Analisis Tingkat Security Awareness-Personal Threat Terhadap Ancaman Phishing Dengan Metode Technology Threat Avoidance Theory (TTAT)

Indah Daila Sari*[1], Dedy Hariyadi[2], Rama Sahtyawan[3] Netania Indi Kusumaningtyas[4]
[1,2,3]Teknologi Informasi, FTTI Unjaya, Yogyakarta, Indonesia
[4]Sistem Informasi, FTTI Unjaya, Yogyakarta, Indonesia
e-mail: ***[1]indahdaila285@gmail.com**, **[2]milisdad@gmail.com**, **[3]ramasahtyawan@gmail.com**,
[4]netania0412@gmail.com

Abstract - Phishing is a sort of cybercrime that involves obtaining sensitive information through the use of email, SMS, or compromised websites. The effects of phishing are caused by factors in the Technology Threat Avoidance Theory. The single best way to stop phishing attacks is to increase awareness of the risk of them happening among users or end users (human firewall). To determine the next steps in raising user knowledge, it is necessary to measure cybersecurity awareness, particularly against phishing assaults. Identify a few significant cybersecurity awareness of FTTI University of Jenderal Achmad Yani students in Yogyakarta. The investigation in this case included a phishing test and also employed online observation using observers who were asked questions based on the Technology Threat Avoidance Theory (TTAT). Using the MANOVA analysis method, factors influencing cybersecurity awareness analysis is conducted. Based on the analysis and testing of phishing tests as well as online questionnaires from the sample population, it shows that the sample is at a poor level of awareness. While the analysis of cybersecurity influence factors using the MANOVA analysis method shows that the results of the sig.> 0.05 value so that h0 is rejected. Based on the results of the study, it was concluded that FTTI students were still vulnerable to phishing attacks. Factor analysis using the MANOVA method shows that the dependent factor affects the level of cybersecurity awareness of the respondents but there is no significant difference between the dependent factors

Keywords *– Social Engineering, Cybersecurity Awareness Level, Technology Threat Avoidance Theory (TTAT), MANOVA, Live-Phishing*

Abstrak - Phishing merupakan tindakan kejahatan digital untuk mendapatkan informasi penting dengan cara melakukan penipuan menggunakan email, sms, atau situs web palsu. Salah satu upaya untuk mencegah terjadinya serangan phishing adalah dengan meningkatkan kesadaran atas ancaman siber dari sisi end user atau pengguna (human firewall). Sehingga mengukur tingkat kesadaran keamanan siber khususnya terhadap serangan phishing perlu dilakukan. Tujuan penelitian ini untuk mengetahui seberapa tingkat kesadaran keamanan siber mahasiswa FTTI Universitas Jenderal Achmad Yani. Penelitian ini menggunakan metode penelitian berupa uji phishing test dan juga observasi menggunakan kuisioner online berdasarkan pada model faktor Technology Threat Avoidance Theory (TTAT). Berdasarkan analisis dan pengujian phishing test dan juga kuisioner online dari populasi sempel menunjukan bahwa sampel berada di level kesadaran buruk. Sedangkan analisis faktor pengaruh keamanan siber menggunakan metode analisis MANOVA menunjukan bahwa hasil nilai sig.>0.05 sehingga h0 ditolak. Berdasarkan pada hasil penelitian disimpulkan bahwa mahasiswa FTTI masih rentan terhadap serangan phishing. Analisis faktor menggunakan metode MANOVA menunjukan bahwa faktor terikat mempengaruhi tingkat kesadaran keamanan siber responden tapi tidak terdapat perbedaan yang signifikan diantara faktor terikat

Kata kunci *– Clustering, Data Mining, Instagram, K-Means, Sistem Rekomendasi*

I. PENDAHULUAN

Penggunaan teknologi informasi semakin meningkat dalam banyak hal. Peningkatan penggunaan ini akan membawa kebiasaan baru pengguna dalam mengumpulkan informasi. Keinginan untuk mendapatkan informasi dengan cepat mengarah pada fakta bahwa pengguna terkadang tidak menyadari kebenaran dan keakuratan informasi yang tersedia [1]. Hal ini membuat pengguna rentan terhadap serangan di dunia digital, termasuk *phishing* [2]. *Phishing* adalah upaya untuk mendapatkan informasi sensitif dari pengguna atau organisasi menggunakan SMS, email, atau pesan yang dikirim melalui situs web palsu, yang mengakibatkan kerugian finansial atau pencurian data sensitif [3]. Berdasarkan laporan perusahaan *cybersecurity*, Kaspersky tentang serangan *phishing* di Asia Tenggara, khususnya Indonesia, yang menempati urutan ketiga setelah Vietnam dan Malaysia. Pada 2019, jumlah korban *phishing* adalah 14,316%. Angka ini meningkat dari sekitar 10,719% pada tahun sebelumnya [4]. Penelitian menunjukkan bahwa penipuan dan pencurian data adalah motif di balik kejahatan *phishing* ini. Rangkuman laporan konten negatif di laman patrolsiber.id menunjukkan bahwa penipuan terjadi melalui perangkat digital di Indonesia dengan 4601 laporan, tingkat kejahatan tertinggi dibandingkan kejahatan lainnya [5].

