bahwa terdapat interaksi antara *anti-phishing self-efficacy* dengan *anticipated regret* dan *gender* dengan *mobile phishing avoidance behavior* (Verkijika, 2019)

Penelitian yang lainnya mengenai pengujian *conceptual knowledge* atau *procedural knowledge* memiliki dampak positif pada *computer user's self-efficacy* terhadap *phishing attacks* dan melakukan evaluasi teori model yang berdasarkan pada (Liang & Xue, 2010) yaitu *Technology Threat Avoidance Theory (TTAT)*. Pengumpulan data berdasarkan pada 161 pengguna komputer yang aktif yang berdasarkan pada tanggapan pengguna melalui kuesioner *online*. Hasil dari penelitian ini yaitu terdapat efek interaksi dari *conceptual* dan *procedural knowledge* mempunyai dampak positif terhadap *computer users' self-efficacy*, meningkatkan *avoidance behavior* terhadap ancaman *phishing*, dan berkontribusi terhadap edukasi keamanan terhadap *end-user* dengan baik (Arachchilage & Love, 2014).

Penelitian yang lainnya mengenai *good information security awareness (ISA)* dan *computer ethics* dengan menggunakan survey kuantitatif terhadap 87 siswa (17 siswa diploma, 31 siswa sarjana, dan 31 siswa master) dengan umur partisipan yaitu antara 20 – 69 tahun. Faktor jenis kelamin, level pendidikan, dan program studi merupakan faktor yang digunakan pada penelitian ini. Hasil dari penelitian ini menunjukkan bahwa faktor level pendidikan dan *computer ethics* merupakan faktor dominan terhadap ISA, akan tetapi *awareness* pada berbagai aspek perlu ditingkatkan (Filippidis et al., 2018).

Dalam peneltian yang lainnya mengenai penggunaan *information security awareness (ISA)* terhadap siswa dari universitas dan bagaimana melakukan analisis dampak faktor perbedaan dari individu dengan melalui pendekatan survey deskriptif dan kuesioner terhadap

614 responden dari 30 item departemen yang terdapat pada universitas. Hasil dari penelitian ini menyatakan bahwa faktor jenis kelamin, umur, dan pengalaman memiliki korelasi statistika yang tinggi terhadap ISA yang termasuk didalamnya adalah kebiasaan individu (Farooq et al., 2015).

Pada penelitian yang mengenai metode *phising* yang termasuk dalam SE dengan menggunakan sebuah pesan resmi dan digunakan untuk menyerang korban dari organisasi / institusi tertentu. *Phising attackss* digunakan untuk menyerang target (korban) yang digunakan untuk menggagalkan informasi rahasia seperti *password*, detail dari kartu kredit, nomor akun bank, atau informasi sensitif lainnya. Kebiasaan manusia *(human)* dan teknologi adalah dua aspek penting dalam menyerang dengan menggunakan *phising* yang lebih fokus terhadap teknologi. Pengujian *phising attackss* tersebut menggunakan objek manusia *(human)* lebih dari 10.000 komunitas dari universitas amerika sharjah (AUS) yang meliputi mahasiswa, almuni, dan staff dengan mengirim pesan melalui *spoofed e-mail* yang dianggap sebagai pesan resmi oleh *user*. Tujuan dari penelitian tersebut yaitu mendapatkan faktor yang akan menjadi kerentanan terjadinya *phising attackss* di AUS, dimana jenis kelamin, umur, dan demografis merupakan faktor yang menyebabkan terjadinya *phising attackss* tersebut (Mohebzada Jamshaid G, Zarka Ahmed El, Bhojani H.Arsalan, 2012).

Dalam penelitian yang lainnya mengenai *awareness* SE terhadap siswa di *International Islamic University Malaysia (IIUM)* dengan pengumpulan data sebesar 245 siswa melalui *online survey* (kuesioner) berdasarkan pada pengujian *E-Mail Phising* yang terdapat di *CyberSAFE – IIUM Website* selama 6 bulan. Tujuan dari penelitian ini adalah pembuatan digital forensik *tools* yang lebih mudah dalam penggunaan terhadap pengujian digital forensik dan menggunakan anti-forensik dalam pendeteksian malicious, serta menguji apakah siswa teknologi informasi lebih aman dari SE, dibandingkan dengan siswa jurusan selain teknologi informasi. Hasil dari penelitian ini adalah siswa teknologi informasi mempunyai *awareness* SE lebih tinggi dibandingkan dengan siswa jurusan lainnya dan merekomendasikan *awareness* (Adam & Yousif, 2011).

Pada penelitian lainnya yang dilakukan oleh (Kim, 2014) mengenai penggunaan sistem teknologi informasi (IT/IS) melalui media *online course*, *instant messaging (e-mail dan social media)*, dan *smartphone* terhadap aktivitas siswa dari sekolah menjadi semakin tinggi, sehingga dibutuhkan perlindungan terhadap informasi pribadi mereka yang mungkin menjadi target dari *security attacks* dengan menggunakan *Information security awarenees training (ISAT)*. Metode yang digunakan dalam penelitian ini yaitu dengan menggunakan *quetionnaire survey* melalui media *E-Mail* terhadap 357 siswa sarjana dan pascasarjana dari

berbagai macam universitas di New England. Hasil dari penelitian ini adalah menghasilkan tingkat hubungan yang signifikan antara *security training* dan persepsi siswa terhadap kemanan sistem informasi.

Dalam penelitian yang lainnya mengenai penggunaan *information security awareness (ISA)* dan edukasi dari *computer ethics* dengan menggunakan survey kuantitatif terhadap 87 siswa (17 siswa diploma, 31 siswa sarjana, dan 31 siswa master) dengan umur partisipan yaitu antara 20 – 69 tahun. Faktor jenis kelamin, level pendidikan, dan program studi merupakan faktor yang digunakan pada penelitian ini. Hasil dari penelitian ini menunjukkan bahwa faktor level pendidikan dan *computer ethics* merupakan faktor dominan terhadap ISA, akan tetapi *awareness* pada berbagai aspek perlu ditingkatkan (Filippidis et al., 2018).

Dalam peneltian yang lainnya mengenai penggunaan *information security awareness (ISA)* terhadap siswa dari universitas dan bagaimana melakukan analisis dampak faktor perbedaan dari individu dengan melalui pendekatan survey deskriptif dan kuesioner terhadap 614 responden dari 30 item departemen yang terdapat pada universitas. Hasil dari penelitian ini menyatakan bahwa faktor jenis kelamin, umur, dan pengalaman memiliki korelasi statistika yang tinggi terhadap ISA yang termasuk didalamnya adalah kebiasaan individu (Farooq et al., 2015).

Dari apa yang telah diterangkan sebelumnya mengenai *phishing attacks* yang terjadi di berbagai sektor organisasi/institusi dengan partisipan (mahasiswa dan dosen/staff/karyawan) berdasarkan pada faktor yang terdapat pada literatur, maka diperlukan penelitian lebih lanjut mengenai analisis faktor yang mempengaruhi partisipan tersebut yaitu *perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard costs, self-efficacy (security awareness), behavioral intention, avoidance motivation,* dan *avoidance behavior* terhadap *phishing attacks* di berbagai sektor organisasi/institusi dengan menggunakan metode MANOVA (*multivariate tests* dan *pairwise comparisons*). Analisis faktor tersebut bertujuan mengetahui keterikatan antar faktor yang sangat berpengaruh terhadap partisipan tersebut, sehingga partisipan dapat mencegah menjadi korban *cybercrime* terhadap *phishing attacks* yang terjadi di sektor tersebut.

Agar mempermudah dalam memahami litertatur yang digunakan dalam penelitian ini yang berdasarkan penelitian – penelitian sebelumnya. Tabel dibawah ini merupakan tabel literatur review yang digunakan dalam penelitian ini.

