Journal of Information System Research (JOSH)
Volume 4, No. 3, April 2023, pp 1026−1032
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i3.3081

Penerapan Metode Technology Threat Avoidance Theory Terhadap Tingkat Kesadaran Data Privasi Pengguna Media Sosial

Achmad Rifai[1,*], Ade Meliyani[2], Putri Chyntia[2], Ichtiar Akbar Sakti[2]

[1]Teknologi Informasi, Informatika, Universitas Nusa Mandiri, Jakarta
Jl. Raya Jatiwaringin No.2, RT.8/RW.13, Cipinang Melayu, Kec. Makasar, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia
[2]Teknologi Informasi, Sistem Informasi, Universitas Nusa Mandiri, Jakarta, Indonesia
Jl. Raya Jatiwaringin No.2, RT.8/RW.13, Cipinang Melayu, Kec. Makasar, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia
Email: [1,*]achmad.acf@gmail.com, [2]ademel11180327@nusamandiri.ac.id, [3]putric11180030@nusamandiri.ac.id, [4]ichtia11180511@nusamandiri.ac.id
Email Penulis Korespondensi: achmad.acf@nusamandiri.ac.id
Submitted: **02/02/2023;** Accepted: **30/04/2023;** Published: **30/04/2023**

Abstrak−Pencurian data kredensial dengan memasukan username dan password pada halaman login hingga akun yang terbuka. Proses autentikasi pada aplikasi dan web digunakan sebagai pengenal kepemilikan data pengguna, hal tersebut dikarenakan terdapat kerentanan terhadap serangan dalam penggunaan username dan password yang kurang aman. Ada beberapa masalah dalam hal keamanan, salah satunya yang paling umum adalah password. Kebanyakan sistem menggunakan password sebagai verifikasi identitas pengguna. Namun, password tersebut datang dengan masalah keamanan utama dikarenakan pengguna cenderung menggunakan yang mudah ditebak, memakai kata sandi yang sama di banyak akun, menulisnya dan menyimpannya di perangkat mereka. Peretas memiliki banyak sekali opsi yang digunakan untuk mencuri kata sandi atau meretas akun pengguna seperti credential stuffing, phising, password spraying, bruce force, prior data breach / reused passwords, password reset, keystroke logging dan local discovery. Untuk mengatasi penyerangan keamanan, teknik Multi-Factor Authentication (MFA) memberikan jaminan keamanan lebih tinggi. Kesadaran masyarakat untuk menjaga informasi identitas merupakan hal fundamental, pencurian identitas bisa melalui berbagai macam jalur dan cara dan hal ini perlu ditekankan. Self-efficacy (security awareness), behavioural intention, avoidance motivation dan avoidance behaviour adalah faktor terpengaruh dari objek. Analisis faktor tersebut bertujuan untuk mengetahui tingkat kesadaran dan pola perilaku pengguna media sosial. Analisis faktor menggunakan metode MANOVA sebagai analisis data dan model TTAT. Berdasarkan hasil analisis MANOVA tests of between – subjects effects, faktor advoidance motivation (r = 0.499 dan Sig. 0.000) dan behavioural intention (r = 0,427 dan Sig. 0.000). Adanya keterkaitan antar faktor tersebut, sehingga pengguna harus menghindari pencurian data melalui tindakan pengamanan dengan menggunakan multi-factor authentication (MFA).

Kata Kunci: Multi-Factor Authentication; Media Sosial; Self-Efficacy; MANOVA; TTAT