Survei yang mengukur tingkat kesadaran mahasiswa program sarjana Teknik Komputer (Tekkom) di Universitas Amikom Yogyakarta menemukan bahwa

mahasiswa Tekkom cenderung memiliki kesadaran keamanan informasi yang lebih tinggi. Ini karena kita sudah tahu apa artinya menggunakan teknologi informasi, terutama potensi serangan siber [6]. Berdasarkan observasi ditunjukkan bahwa masih banyak kasus pelanggaran merugi di kalangan mahasiswa di Kampus l Universitas Jenderal Ahmad Yani Yogyakarta. Lima kasus serupa didaftarkan dari 2018 hingga 2022. Para korban adalah empat mahasiswa Fakultas Teknik dan Teknologi Informasi (FTTI) dan satu mahasiswa Fakultas Ekonomi dan Ilmu Sosial (FES). Pelaku menargetkan siswa dengan tujuan membajak akun media sosial dan menghasilkan kerugian dalam bentuk uang tunai dan pinjaman. Kerentanan terhadap serangan rekayasa sosial, termasuk penipuan dalam bentuk *phishing* [7], salah satu cara untuk mengatasinya adalah dengan meningkatkan kesadaran akan ancaman siber kepada pengguna akhir atau pengguna *(human firewall)* [8]. Inilah sebabnya mengapa diperlukan pengukuran tingkat kesadaran pengguna untuk mempertimbangkan langkah selanjutnya dalam membentuk *human firewall*. Kesadaran pengguna juga diukur oleh Mukhlis Amin menggunakan metode pengumpulan data dengan menyebarkan kuesioner dan analisis data menggunakan metode *Multiple Criteria Decision Analysis* (MCDA) [9]. Penelitian serupa menggunakan metode ANOVA (analisis varians) dilakukan oleh Nunu Vadila dan Ahmad R. Pratama dan menunjukkan bahwa faktor demografi seperti gender mempengaruhi kesadaran keamanan informasi. Hasil penelitian ini menunjukkan bahwa perempuan lebih rentan terhadap ancaman *phishing* [7]. Kun Saidi juga melakukan pengukuran kesadaran siber dalam sebuah penelitian untuk menentukan metrik kunci untuk keamanan informasi menggunakan model *Technology Threat Aversion Theory* (TTAT) [10]. Penelitian ini hanya menggunakan instrumen kuesioner yang disebarkan. Di sisi lain, dalam penelitian ini, kami melakukan analisis komparatif untuk mengukur tingkat kesadaran pengguna terhadap serangan phishing berdasarkan tingkat pendidikan, kami menggunakan model *phishing*. Hasil penelitian ini diharapkan dapat menjadi bahan pertimbangan dalam pengembangan metode pelatihan kesadaran keamanan alternatif untuk meningkatkan kesadaran akan kejahatan penipuan, khususnya *phishing*, di dunia digital.

II. METODE PENELITIAN

Dalam penelitian ini akan menganalisis tingkat *security awareness* terhadap ancaman *phishing* dari objek mahasiswa Fakultas Teknik dan Teknologi Informasi (FTTI). Penelitian dimulai dengan identifikasi masalah, memetakan proses, mengumpulkan data dan bahan penelitian, melakukan analisis, dan menyimpulkan seberapa tinggi tingkat kesadaran objek terhadap ancaman *phishing*. Untuk detailnya dapat dilihat pada Gambar 1.

Gambar 1. Alur Proses Penelitian

A. Bahan dan Alat Penelitian

Bahan penelitian ini terdiri dari 50 data mahasiswa FTTI Universitas Jenderal Achmad Yani Yogyakarta. Selain itu, peneliti juga memerlukan izin tertulis dari pihak kampus untuk penyebaran *phishing*. Alat yang digunakan dalam penelitian ini adalah komputer (PC) dan *smartphone* dengan spesifikasi yang cukup untuk menjalankan sistem operasi dan pengembangan perangkat lunak, konektivitas internet, dan kartu perdana. Sistem operasi dan program aplikasi yang digunakan untuk penelitian ini adalah:

1. Sistem Operasi: Windows 8 atau lebih tinggi atau Linux
2. Google Formulir
3. Google Spreadsheet
4. Aplikasi pesan instan: WhatsApp Business
5. Perangkat lunak IBM SPSS Statistics v.22

Digunakan Responden:

1. Aplikasi pesan instan: WhatsApp
2. Google Form

B. Jalan Penelitian

Penelitian ini melewati beberapa tahap, berikut tahapan dalam penelitian ini:

