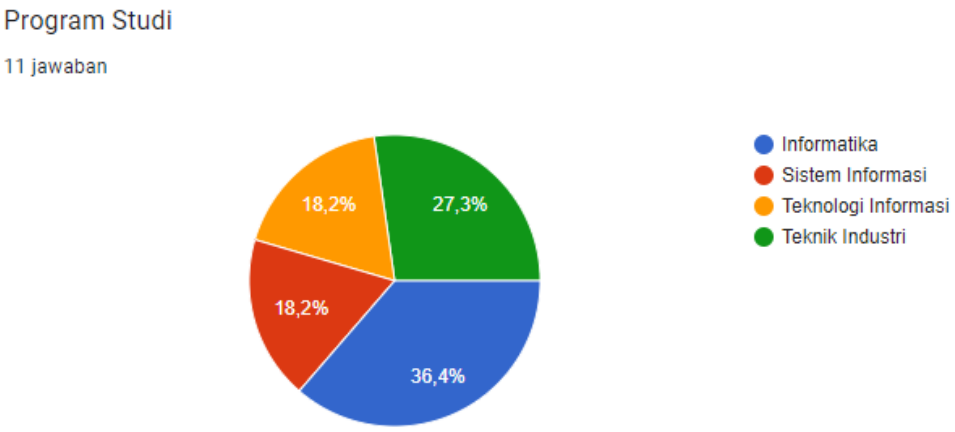
BAB 4
HASIL PENELITIAN

4.1 RINGKASAN HASIL PENELITIAN

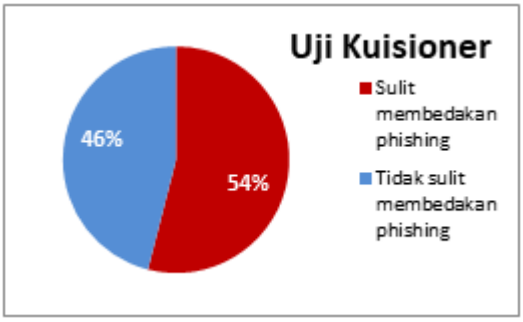
Pada bagian metodologi penelitian telah diterangkan mengenai tahapan yang dikerjakan dalam penelitian ini meliputi studi literatur, persiapan analisis dan pengujian, analisis dan pengujian, hasil analisis dan pengujian, dan laporan. Dari langkah pertama yaitu dilakukannya studi literatur diperoleh teori-teori 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 4.1.



Gambar 4.1 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 4.2 menunjukan bahwa 54% dari responden sulit membedakan *phishing* dan pesan yang asli.



Gambar 4.2 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).

4.2 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.*

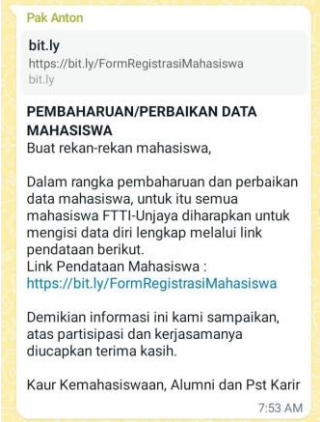
4.2.1 Skenario *Phishing Test*

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 4.1 merupakan skenario penyebaran *phishing attack* pada penelitian ini.

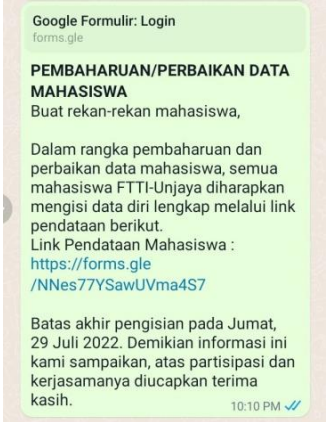
Tabel 4.1 Skenario Penyebaran *Phishing Test*

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 4.3 dan Gambar 4.4 berikut.



Gambar 4.3 Pesan Asli



Gambar 4.4 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 lainya 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.

4.2.2 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* (Arachchilage and Love, 2014). Berikut ini merupakan daftar pertanyaan yang digunakan pada kuesioner dengan penyesuaian terhadap populasi sampel.