Abstract−Theft of credential data by entering a username and password on the login page until the account is open. The authentication process in applications and the web is used to identify ownership of user data, this is because there is a vulnerability to attacks in the use of unsafe usernames and passwords. There are several security issues, one of the most common being passwords. Most systems use passwords to verify user identity. However, these passwords come with major security issues as users tend to use ones that are easy to guess, use the same password across multiple accounts, write it down and store it on their devices. Hackers have many options using which to steal passwords or hack user accounts such as credential stuffing, phishing, password.spraying, bruce force, prior data breach / reused passwords, password reset, keystroke logging and local discovery. To overcome security attacks, Multi-Factor Authentication (MFA) techniques provide higher security guarantees. Public awareness to protect identity information is fundamental, identity theft can go through various channels and ways and this needs to be emphasized. Self-efficacy (security awareness), behavioral intention, avoidance motivation and avoidance behavior are factors that influence the object. This factor analysis aims to determine the level of awareness and behavior patterns of social media users. Factor analysis used the MANOVA method as data analysis and the TTAT model. Based on the results of the MANOVA tests of between – subjects effects, the factor of favorance motivation (r = 0.499 and Sig. 0.000) and behavioral intention (r = 0.427 and Sig. 0.000). There is a link between these factors, so users must avoid data theft through security measures using multi-factor authentication (MFA).

Keywords: Multi-Factor Authentication; SocialMedia; Self-Efficacy; MANOVA; TTAT.

1. PENDAHULUAN

Deformasi digital terus berkembang pada aspek kehidupan manusia untuk menumbuhkan inovasi baru dalam penggunaan teknologi agar tetap relevan dengan masyarakat. Dalam penggunaan aplikasi media sosial terdapat akun yang tentunya merupakan identitas yang digunakan sebagai pengenal dalam dunia maya, biasanya untuk dapat mengakses berbagai macam informasi dalam etika berinternet yang baik.

Asumsi yang diciptakan bahwa media sosial begitu penting dalam kehidupan saat ini, membuat penggunaan media sosial sangatlah tinggi. Rata–rata penggunaan nya dapat mencapai 6 sampai 7 jam dalam sehari. Indonesia adalah salah satu negara yang memiliki populasi pengguna internet terbesar di dunia. Dikutip dari We Are Social, terdapat 204,7 juta pengguna internet per Januari 2022 di Indonesia. Sedangkan pada Januari 2021 telah terdata sebanyak 202,6 juta pengguna internet, angka nya sedikit bertambah 1,03% jikalau dibandingkan dengan 2022. Pada 2018, jumlah pengguna internet melonjak sebesar 54,25%. Jumlah pengguna nya terus meningkat dalam lima tahun terakhir [1].

Journal of Information System Research (JOSH)
Volume 4, No. 3, April 2023, pp 1026−1032
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i3.3081

Pelanggaran sebuah data pribadi merupakan salah satu bagian dari ancaman dunia maya, yang di mana sebagian informasi dikeluarkan dari organisasi, umumnya digunakan dalam kejahatan penipuan identitas. Dapat diartikan bahwa tindakan pelanggaran data menjadi akses ilegal atas data pribadi milik seseorang yang dicatat oleh organisasi tersebut sehingga mendorong kejahatan pencurian identitas [2]. Kesadaran masyarakat untuk menjaga informasi identitas merupakan hal fundamental, pencurian identitas bisa dilakukan dengan berbagai macam cara serta jalur dan hal ini perlu ditekankan. Informasi yang telah didapat akan diperjual belikan ke pasar gelap secara online atau dimodifikasi yang nantinya akan diguunakan untuk membuat identitas sintetis. Laporan yang diterbitkan The University of Texas at Austin, 2017 mengatakan bahwa ada beberapa jalur penyaluran yang melibatkan orang luar serta orang dalam [3]

Proses autentikasi pada aplikasi dan web digunakan sebagai pengenal kepemilikan data pengguna, hal tersebut dikarenakan terdapat kerentanan terhadap serangan dalam penggunaan username dan password yang kurang aman. Ada beberapa masalah dalam hal keamanan, salah satunya yang paling umum adalah password. Peretas memiliki banyak sekali opsi yang digunakan untuk mencuri kata sandi atau meretas akun pengguna seperti credential stuffing, phising, password spraying, bruce force, prior data breach or reused passwords, password reset, keystroke logging dan local discovery [4]. Serangan pencurian data kredensial juga memasukan berbagai kombinasi username dan password yang ditemukan pada halaman login hingga akun yang terbuka. Serangan cyber di dunia maya sering menggunakan kembali username dan password yang sama. Informasi login pengguna yang dicuri pada suatu tempat, kemungkinan akan berfungsi pada tempat lain. Hasil analisis mengenai Social Media Security oleh menjabarkan hasil analisisnya dengan ditemukan 78,9% dari ancaman yang menggerakan jaringan media sosial [5].