1. Tahap Identifikasi. Tahap ini terdiri dari mengidentifikasi dan menganalisis:
   a. Mengidentifikasi masalah yang muncul dan kebutuhan sumber daya.
   b. Identifikasi objek yang digunakan dalam penelitian.
2. Tahap persiapan pengumpulan data. Beberapa langkah dilakukan pada tahap ini adalah sebagai berikut:
   a. Mengajukan izin untuk menggunakan data mahasiswa kepada pihak akademik.
   b. Pengumpulan data objek penelitian.
3. Tahap desain. Pada tahap ini merupakan tahap bagaimana membuat phishing dan database pengumpulan data.
4. Tahap pengujian, mengenai bagaimana phishing didistribusikan ke objek yang telah ditentukan untuk kemudian dilakukan analisis data yang diperoleh.
5. Pada tahap analisis data, data yang terkumpul dianalisis menggunakan metode MANOVA.
6. Tahap pembuatan laporan merupakan tahap akhir dari penelitian ini. Selain menulis dokumen sebagai laporan penelitian, peneliti juga akan meminta maaf kepada objek penelitian sebagai klarifikasi adanya pesan *phishing* yang disebarkan.

Di bawah ini adalah rincian tahapan dari analisis tingkat kesadaran keamanan siber terhadap ancaman *phishing* yang ditujukan untuk mahasiswa FTTI.

1) Studi Literatur

Tahap ini merupakan langkah pertama dalam melakukan identifikasi untuk mengaji dan mempelajari teori-teori yang mendukung penelitian ini. Studi literatur pada penelitian ini dari beberapa artikel, *website*, jurnal, *paper*, dan sumber lainnya yang terkait dengan penelitian ini. Semua sumber yang digunakan pada penelitian ini akan dicantumkan pada bagian referensi.

2) Persiapan Pengujian

Pada tahap persiapan dilakukan pembentukan skenario pengujian *phishing* terhadap 50 mahasiswa. Selain itu, dibentuk juga susunan kuisioner yang akan disebarkan kepada objek mahasiswa untuk mengetahui apakah terdapat perbedaan yang signifikan dari masing-masing faktor pengaruh terhadap kesadaran keamanan siber objek. Untuk mengukur perbandingan seberapa besar pengaruh tiap faktor terhadap objek maka akan digunakan skala ranting. Dimana nantinya dari jawaban responden akan diubah menjadi *interval* angka dari 3 sampai dengan 1 menyesuaikan terhadap pilihan jawaban yang disediakan, dimana:

- Angka 3 bernilai berpengaruh positif
- Angka 2 bernilai berpengaruh positif
- Angka 1 bernilai berpengaruh negatif

3) Analisis dan pengujian

Pada tahapan ini dilakukan penyebaran *phishing* terhadap 50 mahasiswa FTTI Universitas Jenderal Achmad Yani dengan beberapa skenario yang disusun pada tahap sebelumnya. Pada tahapan ini dilakukan juga penyebaran kuisioner setelah dilakukan *phishing test* kepada mahasiswa FTTI secara acak untuk mengetahui seberapa tingkat kesadaran keamanan siber. Metode analisis responden menggunakan metode MANOVA untuk mengetahui perbandingan tiap faktor yang mempengaruhi. Hasil perhitungan MANOVA terhadap analisis model faktor TTAT berdasarkan data kuisioner digunakan untuk menarik kesimpulan apakah terdapat faktor yang sangat mempengaruhi tingkat kesadaran keamanan siber bagi mahasiswa FTTI. Dimana H_0 akan diterima jika uji signifikansi menunjukan sig. <0.05. Sebelum dilakukan uji ini akan dilakukan uji normalitas distribusi sebagai syarat melakukan uji MANOVA. Analisis MANOVA akan dilakukan menggunakan *software* analisis IBM SPSS Statistics v.22.

4) Laporan

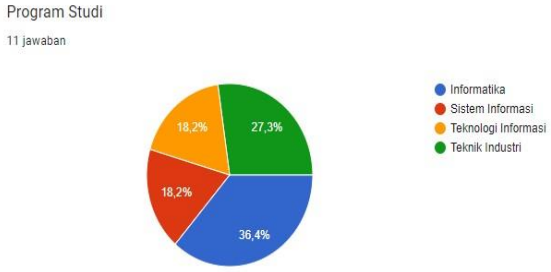
Laporan merupakan tahap terakhir dari metodologi pada penelitian ini. Pada tahap ini meliputi hasil akhir dari langkah-langkah sebelumnya yaitu identifikasi, persiapan analisis dan pengujian, tahap analisis dan penggujian, dan hasil dari analisis serta pengujiannya.