Tabel ***Error! No text of specified style in document.****.1.1* Literatur Review

No.	Nama	Tujuan	Metode	Hasil
1.	(Rege et al., 2019)	Meningkatkan kemampuan siswa dan pengajaran dalam pembuatan aplikasi *cybersecurity*.	*Security awareness training*	Dapat memberikan solusi terhadap dampak dari *cybercriminal.*
2.	(Adam & Yousif, 2011)	Menguji apakah siswa IIUM dengan teknologi informasi lebih aman dari SE, dibandingkan dengan siswa jurusan selain teknologi informasi.	*Anti-forensic tools*	Siswa teknologi informasi mempunyai *awareness* SE lebih tinggi dibandingkan dengan siswa jurusan lainnya dan merekomendasikan *awareness.*
3.	(Kim, 2014)	Perlindungan terhadap informasi pribadi siswa yang menjadi target dari *security attacks.*	*Information security awarenees training (ISAT).*	Mendapatkan hasil mengenai tingkat hubungan yang signifikan antara *security training* dan persepsi siswa terhadap kemanan sistem informasi
4.	(Filippidis et al., 2018)	Menemukan faktor yang mempengaruhi terhadap penggunaan *information security awareness (ISA)* yang baik dan edukasi *computer ethics.*	*Information security awarenees training (ISAT).*	Mendapatkan hasil bahwa faktor level pendidikan dan *computer ethics* merupakan faktor dominan terhadap ISA

5.	(Farooq et al., 2015)	Menghasilkan faktor perbedaan dari individu	*Information security awareness (ISA)*	Faktor jenis kelamin, umur, dan pengalaman memiliki korelasi statistika yang tinggi terhadap ISA (*information security awareness)*
6.	(Arachchilage & Love, 2014)	Pengujian *conceptual knowledge* atau *procedural knowledge* pada *computer user's self-efficacy* terhadap *phishing attacks* dan melakukan evaluasi teori model	*Technology threat avoidance theory (TTAT)*	Terdapat efek interaksi dari *conceptual* dan *procedural knowledge* mempunyai dampak positif terhadap *computer users' self-efficacy*, dan meningkatkan *avoidance behavior* terhadap ancaman *phishing.*
7.	(Abraham & Chengalur-Smith, 2019)	Identifikasi karakteristik yang sesuai dalam mendesain *training programs* pada *web-based information security training*. Evaluasi keefektivan berdasarkan pada *training* dengan menggunakan *critical* sebagai *outcome (training satisfaction, security training performance,*	*Information Security (Isec) Training Effectiveness*	Penggabungan antara *web-based Isec training* dengan hasil *training* yaitu positif.

		self-efficacy, perceived threat sevetiry dan susceptibility).		
8.	(Arachchilage et al., 2016)	Meningkatkan *avoidance behaviour* pengguna melalui *motivation to protect* pengguna dari *phishing attacks*	*Pre-test* dan *post-test* yang terdapat pada *framework*	*Threat perception, safeguard effectiveness, self-efficacy, perceived severity* dan *perceived susceptibility* merupakan efek elemen positif terhadap *avoidance bahviour*, sedangkan *safeguard* memiliki efek negatif
9.	(Verkijika, 2019)	Pembuatan sebuah model mengenai *anti-phishing self-efficacy, anticipated regret* dan *gender* terhadap pengguna *smartphone (phishing avoidance behavior).*	*Common method variance (CMV)*	Pengaruh positif terhadap *anti-phishing self-efficacy* dan *anticipated regret* pada *mobile phishing avoidance motivation* dan *behavior*
10.	(Arachchilage & Love, 2013)	Pembuatan desain *game framework* yang dapat digunakan untuk meningkatkan *avoidance behaviour* melalui *motivation to protect* pengguna dari *phishing attacks*	*Technology Threat Avoidance Theory (TTAT)*	Elemen *perceived theat, safeguard effectiveness, safeguard costs, self-efficacy, perceived severity,* dan *perceived susceptibility* dapat digunakan dalam desain *game framework* pada pengguna komputer

				terhadap *phishing attacks* dan digunakan dalam pencegahan serangan *phishing attacks (malicious IT.* seperti *virus, malware, botnets* dan *spyware)*.

1.7 Metodologi Penelitian

Analisis / Metodologi penelitian ini merupakan susunan langkah – langkah yang digunakan dalam menyelesaikan penelitian ini. Adapun tahapan – tahapan penelitian yang akan digunakan dalam peneltian ini antara lain:

a. Persiapan Analisis dan Pengujian Faktor

   Analisis faktor merupakan langkah persiapan analisis dan pengujian faktor *personality threat* yang terdapat dalam model *Technology Thread Avoidance Theory (TTAT).*

b. Pengumpulan Data Kuesioner

   Pengumpulan data koesioner merupakan metode dalam membuat daftar pertanyaan yang digunakan pada kuesioner penelitian berdasarkan pada literatur yang digunakan, setelah langkah persiapan analisis dan pengujian faktor.

c. Predictor Online Survey

   Predictors Online Survey merupakan partisipan (mahasiswa dan dosen/staff/karyawan) yang bekerja diberbagai sektor di Indonesia dan digunakan sebagai sumber data berdasarkan pada kuesioner pengumpulan data dalam bentuk *google form (online),* setelah langkah pengumpulan data kuesioner.

d. Analisis dan Pengujian Faktor

   Analisis dan pengujian faktor merupakan langkah proses perhitungan terhadap hasil pengumpulan data sebelumnya dengan meggunakan faktor model *Technology Thread Avoidance Theory (TTAT),* setelah langkah *predictor online survey*. Perhitungan MANOVA menggunakan faktor model TTAT meliputi variabel independen dan variabel dependen yang terdapat pada metode tersebut.

e. Hasil Analisis dan Pengujian

   Hasil pengujian merupakan hasil pengujian variabel independen dan dependen yang terdapat pada metode tersebut dengan menggunakan aplikasi SPSS 25 berdasarkan pada metode MANOVA (*multivariate tests* dan *pairwise comparisons*), serta menghasilkan keterkaitan antar variabel dependen dan variabel independen.

f. Laporan

   Laporan merupakan kesimpulan dari masing – masing program yang meliputi persiapan analisis faktor, pengumpulan data kuesioner, *prediktor training survey*, analisis dan pengujian faktor, dan hasil analisis dan pengujian. Pada tahapan ini terdapat *future work researach* untuk dapat dikembangkan pada penelitian selanjutnya.

1.8 Sistematika Penelitian.

Tahapan ini merupakan gambaran secara umum mengenai sistematika penulisan dari penelitian ini yang bertujuan untuk menjelaskan secara ringkas terkait penulisan.

BAB I Pendahuluan

Tahapan ini merupakan tahapan awal yang dilakukan dalam penelitian. Pada tahapan ini terdapat penjelasan mengenai latar belakang masalah penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II Landasan Teori

Pada tahapan ini terdapat penjelasan tentang beberapa teori pendukung dalam penelitian yang sedang dikerjakan mengenai faktor dari model *Technology Thred Avoidance Theory (TTAT)* yang terdapat pada literatur yang digunakan.

BAB III Analisis / Metodologi Penelitian

Pada tahapan ini terdapat penjelasan secara umum mengenai analisis/metodologi terhadap faktor dari model *Technology Thred Avoidance Theory (TTAT)* yang terdapat pada literatur yang digunakan.

BAB IV Pengujian Faktor

Pada tahapan ini membahas mengenai hasil dan pembahasan dari usulan analisis/metodologi penelitian dengan menggunakan metode MANOVA *(multivariate tests dan pairwise comparisons).*

BAB V Kesimpulan dan Saran

Pada tahapan ini merupakan tahapan akhir yang dilakukan peneliti dalam menjelaskan kesimpulan secara keseluruhan pada setiap bab sebelumnya, serta saran yang dapat digunakan oleh peneliti lainnya dalam pengembangan penelitian selanjutnya.

Daftar Pustaka.

Daftar pustaka merupakan referensi yang terkait dengan penelitian yang meliputi buku, artikel, jurnal, makalah, situs yang terkait dan dapat menunjang kegiatan penelitian selanjutnya.

BAB 2
Kajian Pustaka

2.1 Social Engineering

Definisi dari *Social Engineering (SE)* berdasarkan pada (Chenoweth, 2005) yaitu teknik yang digunakan untuk exploitasi kerentanan manusia dengan menggunakan jalan pintas berupa *system security* untuk mendapatkan sekumpulan informasi, dengan kata lain SE *attacks* merupakan interaksi penting antara antar individu dan aspek spikologis dari SE. SE merupakan sebuah ancaman yang nyata pada sebuah industri dalam perkembangannya ke depan, akan tetapi industri sangat tidak menjadikan ancaman utama terhadap SE tersebut. Sehingga *social engineer* tersebut sulit dalam melakukan identifikasi target tersebut (Bezuidenhout et al., 2010).

2.2 Phishing

Phishing merupakan sebuah serangan yaitu dengan membuat *fake website* / mengajuk / tidak resmi (illegal) sebagai cara *attacker* dalam menghilangkan informasi sensitif pengguna seperti *username, password,* nomor akun bank, nomor kartu kredit atau nomor keamanan sosial lainnya. Informasi sensitif tersebut kemudian digunakan untuk mengakses akun personal, sehingga dapat mencuri uang *(financial loss)* dan pencurian identitas. Dalam beberapa tahun terakhir, *phising scams* meningkat secara ekponensial dan memiliki target pada setiap sektor sosial serta mengirimkan *bait* dan *wait* untuk menghasilkan informasi sensitif tersebut (Rao & Ali, 2015).