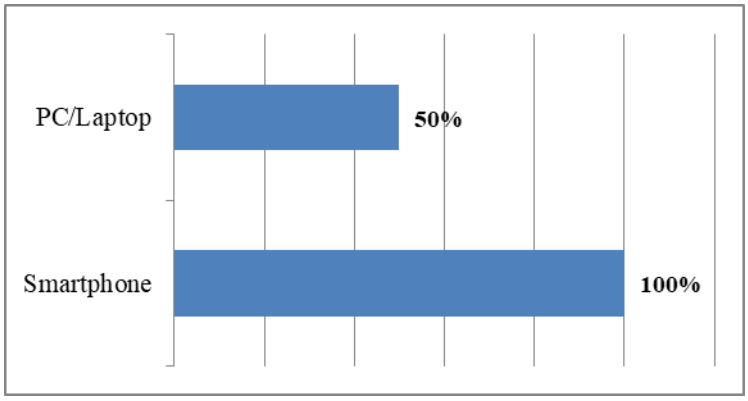
Tabel 4.2 Kuisioner Model Faktor TTAT

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)

4.3 ANALISIS DAN PENGUJIAN

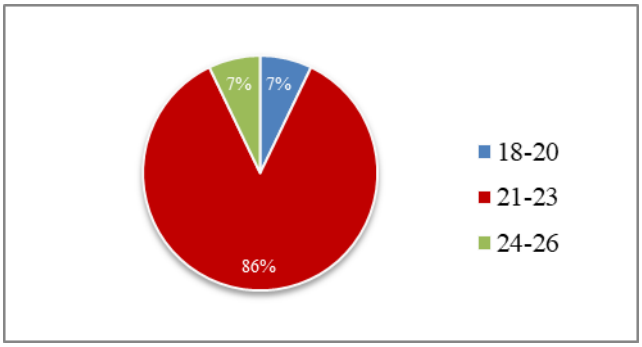
Pada bagian sebelumnya mengenai persiapan analisis dan pengujian telah didapatkan skenario dan kuisioner untuk dilakukan langkah selanjutnya yaitu pengujian. Pengujian terhadap tingkat kesadaran mahasiswa dilakukan secara daring *(online)* menggunakan *platform* WhatsApp Business dan Google Form untuk 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 mahasiwa untuk membedakan pesan *phishing* menjadi faktor independen. Berikut merupakan pembahasan dari langkah analisis dan pengujian.

4.3.1 Analisis Demografis



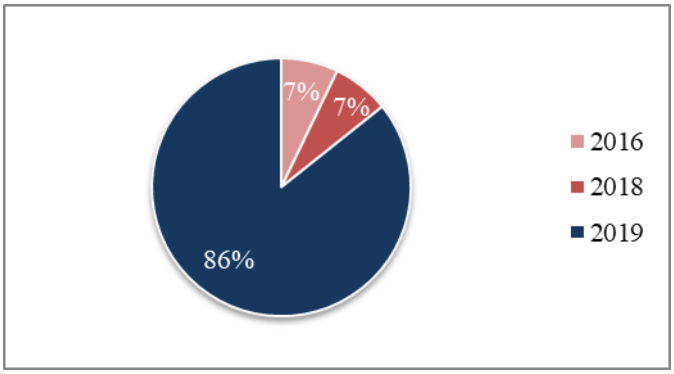
Gambar 4.5 Perangkat Elektronik Responden

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.



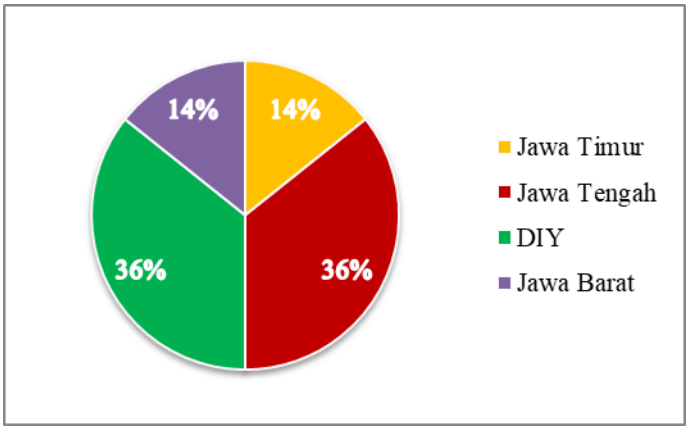
Gambar 4.6 Rentang Umur Responden

Dari Gambar 4.6 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 4.7 berikut.