III. HASIL DAN PEMBAHASAN

A. Ringkasan Hasil Penelitian

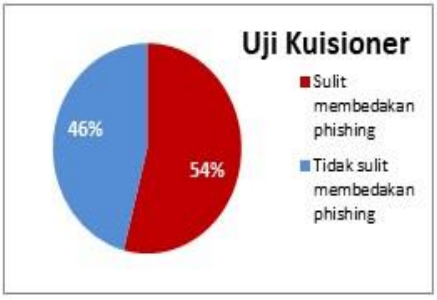
Pada bagian metodologi penelitian telah diterangkan mengenai tahapan yang dikerjakan dalam penelitian ini meliputi studi literatur, persiapan analisis dan pengujian, analisis dan pengujian, hasil analisis dan pengujian, dan laporan. Dari langkah pertama yaitu dilakukannya studi literatur diperoleh teori-teori pendukung pembentukan skenario pengujian *phishing test*, penyusunan pertanyaan pada kuisioner *online* berdasarkan pada model faktor *Technology Threat Avoidance Theory* (TTAT), dan tata cara uji analisis faktor menggunakan metode MANOVA. Pada langkah selanjutnya yaitu persiapan analisis dan pengujian disusun sebuah skenario pengujian *phishing test* yang akan dilakukan selama tiga hari (3x24 jam). Selain itu, disusun pula pertanyaan yang akan dibagikan pada kuisioner *online* berdasarkan pada model faktor *Technology Threat Avoidance Theory* (TTAT). *Phishing test* dan kuisioner berdasarkan pada model faktor *Technology Threat Avoidance Theory* (TTAT) ini akan dibagikan hanya kepada 50 mahasiswa FTTI Universitas Jenderal Achmad Yani Yogyakarta.

Pada analisis dan pengujian dilakukan sebuah *phishing test* dengan skenario dan durasi waktu yang telah ditetapkan pada langkah yang telah diterangkan sebelumnya. *Phishing test* ini menargetkan data pribadi mahasiswa untuk diambil. *Phishing test* dilakukan kepada 50 mahasiswa FTTI dengan program studi yang berbeda-beda dan sebanyak 11 mahasiswa diantaranya terjaring kedalam *phishing test* ini untuk lebih jelas dapat dilihat pada Gambar 2.



Gambar 2. Korban *Phishing Test*

Pada hasil tersebut dapat dilihat bahwa korban didominasi dari program studi Informatika sebesar 36,4% dari total korban. Selain itu, setelah ditinjau kembali terdapat 4 korban yang bukan berasal dari populasi sampel yang ikut menjadi korban *phishing test* ini. Sedangkan terdapat 50 total responden kuisioner yang dibagikan secara acak kepada keseluruhan mahasiswa FTTI termasuk dengan sampel *phishing test* sebelumnya. Kuisioner disebarkan setelah *phishing test* ditutup dan dari data responden dapat dilihat pada Gambar 3 menunjukan bahwa 54% dari responden sulit membedakan *phishing* dan pesan yang asli.



Gambar 3. Respon Kuisioner Mahasiswa

Dari data kuisioner tersebut dilakukan pula analisis MANOVA dan diketahui bahwa hasil uji diketahui bahwa tidak terdapat perbedaan yang signifikan dari masing-masing model faktor TTAT yang berpengaruh terhadap tingkat kesadaran keamanan siber mahasiswa (sig.>0.05).

B. Persiapan Analisis dan Pengujian

Dalam tahap persiapan terdapat beberapa langkah meliputi penentuan penyusunan skenario, dan kuisioner *online* berdasarkan pada model faktor *Technology Threat Avoidance Theory* (TTAT) yang mempengaruhi tingkat kesadaran keamanan siber terhadap serangan *phishing*.

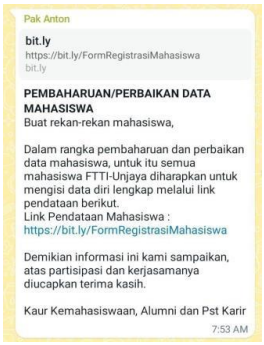
1) Skenario *Phishing Test*

Dalam penyebaran *phishing* disusun sebuah skenario sebagai batasan untuk peneliti dalam melakukan *phishing test*. Skenario meliputi tata cara penyebaran, *platform* penyebaran, waktu dan durasi penyebaran, serta format pengiriman permohonan maaf kepada objek penelitian. Tabel 1 merupakan skenario penyebaran *phishing attack* pada penelitian ini.

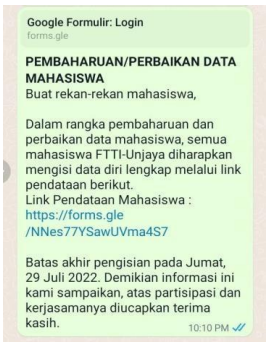
Tabel 1. Skenario Penyebaran *Phishing Test*

Indikator	Keterangan
Waktu penyebaran pesan *phishing*	22.00 WIB
Durasi	3 hari (72 jam)
Platform Phishing	WhatsApp Business
No. WhatsApp	Merupakan no baru dan langsung dinonaktifkan setelah test selesai dilakukan
Format pesan *phishing*	Mengikuti kalimat pengumuman resmi dari pihak akademik
Waktu pengiriman permohonan maaf	29 Juli 2022

Sesuai pada tabel diatas, penyebaran pesan *phishing* dilakukan menggunakan *platform* WhatsApp Business mulai dari tanggal 26 Juli 2022 pukul 22.00 WIB dengan durasi waktu 72 jam atau 3 hari sampai dengan tanggal 28 Juli 2022. Waktu penyebaran pesan *phishing* sengaja dilakukan pada malam hari yang merupakan waktu luar operasional kampus. Format pesan *phishing* merupakan duplikasi dari format pesan *broadcast* resmi yang dibagikan oleh pihak akademik seperti yang ditunjukan pada Gambar 4 dan Gambar 5 berikut.