2.2.1 Phishing E-Mail

Phishing E-Mail merupakan *e-mail* yang dibuat antara SE dan metode dalam mencuri informasi rahasia dari *user* dan melakukan ekspolit karaktersitik terhadap kebiasaan manusia *(human)* serta meningkatkan kesempatan untuk mendapatkan sesuatu dari kebiasaan manusia yang sedang dilakukan. Jadi *Phishing E-Mail* merupakan karakteristik dari *exploitation* dan *deception*. *Phishing e-mail* dapat membuat kepercayaan mereka (manusia) terhadap informasi rahasia mereka menjadi entitas yang legal (resmi). Berdasarkan pada kepercayaan mereka, dimana *provider* pengirim yang legal dapat meyakinkan *user* dalam melengkapi request mereka. *Phishing Attacks* bergantung pada kemampuan *user* dalam membedakan antara entitas legal dan tidak legal dan kepercayaan terhadap entitas legal yaitu user dapat menggagalkan informasi rahasia mereka terhadap akun mereka (Alseadoon, 2014)

2.3 Information Security Awareness

Informasi dapat didefinisikan sebagai suatu sumber, komoditas, dan persepsi dari informasi yang mempengaruhi kehidupan mereka (Braman, 1989). Informasi mempunyai beberapa karakteristik yang membuat penting terhadap penerima dan pengirim informasi tersebut. Beberapa percaya bahwa *confidentiality, integrity,* dan *availability* (Charles P. Pfleeg, Shari Lawrence Pfleeger, 2015) adalah karakterisitk penting yang seharusnya menjadi batasan, sedangkan yang lainnya seperti *avalibility, accuracy, authenticity, integrity, utility,* dan *possession* (Whitman & Mattord, 2011) adalah karakteristik penting dari informasi. Namun, dalam banyak kasus pengukuran *information security* bahwa informasi tidak dapat diakses, digunakan, diungkap, terganggu, dimodifikasi, dilihat, direkam, atau dibuat ulang dengan entitas yang tidak resmi (Caldas, 2003). *Information security awarenees (ISA)* hanya se-waktu digunakan secara langsung terhadap individu ke dalam *information security* yang seharusnya individu tersebut memperhatikan dan memastikan pengaruh dari ISA tersebut (Mikkot Siponen, 2001).

Penelitian mengenai pengujian ISA memiliki target kepada publik umum dan para pekerja secara langsung, sementara untuk yang lainnya memiliki objek lebih spesifik serta alami *(nature)* (Zain, 2018). ISA digunakan dalam meningkatkan *pressure, penalties,* dan *perceived effectiveness* pada sebuah organisasi (Herath & Rao, 2009) dengan menggunakan survey terhadap *password users* sebagai target pengujian yang sering digunakan pada organisasi tersebut (Hodges & Buckley, 2017). ISA dalam organisasi tersebut menggunakan *security feature* pada aplikasi dan *security information policy* yang berbeda berdasarkan pada kepercayaan dan ketertarikan secara formatif (Mikko Siponen et al., 2010).

2.3.1 Social Engineer Attacks Framework

Social engineer harus memiliki beberapa keahlian, teknik yang efektif dan mencari kelemahan dari manusia, sehingga *human* dapat terhindar dari *attacks* dengan tanpa pemberitahuan sebelumnya *(preventive)* (Bezuidenhout et al., 2010). SE *attacks* merupakan sebuah *attacks* yang dibuat berdasarkan pada *direct communication* atau *indirect communication* dan melibatkan seorang *social engineer,* seorang target, sebuah medium, suatu tujuan, satu atau lebih sebagai prinsip pelengkap dan satu atau lebih teknik (Francois Mouton et al., 2014). SE *framework* merupakan *framework* dibuat oleh seorang *social engineer* dengan berbagai macam literatur mengenai SE *framework* pada penelitian sebelumnya.

2.3.2 Seven Psycological Vulnerabilities

Dalam mempertahankan melawan kerentanan spikologi yang berpotensi dengan sukses, maka seseorang membutuhkan pemahaman dari kerentanan spikologi yang berpotensi tersebut yang digunakan selama SE *attacks* terjadi. Berikut merupakan penjelasan mengenai tujuh kerentanan spikologi manusia menurut (Mcguiness & Mcguiness, 2019):

- Strong Affect

Ketika kekuatan emosi dipengaruhi oleh kemarahan, kegembiraan, ketakutan atau kecemasan, dan kemampuan kognitive individual terhambat dengan serius yang mempengaruhi kemampuan mereka dalam mengambil keputusan secara rasional, melakukan evaluasi dari situasi, membuat argumen kontra, dan alasan yang masuk akal, serta bagaimana dapat digunakan oleh *social engineer* dengan efektif (Broadhurst & Chantler, 2012).

- Reciprocation

Satu hal yang dapat membedakan dengan yang lainnya yaitu teori pergantian sosial dimana individu dapat menerima beberapa informasi dari yang lainnya dan berfikir mengenai kawajiban terhadap *reciprocation* dari individu tersebut. *Social engineer* membuat sebuah masalah terhadap individu dan membuat kembali individu tersebut berfikir mengenai kewajiban pemberian informasi dari individu tersebut (Workman, 2009).

- Overloading

Teknik ini mempunyai sebuah elemen dengan hasil bahwa individu menenangkan diriya dengan cara kognitif dan melalui persuasif aksioma (Broadhurst & Chantler, 2012). *Deceptive relationship* untuk menghasilkan informasi, *social engineer* akan melakukan identifikasi individu terhadap tujuan membangun dan membuat sebuah relationship. Hal ini dapat diselesaikan dengan sebuah tujuan tertentu yang menjadi kecenderungan individu untuk menyebarkan informasi secara luas dengan mempererat *relationship* (Broadhurst & Chantler, 2012)

- Diffusion of responsibility and moral duty.

Individu dibuat untuk percaya bahwa tindakan mereka agar mendapatkan informasi, bahkan dengan melawan kebijakan tertentu yang akan menghasilkan keuntungan dan konsekuensi tertentu, seperti untuk membantu karyawan dari institusi tertentu (Broadhurst & Chantler, 2012)

- Authority.

Social engineer menggambarkan seorang figur yang memiliki otoritas, individu lebih memungkinkan dalam memenuhi permintaan untuk mendapatkan informasi dimana seorang figur tersebut tersirat secara implisit merespon kondisi mengikuti harapan dan permintaan mereka dengan melakukan kombinasi ketakutan terhadap individu dengan otoritas asli datang dan melakukan verifikasi terhadap keaslian mereka (Broadhurst & Chantler, 2012; Workman, 2009).

- Integrity and Consistency

Individu mempunyai kecenderungan untuk menipu dan menegakkan komitmen mereka, bahkan jika mereka bukan menjadi orang tersebut (Broadhurst & Chantler, 2012).

2.3.4 Caldini's Six Priciples

Caldini's principles mempengaruhi eksperiment terhadap *SE personality framework (SEPF)* dan dapat digunakan dalam SE. Cialdini's principles mempengaruhi spikologi Gragg's yang secara explisit menggantikan penggunaan SE attackss. Berdasarkan pada penelitian (Scheeres, 2008) yang menggunakan persuasif dari Cialdini's psychologi sebagai basis teori untuk SE dan berikut merupakan six principle tersebut:

- Authority

Mayoritas orang melengkapi otoritas (Milgram, 1965) jika mereka membujuk mereka untuk melakukan perlawanan kepercayaan dan etika yang menggunakan simbol dari otoritas seperti seragam, keuangan, dan percakapan *telephone* dimana otoritas dapat dengan mudah menjadi rentan. Dua tipe dari otoritas yang ada yaitu berdasarkan pada expertise dan bergantung pada *relative hierarchical position* dala organisasi / masyarakat (Skitka & Mckeever, n.d.).

- Commitment & Consistency

Komitmen adalah suatu aksi dari permulaan tetang bagaimana orang berfikir mengenai diri orang tersebut dan apa yang dilakukan, ketika konsisten membuat orang konsisten terhadap komitmen diri orang tersebut dan percaya menggagalkan prinsip yang mempengaruhinya dengan tingkat kesuksesan tinggi. (Skitka & Mckeever, n.d.).