Gambar 4.7 Tahun Angkatan Responden

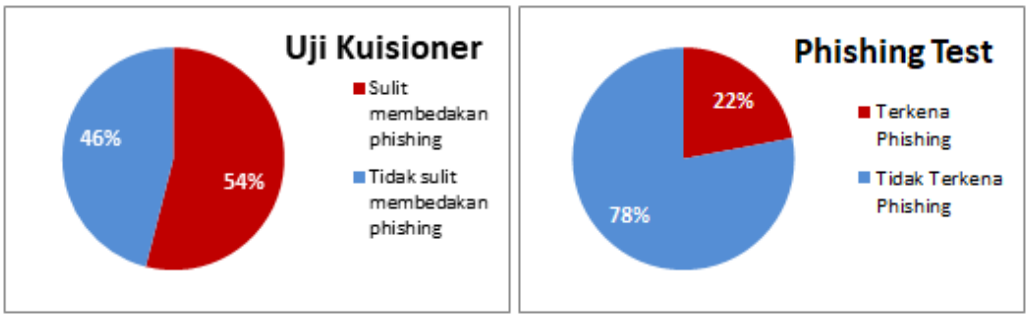
Penyebaran tempat tinggal responden masih berada di Pulau Jawa. Sebagian besar responden tinggal di Provinsi Jawa Tengah dan Daerah Istimewa Yogyakarta. 14% dari responden tinggal di Provinsi Jawa Timur, 14% lainnya tinggal di Provinsi Jawa Barat. Responden yang tinggal di Provinsi Jawa Tengah dan DIY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



Gambar 4.8 Tempat Tinggal Responden

4.3.2 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 4.9.



Gambar 4.9 Uji Kesadaran Terhadap Serangan *Phishing*

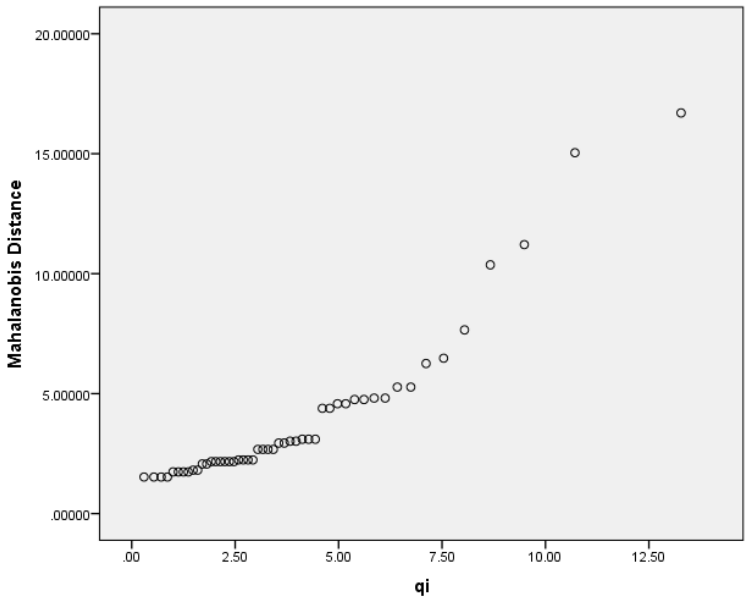
Pada hasil uji *phishing test* menunjukan 11 diantara 50 sampel objek menjadi korban *phishing test* ini. Hasil ini menunjukan angka yang cukup besar. Sedangkan, pada data responden kuisioner terdapat 54% dari total jawaban mengaku bahwa sulit untuk membedakan pesan *phishing* dengan yang asli hanya 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*.

4.3.3 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 4.10 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 4.3 untuk melihat rata-rata tiap faktor.

Tabel 4.3 *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 4.4 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 4.4 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*