Gambar 4. Pesan Asli



Gambar 5. Pesan *Phishing*

Pesan *phishing* disebarkan sekali kepada 50 nomor WhatsApp sampel dengan harapan setiap objek menerima dan menyadari pesan tersebut. Dari 50 pesan terdapat dua pesan yang berstatus pengiriman *checklist* satu atau pesan tidak diterima. 48 pesan lainnya terkirim ke objek yang dituju. Setelah selesai dilakukan *phishing test* selanjutnya peneliti melakukan penyebaran permohonan maaf sekaligus sebagai bentuk klarifikasi dan pembagian kuisioner kepada populasi sampel. Penyebaran dilakukan serentak pada tanggal 29 Juli 2022 dan dilanjutkan dengan pembagian kuisioner kepada mahasiswa FTTI Universitas Jenderal Achmad Yani Yogyakarta secara acak dan *form* kuisioner ditutup pada tanggal 6 Agustus 2022.

2) Kuisioner *Online*

Penyebaran Kuisioner *online* menggunakan *platform* Google Form. Kuesioner ini merupakan langkah dalam pengumpulan data berdasarkan daftar pertanyaan dari faktor *personality threat* pada model TTAT terhadap *phishing attacks* yang meliputi Aspek *Self-Efficacy - Security Awareness*, Aspek *Avoidance Motivation*, Aspek *Avoidance behavior*, Aspek *Behavioral Intention* [11]. Berikut ini merupakan daftar pertanyaan yang digunakan pada kuesioner dengan penyesuaian terhadap populasi sampel.

Tabel 2. Kuisioner Model Faktor TTAT

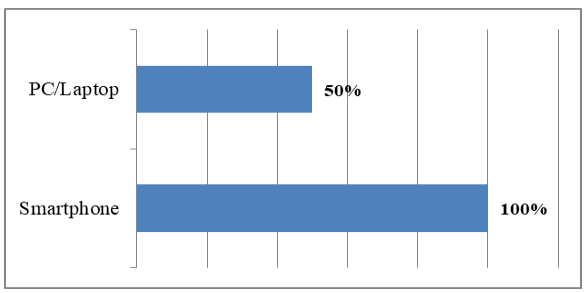
Aspek *Self-Efficacy - Security Awareness*	
1.	Apa sebelumnya Anda belum pernah mendapatkan pengarahan tentang keamanan informasi?
2.	Anda rasa seharusnya mendapatkan pengetahuan mengenai *phishing*, jika Anda belum pernah mengetahui *phishing* sebelumnya.
3.	Menurut Anda apakah penting bagi pihak Universitas untuk menetapkan peraturan dalam penyebaran informasi resmi Universitas?
4.	Anda rasa seharusnya mendapatkan pengetahuan mengenai *phishing*, jika mempunyai sumber yang berhubungan sesuai dengan hal itu.
Aspek *Avoidance Motivation*	
1.	Anda merasakan bahwa tidak akan mendapatkan pengetahuan mengenai *phishing*, jika tidak ada yang membantu saya untuk memulainya.
2.	Anda akan mencari pengetahuan mengenai *phishing*, jika mempunyai banyak waktu.

3.	Anda akan belajar lebih lanjut mengenai bagaimana memperkuat pengamanan informasi Anda.
4.	Anda memiliki niat untuk mendapatkan pengetahuan mengenai *phishing* untuk menghindari *phishing attacks.*
Aspek *Avoidance behavior*	
1.	Anda rasa jika mendapatkan pengetahuan tentang *phishing*, Anda akan dapat mengetahui cara mencegah *phishing attacks*
2.	Terus menerus mempelajari pengetahuan tentang *phishing* dan jenis serangan siber lain adalah sesuatu yang sangat penting untuk dapat menghindari *cyber attacks*.
3.	Apa yang Anda lakukan setelah mendapatkan pesan terkait keperluan Universitas tanpa adanya dokumen resmi pendukung?
Aspek *Behavioral Intention*	
1.	Anda akan melakukan *security procedures* dengan sesuai, jika diberitahu terlebih dulu
2.	Anda telah melakukan *security procedures* dengan sesuai sesuai pengetahuan yang Anda miliki sekarang?
3.	Anda telah memiliki langkah-langkah keamanan tambahan untuk melindungi informasi dan sistem informasi Anda
4.	Anda bersedia membeli beberapa software untuk mengurangi dampak dari *information security breach* (pelanggaran pengamanan informasi)