- Reciprocity.

Suatu norma sosial yang kuat bahwa kewajiban kita untuk membayar membayar orang lain untuk bagaimana kita menerima bentuk dari mereka. *Relationship* dibangun berdasarkan pada masyarakat dan membantu dalam membangun kepercayaan dengan yang lainnya serta menggantikan kebutuhan kita dalam keadilan. Kekuatan utama dalam *reciprocity* dapat

menjadi sangat tinggi dan menjadi target kembali ketika pengumpulan kebaikan dibandingkan dengan apa yang diterima.

- Liking.

Jika kamu membuatnya dan orang menjadi suka, itu sangat sulit terhadap mereka menjadi resisten menyukai kamu kembali. Dengan melengkapi permintaan dari orang yang memahi dan menyukai, sehingga motivasi dari fundamental dapat dibuat dan diperbaiki *relationship* sosial. Meningkatkan persamaan pelengkap yang dapat berasal dari orang yang dipertanggungjawabkan kedepannya. Hal ini dapat menjadi rendah dalam menyebarkan nama atau hari lahir.

- Social Proof.

Berdasarkan pada kepercayaan dan kebiasaan dari orang disekitar kita untuk menjadi *"accepted"* secara sosial. Bukti sosial dapat melengkapi level kepercayaan tertinggi terhadap orang yang menyebarkan pendapat sama khususnya dalam situasi yang ambigu.

- Scarcity.

Mendesain dengan bernilai lebih terhadap rendahnya ketersediaan kesempatan yang menyebabkan percepatan dari ketersediaan terhadap kualitas. Terlebih jika sesuatu menjadi langka dan rasa kebebasan menjadi berkurang. Teori reaktansi (Loss & Reactance, 1993) menyatakan bahwa respon terhadap kelangkaan dengan menunggu untuk mendapatkan kelangkaan menjadi lebih langka dibandingkan sebelumnya. Bahkan akses informasi lebih terbatas dan berharap menjadi lebih baik.

2.4 Information Security Self-Efficacy (ISSe)

Self-efficacy (SE) adalah sebuah bentuk dari evaluasi pada diri sendiri, di mana penentuan proksimal dari kebiasaan *(behaviour)* manusia. SE menggantikan *individual's belief* pada kemampuan mereka terhadap organisasi berdasarkan pada motivasi dan sumber kognitif. *Users* dengan level tinggi dari SE menunjukkan level tinggi dari SE yaitu mengenai keberhasilan terhadap implementasi SE. SE berdampak pada *effort, self-regulation, persistence* atau inisiasi pada hal tersebut *(Information security self-efficacy (ISSe)*. Menurut penelitian dari (Rhee et al., 2009) menjelaskan bahwa ISSe merupakan landasan utama dari *protection – behaviors*. Sejak *individual employee's* dilengkapi dengan kebijakan *information security* yang sangat berpengaruh terhadap keberhasilan dari kebijakan tersebut. Meskipun demikian, pemahaman mengenai kepercaayaan pekerja merupakan merupakan pemahaman yang wajib dimiliki.

2.5 Technology Threat Avoidance Theory (TTAT)

Beradasarkan pada (Liang & Xue, 2009) mengenai *Technology Threat Avoidance Theory (TTAT)* dapat menjelaskan serangan IT terhadap *avoidance behavior* berdasarkan pada sistem yang dinamis, teori *cybernetic,* berbagai serangan IT, dan populasi users. TTAT menyediakan *framework* yang relevan dalam menjelaskan *avoidance* dari fenomena *malicious,* dimana tidak dapat dijelaskan dengan tepat dengan menggunakan *information system (IS)* atau pendekatan beberapa teori. TTAT menjelaskan bahwa *users* dapat merasakan serangan IT yang terjadi dan mereka dapat merespon positif serta memiliki motivasi kembali dalam mengatasi diri *users* dari serangan dengan menggunakan *safeguarding measure* atau penyelesain dari behavior. TTAT penyelesaian *behaviors* yang dilakukan dan direspon positif dalam dua proses kognitif yaitu *threat apprasial (primary)* dan *coping appraisal (secondary).*

Dalam pengukuran TTAT yang menganggap suatu serangan dapat menjadi ancaman dan dua penyeleaian proses *behavior (avoidance mitigation, avoidance behavior)* digunakan dalam ancaman yang akan datang. Penyelesaian behavior ini menggunakan TTAT dengan respon positif antara lingkup IT dan keadaan TI yang tidak diinginkan dan berbahaya. TTAT dapat digunakan oleh *users* IT agar menjadi lebih memahami konsekuensi negatif dari serangan *malicious* IT dengan pertimbangan kesesuaian *safeguard* untuk pengujian yang terbaik dan berhubungan dengan penyalahgunaan *IS Security (ISS)*. Pada pengembangan terhadap ISS, TTAT dapat digunakan sebagai *framework* yang relevan dalam memahami ancaman *avoidance behavior* berdasarkan pada ISA.

2.5.1 Hubungan Individu dengan Personality Threat

Berdasarkan pada penelitian yang dilakukan oleh (Arachchilage & Love, 2014) terdapat beberapa faktor *personality threat* meliputi faktor *perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard costs, self-efficacy, avoidance motivation, behavioural intention* dan *avoidance behaviour* berdasarkan pada model *technology thread avoidance theory (TTAT). Perceived severity* merupakan kepercayaan individu terhadap *severity* dari *phishing attacks* yang bersumber dari luar information security mereka. *Perceived susceptibility* merupakan kepercayaan individu akan menjadi *victim* akibat dari *phishing attacks.*

Partisipan's avoidance behavior dapat meningkatkan pertahanan terhadap *phishing attacks* berdasarkan pada nilai *post-test* setelah memainkan *game phishing.* Faktor *avoidance bahavior* melalui *motivation to protect* berpengaruh dalam pertahanan terhadap *phishing attacks*. *Avoidance motivation* berpengaruh terhadap ancaman *avoidance*

behaviour users's IT terhadap *behavioural intention* dalam *safeguard measure.* Faktor *behavioural intention* tersebut sangat berpengaruh pada teori *cognitive*. *Mobile game prototype* (pembuatan *game framework*) yang digunakan oleh partisipan berdampak signifikan pada *avoidance motivation*. *Self-efficacy* didefinisikan sebagai *individuals' confidence* dalam *safeguard measure.*

Pengukuran *safeguarding measure* terhadap *user's* tidak membutuhkan sumber IT seperti *anti – phishing tools*, jika dibandingkan dengan *behavior (anti phishing education).* Pengaruh *user's* tersebut terhadap *avoidance behavior* ditentukan oleh *avoidance motivation* yang berpengaruh pada *perceived threat. Perceived treat* dipengaruhi oleh *perceived severity* dan *susceptibility* serta dipengaruhi oleh kombinasi antara *perceived severity* dan *susceptibility. User's avoidance motivation* dipengaruhi oleh *safeguard effectiveness, safeguard costs* dan *self-efficacy. Self-efficacy* didevinisikan sebagai *individual's confidence* dalam *safeguard measure* dan merupakan determinan pada *avoidance motivation. User's IT threat avoidance behavior* ditentukan oleh *avoidance motivation* dan berdampak kembali pada *self-efficacy* yang dipengaruhi oleh *procedural knowledge* dan *conceptual knowledge.*

Partisipan merasakan *phishing attacks* dan percaya *phishing attacks* akan selalu datang, sehingga meningkatkan motivasi mereka terhadap *avoidance* dari *phishing attacks.* Partisipan menyadari resiko dari *phishing attacks* yang berdampak pada kualitas teknologi internet partisipan. *Users' failure* terhadap ancaman presepsi disebabkan oleh *users's* tidak dapat *avoidance* dari *phishing attacks.* Hubungan antara partisipan dengan *mobile game prototype* berdampak signifikan terhadap *perceived threat, perceived severity, susceptibility* dalam pembuatan *game framework* dan manajemen *knowledge meliputi creation, transfer,* dan *application of knowledge*. Efek dari *belief* terhadap *personal efficacy* dalam *knowledge* disebut dengan *knowledge sharing self-efficacy (KSSE).*

2.5.2 Hubungan Teknologi dengan Personality Threat

Technology Threat Avoidance Theory (TTAT) digunakan untuk menguji apakah *conceptual* atau *procedural knowledge* mempengaruhi *computer users' self-efficacy* terhadap *phishing attacks. Perceived threat* dipengaruhi oleh kombinasi dari *perceived severity* dan *susceptibility. Game prototype* meningkatkan personal *computer users' motivation* terhadap *phishing attaks* dan terdapat hubungan dengan faktor *personality threat* meliputi *computer user's* dan *mobile game,* sehingga berpengaruh terhadao *safeguard measure* dalam menghindari *IT Threat* dengan efektif.

