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

Kun Saidi[1], Yudi Prayudi[2]

[1]Universitas Islam Indonesia, [2]Universitas Islam Indonesia
[1]16917211@students.uii.ac.id, [2]prayudi@uii.ac.id

(Naskah masuk: 19 Desember 2020, diterima untuk diterbitkan: 20 Februari 2021)

Abstrak:

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 metode *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 metode 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.*

Abstract

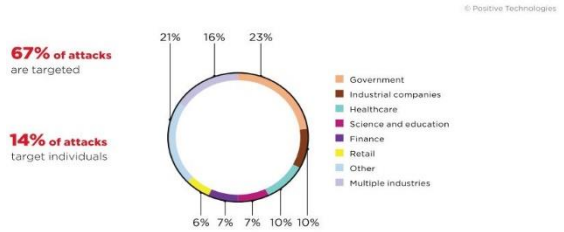
Social engineering (SE) is an activity that involves human beings, human psychology, and technology, thus causing losses to the victim where computer science and social psychology are used to determine the dangers of SE to society, and can threaten various organizational / institutional sectors, one 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) method. This factor analysis aims to determine the factors that have a strong influence on these 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 very influential factors, namely the behavioral intention factor with the self-efficacy - security awareness factor based on the factors contained in the model with a value 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.*

1. PENDAHULUAN

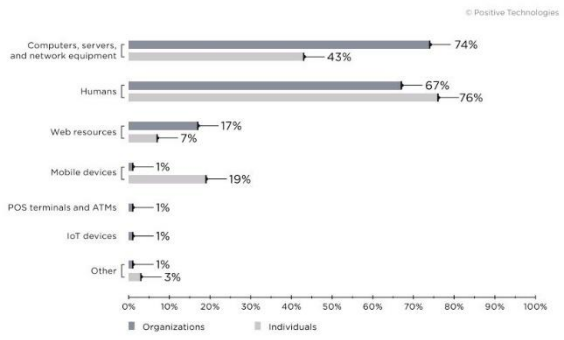
Seiring dengan berkembangnya teknologi yang semakin pesat, menyebabkan aktivitas masyarakat dengan menggunakan teknologi tersebut semakin tidak terkendali. Dampak positif dari penggunaan teknologi tersebut yaitu sangat beragam seperti pada kegiatan akademik, sosial, kesehatan, dan lain sebagainya. Peningkatan *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, 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 SE terhadap partisipan (Mouton, 2013). Berdasarkan pada (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 attacks.* Berikut merupakan info grafis mengenai beberapa institusi yang mengalami *SE attacks* dan terdapat pada Gambar 1.1



Gambar 1.1 Kategori Tingkat Attacks Terhadap Institusi 2020

Berdasarkan pada (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 *attacks* terhadap institusi tersebut yang tertuang pada Gambar 1.2



Gambar 1.2 Kategori Attacks Target 2020

Pada penelitian sebelumnya yang dilakukan oleh (Rege, 2019) mengenai edukasi dan keterbatasan kurikulum pendidikan khususnya strata-1 (sarjana) terhadap SE dengan objek siswa dan

p-ISSN : 2502-5724; e-ISSN : 2541-5735

pengajar. Tujuan penelitian ini adalah meningkatkan kemampuan dalam pembuatan aplikasi *cyber security* yang baru dengan menggabungkan faktor dari *human,* aspek sosial, spikologi dan teknik interaksi sosial. Hasil penelitian ini adalah dapat memberikan solusi terhadap dampak dari *cyber criminal* dengan mempertimbangkan waktu yang dibutuhkan dalam pembuatan projek SE kurikulum pendidikan *cyber security* tersebut.

Dalam penelitian yang dilakukan oleh (Arachchilage, 2014) mengenai pengujian *conceptual knowledge* atau *procedural knowledge* memiliki dampak positif pada *computer user's self-efficacy* terhadap *phishing attacks* dan melakukan evaluasi teori metode yang berdasarkan pada (Liang, 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 metode *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, 2013)

Penelitian yang lainnya mengenai pembuatan laporan desain dan pembuatan *game mobile prototype* sebagai perangkat *(tools)* edukasi serta membantu melindungi pengguna komputer terhadap *phishing attack* bedasarkan pada *pre-test* dan *post-test* yang terdapat pada *framework* tersebut. Tujuan dari desain *framework game mobile* yaitu meningkatkan *avoidance behaviour* pengguna melalui *motivation to protect* pengguna dari *phishing attack.* 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 behaviour,* sedangkan *safeguard* memiliki efek negatif (Arachchilage, 2016).