C. Analisis dan Pengujian

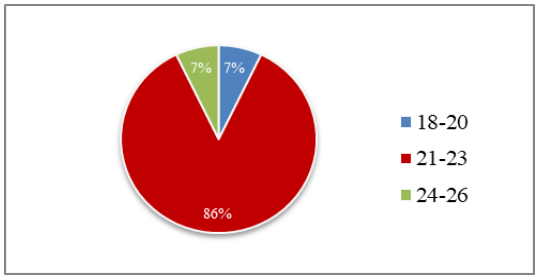
Pada bagian sebelumnya mengenai persiapan analisis dan pengujian telah didapatkan skenario dan kuisioner untuk dilakukan langkah selanjutnya yaitu pengujian. Pengujian terhadap tingkat kesadaran mahasiswa dilakukan secara daring *(online)* menggunakan *platform* WhatsApp Business dan Google Form untuk Kuisioner. Analisis data pengujian mahasiswa tersebut menggunakan aplikasi IBM SPSS Statistics v.22 dalam perhitungan berdasarkan hasil pengumpulan data kuesioner *online* sebelumnya. Metode MANOVA menggunakan variabel faktor yang terdapat pada model TTAT dan berpengaruh terhadap *phishing attacks* sebagai faktor terikat atau dependen dan pengakuan mahasiswa untuk membedakan pesan *phishing* menjadi faktor independen. Berikut merupakan pembahasan dari langkah analisis dan pengujian.

1) Analisis Demografis



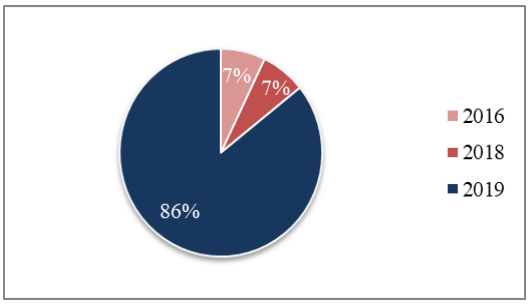
Gambar 6. Perangkat Elektronik Responden

Analisis demografis digunakan untuk menentukan kategori responden dalam melakukan analisis faktor pengaruh tingkat kesadaran keamanan siber objek. Berdasarkan pada kuisioner yang disebarkan keseluruhan responden telah memiliki email dan fasih menggunakan aplikasi WhatsApp. Keseluruhan responden memiliki *smartphone* dan 50% dari responden memiliki perangkat PC/laptop.



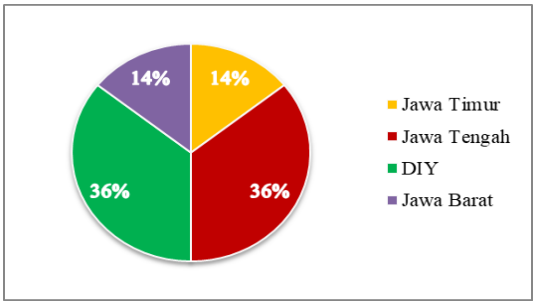
Gambar 7. Rentang Umur Responden

Dari Gambar 7 diatas responden memiliki rentang umur antara 18-26 tahun. Dimana mayoritas responden memiliki rentang umur 21-23 tahun yaitu sebanyak 86% responden. Responden terdiri dari perempuan dan laki-laki dengan responden perempuan lebih banyak laki-laki. Dari keseluruhan partisipasi 57,1% merupakan perempuan. Dari keseluruhan responden 86% responden merupakan mahasiswa tahun angkatan 2019 dan yang lainya dari angkatan 2016 dan 2018. Perbandingan tahun angkatan responden dapat dilihat pada Gambar 8 berikut.



Gambar 8. Tahun Angkatan Responden

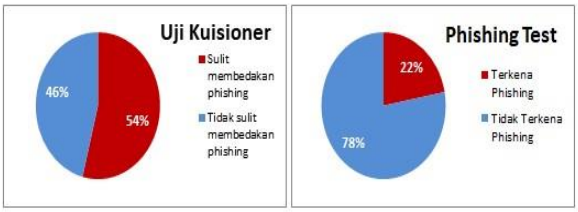
Penyebaran tempat tinggal responden masih berada di Pulau Jawa. Sebagian besar responden tinggal di Provinsi Jawa Tengah dan Daerah Istimewa Yogyakarta. 14% dari responden tinggal di Provinsi Jawa Timur, 14% lainnya tinggal di Provinsi Jawa Barat. Responden yang tinggal di Provinsi Jawa Tengah dan DIY masing-masing sebanyak 36%.