Faktor *knowledge* dipengaruhi oleh *learning procedural* dan *conceptual knowledge* yang digabungkan dengan *technological activities*. *Procedural* dan *conceptual knowledge*

merupakan interaksi terbaik yang memiliki efek positif terhadap *self-efficacy* dalam meningkatkan *computer user's phishing* terhadap *avoidance behavior. Knowledge* dipengaruhi oleh *leaning procedural* dan *conceptual knowledge* yang dikombinasikan dengan *technological activities*. Hubungan *conceptual* dan *procedural* dapat digunakan secara terpisah dan dapat digabungkan (terdapat interkasi) dalam meningkatkan *computer users' phishing* terhadap *avoidance behavior*

TTAT mencangkup aspek *psychology, health care, risk analysis,* dan *information system (IS).* TTAT digunakan ketika users menerima *IT threat* dan *users* memiliki motivasi dengan efektif dalam *avoid of threat* dengan menggunakan *safeguarding measure,* jika *users* menerima ancaman dan mampu menghindari dengan menggunakan *safeguarding measure* dan *users* mungkin dengan efektif menghindari ancaman berdasarkan hasil dari penyelesaian *emotion-focused* (Liang & Xue, 2010). TTAT menjelaskan mengapa dan bagaimana *individual IT* (pengguna) terlibat dalam serangan *avoidance behavior* yang berfokus pada *framework* pada tingkatan *individual user* dan proses serta faktor berpengaruh terhadap *individual users' IT* terhadap *avoidance behavior.* TTAT berpengaruh terhadap *users IT* melawan *avoidance behavior* yang direprentasikan oleh proses *cybernetic,* dimana dapat mempengaruhi perbedaan keamanan antar *users' IT* pada kondisi awal dengan mempertimbangkan keamanan pada kondisi akhir *users' IT* tersebut.

Perceived threat merupakan faktor yang mendorong individu untuk merubah sikap mereka terhadap *phishing attacks. Safeguard effectiveness* merupakan pengujian individu terhadap *safeguard measure* mengenai tingkat efektivitas dalam penghindaran *phishing attacks. Safeguard costs* merupakan besarnya usaha yang dilakukan individu terhadap *phishing attacks* meliputi waktu, uang, keresahan, dan usaha lainnya yang digunakan dalam *safeguard measure. Self – efficacy* merupakan *individuals' confidence* terhadap *safeguard measure. Avoidance behavior* memotivasi individu untuk melindungi diri mereka dari *phishing attacks.* Berikut merupakan model faktor TTAT dari penjelasan diatas.

2.6 Statistical Product and Service Solutions (IBM SPSS Statistics)

Berdasarkan pada (George & Mallery, 2018) yang menerangkan sejarah mengenai SPSS. SPSS dibuat oleh tiga mahasiswa strata (satu) 1 pada akhir tahun 1960. Akronim dari SPSS yaitu *statistical package for the social science*. SPSS diperluas pada bidang *hard science* dan *business markets,* sehingga berganti nama menjadi *"Statistical Product and Service Solutions"* dan berganti nama kembali pada tahun 2009 yaitu IBM SPSS Statistik. Pada perkembangan SPSS terakhir yaitu dapat memperluas pada standar industri dan dapat

membantu pada banyak sektor. IBM SPSS Statistik merupakan perusahaan *software* statistik yang sangat terkenal, mudah digunakan, dan terbesar di dunia.

2.6.1 MANOVA (Multivariate Analysis of Variance)

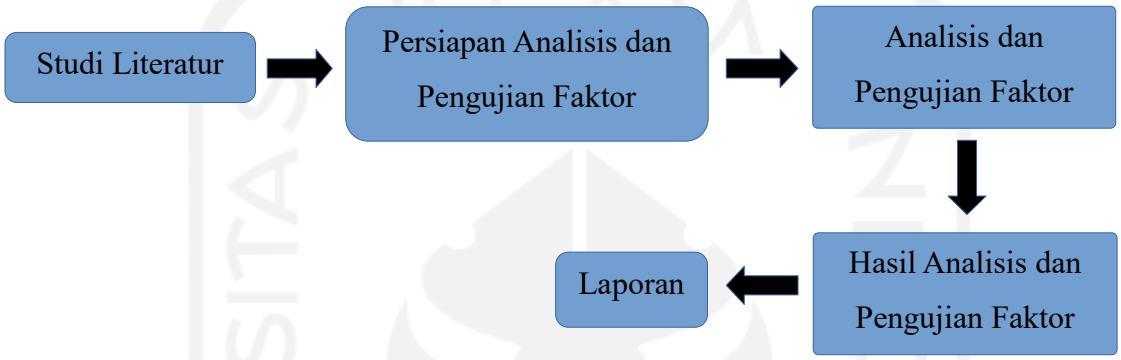
MANOVA *(Multivariate Analysis of Variance)* merupakan prosedur *general linear model* yang digunakan dalam SPSS statistik dan memiliki lebih banyak *comment* yang kompleks, sehingga dapat digunakan dalam melakukan komputasi analisis regresi *multivariate.* Variabel independen merupakan sample t-test yang terdapat perbedaan antara dua kelompok yang berbeda pada setiap variabel dependen. MANOVA terbagi menjadi 3 yaitu satu variabel independen dengan lebih dari dua level (*one-way* ANOVA), banyak variabel independen (*two- and three-way* ANOVA), ANOVA *covariates* (ANCOVA). Independen variabel dan *covariates* berpengaruh terhadap prosedur dari MANOVA dan MANCOVA, sehingga akan tidak lebih kompleks dalam memproses data.

2.6.1.1 Multivariate Test dan Pairwise Comparisons

Multivariate tests merupakan hasil dari prosedur dari model *general linear* berdasarkan pada *univariate F tests* pada setiap variabel dependen. Prosedur ini tidak berpengaruh positif terhadap MANOVA dalam pengujian variabel dependen secara simultan. *Pairwise comparisons* digunakan untuk semua kombinasi dari setiap level variabel independen yang digunakan, sehingga SPSS dapat menujukkan perbedaan antara dua pengertian yaitu *standard error* dari perbedaan (apakah ada perbedaan yang signifikan dan memiliki nilai 95% *confidence interval* dari setiap perbedaan tersebut).

BAB 3
Metodologi Peneltian

Bab ini menjelaskan bagaimana proses penelitian dilakukan. Tujuan dari tahapan ini adalah untuk mengetahui langkah-langkah yang dapat dijadikan sebagai pedoman yang jelas dalam menyelesaikan permasalahan. Adapun tahapan-tahapan pada penelitian ini dapat dilihat pada gambar 3.1.



Gambar 3.1 Alur Metodologi Penelitian

3.1 Studi Literatur

Studi Literatur merupakan langkah untuk mengkaji dan mempelajari berbagai sumber literatur dan teori-teori yang mendukung tentang penelitian yang dilakukan. Adapun sumber pembelajaran pada studi literatur dapat bersumber dari jurnal, paper, artikel, buku buku, website, dan sumber pembelajaran lainnya yang membahas mengenai *information security – personality threat.*

3.2 Persiapan Analisis dan Pengujian

Persiapan analisis dan pengujian merupakan langkah persiapan sebelum melakukan analisis dan pengujian faktor dalam penelitian ini. Persiapan analisis dan pengujian tersebut meliputi langkah pengumpulan data kuesioner dan langkah *prediktor online survey* dengan menggunakan model penelitian kualitatif berdasarkan pada literatur yang digunakan dalam penelitian ini. Berikut merupakan pembahasan dari langkah – langkah tersebut.

3.2.1 Pengumpulan Data Kuesioner

Pengumpulan data koesioner merupakan langkah selanjutnya dalam membuat daftar pertanyaan yang digunakan pada kuesioner penelitian berdasarkan pada literatur yang digunakan. Kuesioner tersebut dibuat dengan menggunakan *google form (online)* dan dibagikan melalui media sosial *(WhatsApp, Line, Facebook),* agar pengumpulan data

menjadi lebih relevan dengan yang sebenarnya (lapangan). Koesioner *online* tersebut menggunakan beberapa pertanyaan mengenai faktor yang terdapat dalam model *Technology Threat Avoidance Theory (TTAT)* dan mempengaruhi partisipan tersebut terhadap *phishing attacks.*

3.2.2 Predictors Online Survey

Pada bagian yang telah diterangkan sebelumnya mengenai langkah persiapan analisis dan pengujian faktor, dan pengumpulan data kuesioner. *Predictors online survey* merupakan langkah selanjutnya dalam penentuan partisipan yang tepat dalam penggunaan kuesioner online tersebut berdasarkan pada literatur yang digunakan.