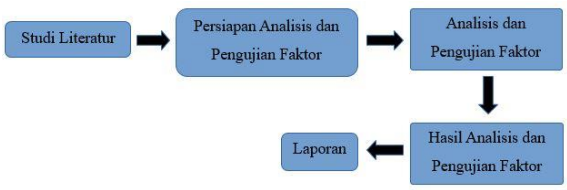
Dalam penelitian yang lainnya mengenai ancaman *mobile phishing* terhadap pengguna *smartphone (anti phishing self-efficacy)* berpengaruh terhadap *mobile phishing avoidance behavior)*. Tujuan dari penelitian yaitu membuat sebuah model mengenai *anti-phishing self-efficacy, anticipated regret* dan *gender* terhadap pengguna *smartphone (phishing avoidance behavior).* Pada penelitian ini, terdapat 231 responden yang digunakan dan menunjukkan adanya pengaruh positif terhadap *anti-phishing self-efficacy* dan *anticipated regret* pada *mobile phishing avoidance motivation* dan *behavior.* Sebagai tambahan, *gender* dengan

signifikan mempengaruhi *anti-phishing self-efficacy* terhadap *avoidance behavior* dan *motivation* (wanita lebih tinggi dibandingkan pria). Hasil penelitian menunjukkan bahwa terdapat interaksi antara *anti-phishing self-efficacy* dengan *anticipated regret* dan *gender* terhadap *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 metode *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.

2. METODOLOGI PENELITIAN

Pada bagian metologi penelitian 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 2.1.



Gambar 2.1 Alur Metodologi Penelitian

2.1. 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.*

2.2 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.

2.2.1 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 metode *Technology Threat*

Avoidance Theory (TTAT) dan mempengaruhi partisipan tersebut terhadap *phishing attacks.*

2.2.2 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.

2.3 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.

2.3.1 Multivariate Test

Multivariate Tests merupakan metode yang digunakan dalam analisis faktor motode TTAT (variabel independen dan dependen) berdasarkan pada hasil pengumpulan data kuesioner *online* dengan menggunakan variabel independen dan dependen yang terdapat pada 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 metode TTAT secara bersamaan dalam penentuan diterima atau tidaknya hubungan faktor metode tersebut pada *personality threat* terhadap *phishing attacks.*

2.4 Hasil Analisis dan Pengujian Faktor Metode 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 metode TTAT merupakan langkah selanjutnya ketika hasil dari nilai perhitungan *F tests* dapat diterima *(.sig <0.05).* Hasil analisis dan pengujian faktor metode TTAT tersebut digunakan dalam menunjukkan keterikatan antar variabel dependen dan independen pada *personality threat* terhadap *phishing attacks.*

2.4.1 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 faktor metode TTAT.

2.4.2 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 faktor metode TTAT. Hasil dari metode tersebut yaitu keterkaitan antar variabel dependen dan independen yang sangat berpengaruh pada *personality threat* terhadap *phishing attacks.*

2.5 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.

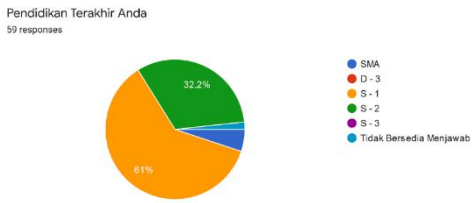
3. Hasil dan Pembahasan

3.1 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 faktor metode *Technology Threat Avoidance Theory (TTAT)* pada *personality threat* partisipan terhadap *phishing attacks* meliputi *predictor online survey* dan *kuesioner online.*

3.1.1 Predictor Online Survey

Predictiors online survey digunakan dalam melakukan analisis dan pengujian faktor metode 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 metode TTAT tersebut berdasarkan pada literatur yang digunakan. Berikut merupakan diagram dari jawaban 59 partisipan mengenai latar belakang pendidikan partisipan tersebut yang terdapat pada gambar 3.1.



Gambar 3.1 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 faktor metode TTAT.

3.1.2 Kuesioner Online

Kuesioner *online* digunakan dalam pengumpulan data *predictors online survey* berdasarkan pada daftar pertanyaan yang terdapat pada literatur (Arachchilage, 2014) yaitu mengenai faktor *personality treat* pada metode 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 metode tersebut dengan kriteria pilihan jawaban “sangat setuju, setuju, netral, tidak setuju, sangat tidak setuju, tidak bersedia menjawab” yang diterdapat pada tabel 3.1.

p-ISSN : 2502-5724; e-ISSN : 2541-5735

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.