Gambar 9. Tempat Tinggal Responden

2) Tingkat Kesadaran Mahasiswa

Tingkat kesadaran mahasiswa dihitung dari dua hasil pengujian yaitu pengujian dengan *phishing test* dan kuisioner. *Phishing test* dan kuisioner disebarkan ke 50 mahasiswa FTTI secara acak dengan durasi penyebaran untuk *phishing test* selama 3 hari dan untuk kuisioner selama 9 hari. Untuk gambaran lebih jelas dapat dilihat pada Gambar 10.



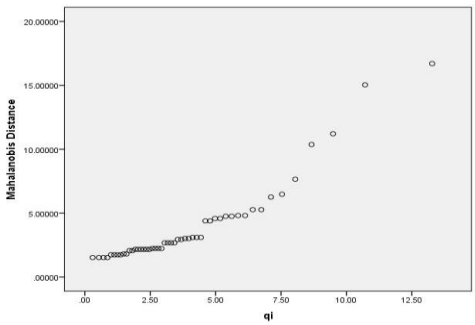
Gambar 10. Uji Kesadaran Terhadap Serangan *Phishing*

Pada hasil uji *phishing test* menunjukan 11 diantara 50 sampel objek menjadi korban *phishing test* ini. Hasil ini menunjukan angka yang cukup besar. Sedangkan, pada data responden kuisioner terdapat 54% dari total jawaban mengaku bahwa sulit untuk membedakan pesan *phishing* dengan yang asli hanya 46% diantara sampel yang tidak kesulitan membedakan pesan *phishing* dengan pesan asli. Hasil ini menunjukan bahwa tingkat kesadaran mahasiswa FTTI terhadap serangan *phishing* berada pada level buruk yaitu di tingkat 0-59% yang sadar terhadap serangan *phishing*.

3) Analisis Faktor

Analisis faktor pengaruh tingkat kesadaran keamanan siber dalam kasus ini merupakan serangan *phishing* berdasarkan pada model TTAT dilakukan dengan metode MANOVA. Analisis MANOVA disini digunakan untuk melakukan analisis secara keseluruhan dari faktor terikat (dependen) pada tingkat kesadaran mahasiswa terhadap serangan *phishing.* Analisis dilakukan untuk mengetahui apakah ada perbedaan yang signifikan dari masing-masing faktor terhadap tingkat kesadaran mahasiswa pada serangan *phishing.* Apabila dari analisis ini ditunjukan perbedaan yang signifikan maka akan dilanjutkan kedalam uji ANOVA untuk mengetahui seberapa besar masing-masing faktor dalam mempengaruhi tingkat kesadaran terhadap serangan *phishing.*

Dalam uji analisis MANOVA salah satu syarat adalah data terdistribusi secara normal *multivariat.* Sehingga perlu dilakukan uji normalitas *multivariat* terhadap data penyebaran kuisioner. Berikut merupakan uji normalitas terhadap data yang ada.



Gambar 11. Grafik Uji Normalitas Data

Pada Grafik menunjukan penyebaran antar variabel cenderung menunjukan garis lurus sehingga dapat ditarik asumsi bahwa data terdistribusi normal multivariat. Untuk memperkuat asumsi ini dilakukan uji korelasi antar variabel dan menunjukan hasil kolerasi sebesar 0.943 sehingga dapat dikatakan bahwa data terdistribusi secara normal multivariat dan dapat dilanjutkan ke uji analisis MANOVA.

Analisis MANOVA faktor model TTAT berdasarkan pada data 50 responden kuisioner. Uji multivariate dilakukan menggunakan *software* IBM SPSS Statistics v.22. Hasil perhitungan uji ini menunjukan bahwa rata-rata setiap faktor tidak menunjukan perbandingan yang signifikan terhadap kesadaraan mahasiswa terhadap serangan *phishing*. Dapat dilihat pada Tabel 3 untuk melihat rata-rata tiap faktor.

Tabel 3. *Descriptive Statistics*

	Apa sulit bagi Anda membedakan antara *Phishing* dengan pesan asli?	Mean	Std. Deviation	N
Aspek Self-Efficacy - Security Awareness	Sulit Mendeteksi *Phishing*	7.26	.689	23
	Tidak Sulit Mendeteksi *Phishing*	7.52	.643	27
	Total	7.40	.670	50
Aspek Avoidance Motivation	Sulit Mendeteksi *Phishing*	7.39	.839	23
	Tidak Sulit Mendeteksi *Phishing*	7.37	.688	27
	Total	7.38	.753	50
Aspek Avoidance behavior	Sulit Mendeteksi *Phishing*	6.00	.798	23
	Tidak Sulit Mendeteksi *Phishing*	6.33	.480	27
	Total	6.18	.661	50
Aspek Behavioral Intention	Sulit Mendeteksi *Phishing*	7.17	1.029	23
	Tidak Sulit Mendeteksi *Phishing*	7.22	.801	27
	Total	7.20	.904	50