3.3 Analisis dan Pengujian Faktor TTAT

Pada bagian yang telah diterangkan sebelumnya mengenai langkah persiapan analisis dan pengujian faktor, pengumpulan data kuesioner, dan *predictors online survey*. Analisis dan pengujian faktor merupakan langkah selanjutnya dengan model penelitian kuantitatif dan menggunakan metode MANOVA *(multivariate tests* dan *pairwise comparisons)* dalam analisis dan pengujian model indiaktor tersebut

3.3.1 Multivariate Tests

Multivariate Tests merupakan metode yang digunakan dalam analisis model faktor TTAT (variabel independen dan dependen) berdasarkan pada hasil pengumpulan data kuesioner *online* dengan menggunakan variabel independen dan dependen yang terdapat pada model faktor tersebut dan berdasarkan pada perbandingan *F test* dan *descriptive discriminant analysis (DDA)*. *F test* digunakan untuk uji siginifikansi (sig. <0.05) variabel dependen dan variabel independen yang terdapat pada faktor model TTAT secara bersamaan dalam penentuan diterima atau tidaknya hubungan faktor model tersebut pada *personality threat* terhadap *phishing attacks*

3.4 Hasil Analisis dan Pengujian Faktor TTAT

Pada bagian yang telah diterangkan sebelumnya mengenai langkah persiapan analisis dan pengujian faktor, analisis dan pengujian faktor, dan *predictors online survey.* Hasil analisis dan pengujian faktor TTAT merupakan langkah selanjutnya ketika hasil dari nilai perhitungan *F tests* dapat diterima (.sig <0.05). Hasil analisis dan pengujian faktor TTAT tersebut digunakan dalam menunjukkan keterikatan antar variabel dependen dan independen pada *personality threat* terhadap *phishing attacks.*

3.4.1 Tests of Between – Subjects Effects

Test of between – subjects effecs merupakan metode yang digunakan dalam menghitung nilai dari R^2 *(Adjusted R Squared)* berdasarkan pada variabel dependen dan independen pada *personality threat* terhadap phishing attacks. Nilai R^2 tersebut menunjukkan terdapat hubungan di luar variabel (faktor) dependen dan variabel (faktor) independen yang terdapat pada model faktor TTAT.

3.4.2 Pairwise Comparisons

Pairwise comparisons merupakan metode yang digunakan dalam mengukur tingkat keterkaitan antar variabel independen dan dependen yang berpengaruh terhadap *personality threat* partisipan berdasarkan pada model faktor TTAT. Hasil dari metode tersebut yaitu keterkaitan antar variabel dependen dan independen yang sangat berpengaruh pada *personality threat* terhadap *phishing attacks.*

3.5 Laporan

Laporan merupakan akhir dari metodologi penelitian yang meliputi kesimpulan dari masing – masing langkah yaitu persiapan analisis faktor, analisis dan pengujian faktor, dan hasil analisis dan pengujian.

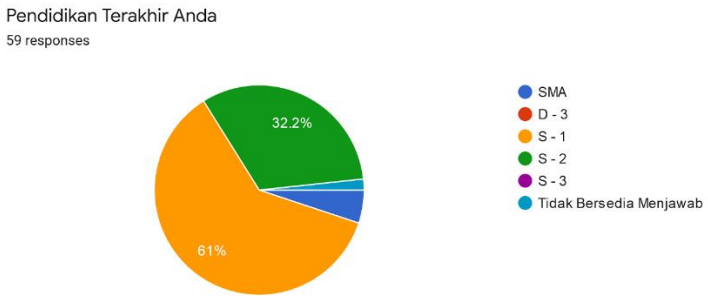
BAB 4
Hasil dan Pembahasan

4.1 Persiapan Analisis dan Pengujian Faktor

Pada bagian yang telah diterangkan sebelumnya di metodologi penelitian yaitu mengenai langkah – langkah yang dikerjakan dalam peneliltian ini meliputi studi literatur, persiapan analisis dan pengujian faktor, analisis dan pengujian faktor, hasil analisis dan pengujian faktor, dan laporan. Persiapan analisis dan pengujian merupakan langkah persiapan analisis dan pengujian model faktor *Technology Threat Avoidance Theory (TTAT)* pada *personality threat* partisipan terhadap *phishing attacks* meliputi *predictor online survey* dan *kuesioner online.*

4.1.1 Predictor Online Survey

Predictiors online survey digunakan dalam melakukan analisis dan pengujian faktor TTAT pada *personality threat* partisipan terhadap *phishing attacks* berdasarkan jawaban partisipan pada kuesioner *online.* Terdapat 59 partisipan yang merupakan pekerja diberbagai sektor dengan latar belakang teknologi informasi, dan pendidikan SMA, D3, S1, dan S2. Data yang didapatkan dari kuesioner online tersebut merupakan data yang sesuai dan tepat dalam analisis dan pengujian model faktor TTAT tersebut berdasarkan pada literatur yang digunakan. Berikut merupakan diagram dari jawaban 59 partisipan mengenai latar belakang pendidikan partisipan tersebut.



Gambar 4.1 Tingkat Pendidikan Partisipan

Pada diagram diatas menunjukkan bahwa partisipan memiliki latar belakang pendidikan S-1 dan S-2 yang merupakan presentase terbesar dalam pengisian kuesioner tersebut yaitu sebesar 61%, 32.2% dan diikuti oleh partisipan dengan latar pendidikan yang lainya yaitu SMA, D-3, S-3 dan partisipan yang tidak bersedia menjawab. Berikut merupakan pembahasan kuesioner online tersebut berdasarkan pada model faktor TTAT.

4.1.2 Kuesinoner Online

Kuesioner *online* digunakan dalam pengumpulan data *predictors online survey* berdasarkan pada daftar pertanyaan yang terdapat pada literatur (Arachchilage & Love, 2014) yaitu mengenai faktor *personality treat* pada model TTAT terhadap *phishing attacks* yang meliputi faktor *perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard costs, self-efficacy (security awareness), behavioral intention, avoidance motivation,* dan *avoidance behavior*. Berikut merupakan daftar pertanyaan yang digunakan dalam kuesioner tersebut berdasarkan pada faktor tersebut dengan kriteria pilihan jawaban "sangat setuju, setuju, netral, tidak setuju, sangat tidak setuju, tidak bersedia menjawab".

Aspek Self-Efficacy - Security Awareness	
1.	Saya seharusnya mendapatkan pengetahuan mengenai *email-phishing,* jika saya tidak pernah mengetahui *email-phishing* sebelumnya.
2.	Saya seharusnya mendapatkan pengetahuan mengenai *email-phishing,* jika saya mempunyai sumber yang berhubungan sesuai dengan hal itu.
3.	Saya seharusnya mendapatkan pengetahuan mengenai *email-phishing,* jika saya mempunyai banyak waktu.
4.	Saya seharusnya mendapatkan pengetahuan mengenai *email-phishing,* jika tidak ada yang mengajarkan kepada saya bagaimana belajar pertama kali.
5.	Saya merasakan bahwa tidak mendapatkan pengetahuan mengenai *email-phishing,* jika tidak ada satupun yang membantu saya untuk memulainya.
Aspek Avoidance Motivation	
1.	Saya berniat untuk mendapatkan pengetahuan mengenai *email-phishing* untuk menghindari *phishing attacks*
2.	Saya memprediksi bawah saya akan mendapatkan pengetahuan *email-phishing* untuk menghindari *phishing attacks*
3.	Saya merasakan bahwa saya tidak ingin mendapatkan pengetahuan *email-phishing* untuk menghindari *phishing attacks.*
Aspek Avoidance behavior	
1.	Saya mendapatkan pengetahuan *email-phishing* untuk menghindari *phishing attacks*
2.	Saya belajar terus menerus mengenai *email-phishing.*
3.	Terus menerus mempelajari pengetahuan *email-phishing* adalah sesuatu yang sangat tidak penting untuk dapat menghindari *phishing attacks*

Aspek Behavioral Intention	
1.	Saya akan melakukan *security procedures* dengan sesuai
2.	Saya akan menambahkan langkah-langkah keamanan tambahan untuk melindungi informasi saya dan sistem informasi saya.
3.	Saya akan membeli beberapa *software* untuk mengurangi dampak dari *information security breach* (pelanggaran pengamanan informasi)
4.	Saya akan belajar lebih lanjut mengenai bagaimana memperkuat pengamanan informasi saya.