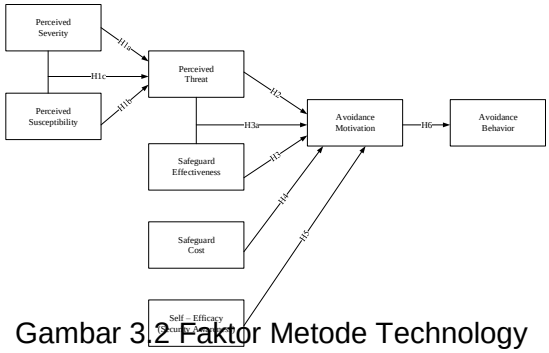
Tabel 3.1 Kuesioner Faktor Metode TTAT

3.2 Analisis dan Pengujian Faktor

Pada bagian yang telah diterangkan sebelumnya mengenai persiapan analisis dan pengujian faktor metode TTAT. Analisis dan pengujian faktor metode 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 TTAT dan berpengaruh terhadap *phishing attacks.* Berikut merupakan pembahasan dari langkah analisis dan pengujian faktor metode TTAT tersebut meliputi variabel faktor dan perhitungan *multivariate tests.*

3.2.1 Variabel Faktor Metode TTAT

Variabel faktor TTAT merupakan variabel faktor yang terdapat dalam metode 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 faktor metode TTAT tersebut yang terdapat pada gambar 3.2



Gambar 3.2 Faktor Metode Technology Threat Avoidance Theory (TTAT)

3.2.2 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 metode 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 3.2 Multivariate Test

Berdasarkan pada perhitungan multivariate tests di atas, dimana nilai dari koefisien signifikansi (Sig. <0.05) terhadap faktor tersebut. Maka faktor metode TTAT tersebut dapat diterima dan saling berkaitan antar satu dengan yang lainnya dalam *personality threat* terhadap *phishing*

attacks. Faktor metode TTAT tersebut dapat digunakan dalam proses selanjutnya mengenai hasil analisis dan pengujian faktor.

3.3 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.*

3.3.1 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 faktor metode TTAT. Perhitungan tersebut menunjukkan bahwa nilai dari R^2 *(Adjusted R Squared = 0.698),* menunjukkan bahwa terdapat hubungan faktor metode TTAT yang saling berpengaruh pada *personality threat* partisipan/individu terhadap *phishing attacks.*

3.3.2 Pairwise Comparisons

Perhitungan *pairwise comparisons* diproses setelah perhitungan *multivariate tests* berdasarkan pada variabel dependen dan variabel independen faktor metode 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* yang terdapat pada tabel 3.3.

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 3.3 Keterkaitan Faktor Metode TTAT

Berdasarkan pada tabel 3.3 di atas 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 faktor metode TTAT tersebut. Namun demikian, terdapat pengaruh keterikatan antar faktor yang lainnya diluar dari faktor metode 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).

3.3.3 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 *phishing attacks* berdasarkan pada faktor *avoidance behavior* dari setiap partisipan/individu tersebut. *Behavioral intention* dari setiap individu/partisipan

p-ISSN : 2502-5724; e-ISSN : 2541-5735

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/partisipan 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 faktor metode 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 metode TTAT tersebut dan terdapat nilai R^2 yaitu 0,598 yang menunjukkan nilai keterikatan faktor berpengaruh lainnya diluar faktor metode 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.

4. Kesimpulan dan Saran

Berdasarkan pada penjelasan sebelumnya mengenai latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan hasil pembahasan, terdapat beberapa kesimpulan dan saran dari penelitian ini yaitu:

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

DAFTAR PUSTAKA

Abraham, S. C.-S. I. S., 2019. Evaluating the effectiveness of learner controlled information security training. *Computers and Security.*

Arachchilage, N. A. G. L. S., 2013. A game design framework for avoiding phishing attacks. *Computers in Human Behavior.*

Arachchilage, N. A. G. L. S., 2014. Security awareness of computer users: A

phishing threat avoidance perspective. *Elsevier.*

Arachchilage, N. A. G. L. S. B. K., 2016. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior.*

Jimada-Ojuolape, B., 2020. Impact of the Integration of Information and Communication Technology on Power System Reliability: A Review. *IEEE Access.*

Liang, H. X. Y., 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems.*

Mouton, F. M. M. M. V. H. S., 2013. Social engineering from a normative ethics perspective. *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference.*

Rege, A. W. K. M. 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.*

Technologies, P., 2018. *Cybersecurity threatscape 2018 Trends and forecasts.* s.l.:s.n.

Technologies, P., 2020. *Cybersecurity threatscape.* s.l.:s.n.

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.*