Pada tabel diatas rata-rata setiap faktor menunjukan perbedaan yang kecil ini memberikan asumsi bahwa masing-masing faktor tidak memiliki perbedaan yang signifikan terhadap kesadaran pada serangan *phishing*. Untuk memperkuat asumsi ini dapat dilihat pada Tabel 4 berikut ini yang menunjukan hasil uji multivariat dengan hasil nilai sig.>0.05 yaitu sebesar 0.442. Dari hasil ini disimpulkan bahwa H_a diterima yaitu semua faktor saling mempengaruhi tingkat kesadaran terhadap serangan *phishing*. Namun, tidak ada perbedaan yang signifikan dari masing-masing faktor dalam mempengaruhi tingkat kesadaran terhadap serangan *phishing*. Dari hasil ini pengujian faktor tidak dapat dilanjutkan ke pengujian ANOVA untuk mengetahui seberapa besar masing-masing faktor mempengaruhi tingkat kesadaran terhadap serangan *phishing*.

Tabel 4. Uji *Multivariat Statistics*

Effect		Value	F	Hypothesis df	Error df	Sig.
Intercept	Pillai's Trace	.996	2940.171[b]	4.000	45.000	.000
	Wilks' Lambda	.004	2940.171[b]	4.000	45.000	.000
	Hotelling's Trace	261.348	2940.171[b]	4.000	45.000	.000
	Roy's Largest Root	261.348	2940.171[b]	4.000	45.000	.000
Apa sulit bagi Anda membedakan antara *Phishing* dengan pesan asli	Pillai's Trace	.078	.954[b]	4.000	45.000	.442
	Wilks' Lambda	.922	.954[b]	4.000	45.000	.442
	Hotelling's Trace	.085	.954[b]	4.000	45.000	.442
	Roy's Largest Root	.085	.954[b]	4.000	45.000	.442

a. *Design: Intercept* + Apa sulit bagi Anda membedakan antara *Phishing* dengan pesan asli

b. *Exact statistic*

IV. KESIMPULAN

Berdasarkan pada analisis dan pengujian secara menyeluruh dapat disimpulkan bahwa dari level tingkat kesadaran keamanan siber terutama dalam menghadapi serangan *phishing* yang dihasilkan, mahasiswa FTTI Universitas Jenderal Achmad Yani masih rentan terkena serangan *phishing*. Faktor Model TTAT yaitu meliputi Aspek *Self-Efficacy - Security Awareness*, Aspek *Avoidance Motivation*, Aspek *Avoidance behavior*, Aspek *Behavioral Intention* memiliki pengaruh terhadap tingkat kesadaran serangan *phishing*. Namun, diantara setiap faktor tidak memiliki perbedaan yang signifikan terhadap tingkat kesadaran keamanan siber.

DAFTAR PUSTAKA

[1] H. Wijayanto, A. H. Muhammad, and D. Hariyadi, "Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid," *Jurnal Ilmiah SINUS*, vol. 18, no. 1, pp. 1–10, 2020.

[2] T. Gunawan, "ANALISIS PERILAKU MAHASISWA TERHADAP REKAYASA SOSIAL DENGAN PENDEKATAN SKENARIO TERSTRUKTUR (Studi Kasus: Mahasiswa Departemen Sistem Informasi ITS) ANALYSIS OF STUDENT BEHAVIOR TOWARD SOCIAL ENGINEERING WITH STRUCTURED SCENARIO APPROACH (Case Study: Student Of ITS Information System Department)."

[3] S. Destya, "MODEL PENGUKURAN TINGKAT KESADARAN KEAMANAN INFORMASI DI UNIVERSITAS AMIKOM YOGYAKARTA," *SEMNASTEKNOMEDIA ONLINE*, vol. 6, no. 1, pp. 1–12, 2018.

[4] D. Irawan, "Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebook Dengan Metode Phising," *JIKI (Jurnal llmu Komputer & lnformatika)*, vol. 1, no. 1, 2020.

[5] "Laporan Kasus Kejahatan Siber." Accessed: Nov. 07, 2021. [Online]. Available: https://patrolisiber.id/

[6] S. Destya, "Pengukuran Tingkat Kesadaran Keamanan Informasi Berdasarkan Behavior Dan Offence Scale," *CESS (Journal of Computer Engineering, System and Science)*, vol. 5, no. 2, pp. 236–240, 2020.

[7] N. Vadila and A. R. Pratama, "Analisis Kesadaran Keamanan terhadap Ancaman Phishing," *AUTOMATA*, vol. 2, no. 2, 2021.

[8] M. Z. Huwaidi and S. Destya, "Mencegah Serangan Rekayasa Sosial dengan Human Firewall," *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, vol. 10, no. 1, pp. 107–112.

[9] M. Amin, "Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda) Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (Mcda)," *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika Vol*, vol. 5, no. 1, 2014.

[10] K. Saidi and Y. Prayudi, "Analisis Indikator Utama Dalam Information Security-Personality Threat Terhadap Phishing Attack," *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, vol. 6, no. 1, pp. 21–30, 2021.

[11] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Comput Human Behav*, vol. 38, pp. 304–312, 2014.