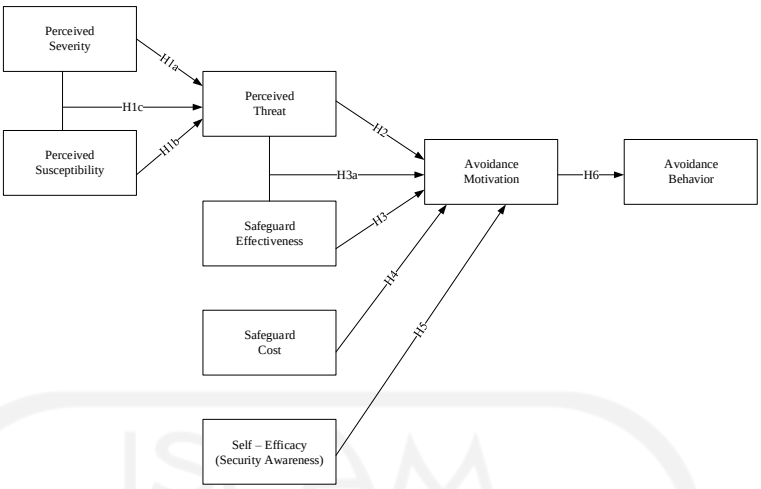
Tabel 4.2 Kuesioner Model Faktor TTAT

4.2 Analisis dan Pengujian Faktor

Pada bagian yang telah diterangkan sebelumnya mengenai persiapan analisis dan pengujian faktor model TTAT. Analisis dan pengujian faktor TTAT tersebut menggunakan aplikasi SPSS 25 dalam perhitungan berdasarkan hasil pengumpulan data kuesioner *online* sebelumnya. Metode MANOVA (*Multivariate Tests* dan *Pairweise Comparisons*) menggunakan variabel faktor yang terdapat pada model TTAT dan berpengaruh terhadap *phishing attacks.* Berikut merupakan pembahasan dari langkah analisis dan pengujian faktor TTAT tersebut meliputi variabel faktor model dan perhitungan *multivariate tests.*

4.2.1 Variabel Faktor Model

Variabel faktor model merupakan variabel faktor yang terdapat dalam model TTAT, dimana faktor tersebut merupakan faktor yang berpengaruh terhadap *personalty threat* partisipan. Variabel tersebut meliputi variabel independen yaitu *percerived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard costs, self-efficacy (security awareness),* dan *avoidance motivation* dan variabel dependen yaitu *perceived threat, avoidance motivation* dan *avoidance behavior.* Berikut merupakan bagan dari model faktor TTAT tersebut.



Gambar 5.2 Model Faktor Technology Treat Avoidance Theory (TTAT)

4.2.2 Perhitungan Multivariate Tests

Perhitungan *multivariate tests* digunakan dalam proses perhitungan berdasarkan pada data dari langkah pengumpulan data kuesioner dengan menggunakan *google form (online).* Pengumpulan data kuesioner tersebut berdasarkan pada faktor model TTAT yang meliputi variabel dependen dan variabel independen. Berikut merupakan hasil dari perhitungan *multivariate tests* dengan menggunakan aplikasi SPSS 25 berdasarkan pada variabel tersebut

F	Sig
2962	0.000

Tabel 4.3 Multivariate Tests

Berdasarkan pada perhitungan *multivariate tests* di atas, dimana nilai dari *koefisien signifikansi* (Sig. <0.05) terhadap faktor tersebut. Maka faktor model TTAT tersebut dapat diterima dan saling berkaitan antar satu dengan yang lainnya pada *personality threat* terhadap *phishing attacks*. Faktor model TTAT tersebut dapat digunakan dalam proses selanjutnya mengenai hasil analisis dan pengujian faktor.

4.3 Hasil Analisis dan Pengujian Faktor

Pada bagian yang telah diterangkan sebelumnya mengenai persiapan analisis dan pengujian faktor dan analisis dan pengujian faktor. Analisis dan pengujian faktor tersebut meliputi perhitungan *multivariate tests* yang telah diproses sebelumnya, di mana nilai dari siginifikansi (.sig <0.05) berdasarkan pada nilai *F tests*. Maka diperlukan perhitungan lebih lanjut yaitu mengenai *tests of between-subjects effects* dan *pairwise comparisons.* Hasil dari perhitungan tersebut yaitu keterikatan antar variabel independen dan dependen pada *personality threat* terhadap *phishing attacks.*

4.3.1 Tests of Between-Subjects Effects

Perhitungan *tests of between – subjects effects* diproses setelah perhitungan *multivariate tests* berdasarkan pada variabel dependen dan variabel independen yang terdapat pada model faktor TTAT. Perhitungan tersebut menunjukkan bahwa nilai dari R^2 *(Adjusted R Squared = 0.698),* menunjukkan bahwa terdapat hubungan model faktor TTAT yang saling berpengaruh pada *personality threat* partisipan/individu terhadap *phishing attacks.*

4.3.2 Pairwise Comparisons

Perhitungan *pairwise comparisons* diproses setelah perhitungan *multivariate tests* berdasarkan pada variabel dependen dan variabel independen model faktor TTAT. Berikut merupakan tabel keterkaitan tertinggi antar faktor tersebut meliputi nilai *mean difference* dan siginifikansi dari setiap keterkaitan faktor tersebut. Keterkaitan faktor tersebut meliputi faktor *self-efficacy (security awareness) – behavioral intention, self-efficacy (security awareness) – avoidance behaviour, avoidance behaviour – avoidance motivation.*

No	Variabel Dependen	Variabel Independen	Mean Difference	Signifikansi
1.	Self – Efficacy (Security Awareness)	Behavioral Intention	12.305.925	0.000
2.	Self – Efficacy (Security Awareness)	Avoidance Behaviour	6.729.933	0.380
3.	Avoidance Behaviour	Avoidance Motivation	7.335.667	0.405

Tabel.4.4 Keterikatan Indikator

Berdasarkan pada tabel 4.4 menunjukkan perhitungan *pairwise comparisons* bahwa terdapat keterkaitan yang sangat berpengaruh antar faktor (variabel) tersebut yaitu faktor *behavioral intention* (variabel independen) dengan faktor *self-efficacy (security awareness)* (variabel dependen) dengan nilai *mean difference* yaitu 12.305.925 (Sig.< 0,05) berdasarkan pada analisis model faktor TTAT tersebut. Namun demikian, terdapat pengaruh keterikatan antar faktor yang lainnya diluar dari model faktor TTAT tersebut (*avoidance behaviour, avoidance motivation, safeguard effectiveness, safeguard cost, perceived severity, dan perceived susceptibility*) berdasarkan pada hasil perhitungan *test of between – subject effects* (R^2).

4.3.3 Keterkaitan Antar Faktor TTAT

Berdasarkan pada perhitungan sebelumnya mengenai perhitungan *pairwise comparisons* dan *test of between – subject effects* (R^2), di mana faktor *behavioral intention* merupakan faktor niat dari perilaku individu/partisipan yang mempengaruhi faktor *self-efficacy (security*

awareness) merupakan faktor kepercayaan diri terhadap *phshing attacks* berdasarkan pada faktor *avoidance behavior* dari setiap partisipan/individu tersebut. *Behavioral intention* dari setiap individu/partisipan dipengaruhi oleh *safeguard cost* meliputi waktu, uang, keresahan, dan usaha lainnya pada *safeguard measure* yang berpengaruh terhadap *avoidance motivation* dalam *self-efficacy (security awareness)* dari setiap individu/partisipan tersebut terhadap *phishing attacks.* Namun demikian, terdapat faktor lainnya yang berpengaruh terhadap *self-efficacy (security awarenss)* dari setiap individu/paeritisipan yaitu faktor *knowledge*.

Dengan demikian, partisipan/individu yang memiliki keterikatan yang tinggi terhadap faktor *behavioral intention – personality threat* sangat berpengaruh terhadap faktor *self-efficacy (security awareness) – personality threat* partisipan/individu tersebut terhadap *phishing attacks (cybercrime)* berdasarkan pada perhitungan MANOVA terhadap model faktor TTAT tersebut, dikarenakan faktor tersebut memiliki nilai *mean difference* dan signifikansi tertinggi. Namun demikian, terdapat nilai R^2 yaitu 0,698 yang menunjukkan nilai keterikatan antar faktor model TTAT tersebut dan terdapat nilai R^2 yaitu 0,598 yang menunjukkan nilai keterikatan faktor berpengaruh lainnya diluar faktor model TTAT tersebut. Sehingga keterikatan faktor *personality threat* tersebut dapat menurunkan tingkat korban dari setiap individu/partisipan terhadap *cybercrime* berdasarkan pada model penelitian kualitatif dan kuantitatif dengan menggunakan metode MANOVA tersebut.

Bab 5
Kesimpulan Dan Saran.

Berdasarkan pada penjelasan sebelumnya mengenai latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan hasil pembahasan. Maka dapat disimpulkan yang meliputi kesimpulan dan saran dari penelitian ini yaitu:

Kesimpulan:

- Penerapan metode penelitian kualitatif dan kuantitatif yaitu berupa data yang tepat dan dapat digunakan dalam analisis faktor *personality threat* berdasarkan pada data kuesioner *online* dengan menggunakan metode MANOVA.
- Keterikatan faktor *behavioral intention - personality threat* dengan *self-efficacy (security awareness) – personality threat* dan faktor yang lainnya yang berpengaruh diluar faktor *Technology Avoidance Threat Theory (TTAT)* dapat menurunkan tingkat korban dari setiap individu/partisipan tersebut terhadap *cybercrime*. Keterikatan faktor tersebut berdasarkan pada analisis data model penelitian kualitatif dan kuantitatif tersebut dengan menggunakan model faktor TTAT dan metode MANOVA.

Saran:

- Perlu dilakukan penelitian lebih lanjut dari penelitian ini, dimana belum dilakukan *real – phishing* kepada masing – masing partisipan/individu yang berkerja di berbagai sektor organisasi/institusi. Maka diperlukan penelitian analisis lebih lanjut dengan *real – phishing* kepada masing – masing partisipan/individu tersebut, sehingga terdapat perbedaan hasil perhitungan MANOVA dengan menggunakan model faktor TTAT dari sebelum dan sesudah dilakukan *real – phishing* terhadap setiap partisipan/individu tersebut.

Daftar Pustaka

Abraham, S., & Chengalur-Smith, I. S. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers and Security*, *87*, 101586. https://doi.org/10.1016/j.cose.2019.101586

Adam, M. E., & Yousif, O. (2011). Awareness of Social Engineering Among IIUM Students. *World of Computer Science and Information Technology Journal*, *1*(9), 409–413. http://wcsit.org/pub/2011/vol.1.no.9/Awareness of Social Engineering Among IIUM Students.pdf

Alseadoon, I. (2014). The impact of users' characteristics on their ability to detect phishing emails. *Doctoral Thesis*.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706–714. https://doi.org/10.1016/j.chb.2012.12.018

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185–197. https://doi.org/10.1016/j.chb.2016.02.065

Bezuidenhout, M., Mouton, F., & Venter, H. S. (2010). Social engineering attack detection model: SEADM. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010, February 2014*. https://doi.org/10.1109/ISSA.2010.5588500

Braman, S. (1989). Defining information. An approach for policymakers. *Telecommunications Policy*, *13*(3), 233–242. https://doi.org/10.1016/0308-5961(89)90006-2

Broadhurst, R., & Chantler, N. (2012). Social Engineering and Crime Prevention in Cyberspace. *SSRN Electronic Journal*, *October*. https://doi.org/10.2139/ssrn.2138714

Caldas, M. P. (2003). Management information systems: managing the digital firm. In

Revista de Administração Contemporânea (Vol. 7, Issue 1). https://doi.org/10.1590/s1415-65552003000100014

Charles P. Pfleeg, Shari Lawrence Pfleeger, J. M. (2015). *Security in Computing F I F T H E D I T I O N* (FIFTH EDIT). http://ptgmedia.pearsoncmg.com/images/9780134085043/samplepages/9780134085043.pdf

Chenoweth, J. D. (2005). Book Review: The Art of Deception: Controlling the Human Element of Security. *Journal of Information Privacy and Security*, *1*(2), 69–70. https://doi.org/10.1080/15536548.2005.10855769

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information security awareness in educational institution: An analysis of students' individual factors. *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, *1*, 352–359. https://doi.org/10.1109/Trustcom.2015.394

Filippidis, A. P., Hilas, C. S., Filippidis, G., & Politis, A. (2018). Information security awareness of Greek higher education students - Preliminary findings. *2018 7th International Conference on Modern Circuits and Systems Technologies, MOCAST 2018*, 1–4. https://doi.org/10.1109/MOCAST.2018.8376578

George, D., & Mallery, P. (2018). IBM SPSS Statistics 25 Step by Step. In *IBM SPSS Statistics 25 Step by Step*. https://doi.org/10.4324/9781351033909

Halevi, T., Lewis, J., & Memon, N. (2013). *Phishing, Personality Traits and Facebook*. http://arxiv.org/abs/1301.7643

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Hodges, D., & Buckley, O. (2017). Its not all about the money: Self-efficacy and motivation in defensive and offensive cyber security professionals. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 10292 LNCS*. https://doi.org/10.1007/978-3-319-58460-7_34

Jimada-Ojuolape, B., & Teh, J. (2020). Impact of the Integration of Information and Communication Technology on Power System Reliability: A Review. *IEEE Access*, *8*, 24600–24615. https://doi.org/10.1109/ACCESS.2020.2970598

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management and Computer Security*, *22*(1), 115–126. https://doi.org/10.1108/IMCS-01-2013-0005

Liang, H., & Xue, Y. (2009). Journal of the Association for Information Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective * Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Loss, I., & Reactance, P. (1993). *Control, Its Loss, and Psychological Reactance*. 3–30.

Mcguiness, T., & Mcguiness, T. (2019). *Information Security Reading Room Defense In Depth _____ tu , A ho ll r igh ts*.

Milgram, S. (1965). Some Conditions of Obedience and Disobedience to Authority. *Human Relations*, *18*(1), 57–76. https://doi.org/10.1177/001872676501800105

Mohebzada Jamshaid G, Zarka Ahmed El, Bhojani H.Arsalan, D. A. (2012). Phising in a University Community. *2012 International Conference on Innovations in Information Technology (IIT)*, 249–254.

Mouton, F., Malan, M. M., & Venter, H. S. (2013). Social engineering from a normative ethics perspective. *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference*. https://doi.org/10.1109/ISSA.2013.6641064

Mouton, Francois, Leenen, L., Malan, M., Venter, H., Mouton, F., Leenen, L., Malan, M., Towards, H. V., Defining, M., Domain, E., Kimppa, K., Whitehouse, D., Kuusela, T., & Phahlam-, J. (2014). Towards an Ontological Model Defining the Social Engineering Domain To cite this version : HAL Id : hal-01383064 Towards an Ontological Model Defining the Social Engineering Domain. *11th IFIP International Conference on Human Choice and Computers (HCC)*.

Positive Technologies. (2020). *Cybersecurity threatscape*.

Rao, R. S., & Ali, S. T. (2015). A computer vision technique to detect phishing attacks. *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, 596–601. https://doi.org/10.1109/CSNT.2015.68

Rege, A., Williams, K., & Mendlein, A. (2019). A social engineering course project for undergraduate students across multiple disciplines. *2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019*, 1–8. https://doi.org/10.1109/CyberSecPODS.2019.8885085

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Scheeres, J. W. (2008). *Establishing the Human Firewall: Reducing an Individual'S Vulnerability To Social Engineering Attacks*. 49.

Siponen, Mikko, Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64–71. https://doi.org/10.1109/MC.2010.35

Siponen, Mikkot. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society*, *31*(2), 24–29. https://doi.org/10.1145/503345.503348

Skitka, L. J., & Mckeever, W. (n.d.). *The social net: The social psychology of the Internet.* 1–36.

Sun, J. C. Y., Yu, S. J., Lin, S. S. J., & Tseng, S. S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, *59*, 249–257. https://doi.org/10.1016/j.chb.2016.02.004

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*(July), 286–296. https://doi.org/10.1016/j.chb.2019.07.034

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*, 269, 289.

Workman, M. (2009). Information Management & Computer Security A test of interventions for security threats from social engineering. *Computer Security Iss Information Management Computer Security International Journal of Accounting &amp Information Management*, *16*(4), 463–483. http://dx.doi.org/10.1108/09685220810920549%5Cnhttp://dx.doi.org/10.1108/09685220810920549%5Cnhttp://dx.doi.org/10.1108/09685220810920549

Zain, Z. M. (2018). *Modelling Semantics of Security Risk Assessment for Bring*. *July*.