TTAT juga dijabarkan Sebenarnya, tampaknya cukup masuk akal untukmenerapkan teori penerimaan dalam konteks keamanan TI karena penting untuk memahami adopsi individu dalam menjaga TI. Namun, bukti teoretis dan empiris yang kuat menunjukkan bahwa ada perbedaan mendasar antara keduanya adopsi dan perilaku menghindar [6]. Peretas terus mengidentifikasi cara baru dari mencuri informasi. Sayangnya, kehadiran pengguna "tidak berpendidikan" dalam suatu organisasi membuat mereka sasaran empuk bagi para hacker. Pendidikan pengguna dan pelatihan adalah suatu keharusan untuk memerangi ancaman keamanan TI. Pengguna seharusnya tidak hanya mempelajari materi tetapi mereka juga harus menerapkannya dalam kehidupan sehari-hari. Ini bukan tugas sederhana untuk dicapai dan bukan satu-satunya tanggung jawab pengguna atau organisasi. Banyak kelompok harus terlibat untuk menghasilkan penduduk yang sadar akan keamanan TI tidak dapat atau tidak akan mengelola perilaku penghindaran), dan tindakan terbuka (yaitu, penanggulangan penghindaran TTAT) untuk menghindari, mengurangi, atau meniadakan ancaman.[7].

Penelitian yang dilakukan Seperti yang diilustrasikan, motivasi penghindaran adalah prediktor signifikan dari perilaku penghindaran dalam setiap studi. Persepsi ancaman dan perlindungan efektivitas keduanya berpengaruh signifikan dan positif terhadap motivasi menghindar. Demikian juga, tingkat keparahan yang dirasakan memiliki pengaruh yang signifikan dan kuat terhadap ancaman yang dirasakan. Biaya perlindungan memiliki pengaruh yang signifikan tetapi negatif pada motivasi penghindaran di sebagian besar studi, yang menunjukkan bahwa ketika biaya perlindungan meningkat, pengguna kurang termotivasi untuk mengimplementasikan tindakan pengamanan. Namun, untuk penelitian ini biaya perlindungan tidak signifikan. Efikasi diri secara umum menunjukkan pengaruh yang signifikan terhadap motivasi penghindaran satu studi menemukan itu tidak signifikan. Modifikasi model TTAT untuk penelitian ini memberikan hasil yang menarik. Misalnya, memposisikan kerentanan yang dirasakan sebagai anteseden terhadap keparahan yang dirasakan dalam kalkulus ancaman menghasilkan pengaruh yang kuat dan signifikan [8]

Selain itu penelitian lain menyebutkan, model alternatif TTAT memberikan nilai penjelas yang lebih baik dari penilaian ancaman proses. Selain itu, model TTAT untuk memperhitungkan perbedaan individu yang memengaruhi ancaman persepsi, tingkat motivasi penghindaran, dan perilaku. Kami menguji model yang kami usulkan menggunakan sampel besar yang kami kumpulkan dari sekumpulan individu yang sangat heterogen, yang memperkuat generalisasi teori. Hasil mendukung generalisasi TTAT. Akhirnya, wawasan utama terakhir kami berkaitan dengan pengurangan persepsi individu tentang tingkat upaya yang di perlukan menerapkan pengamanan. Dalam upaya terkait dengan penerapan pengamanan keamanan dikaitkan secara negatif dengan penerapan pengamanan target. Temuan ini logis dan lugas. Individu tidak akan memiliki motivasi untuk berperilaku aman jika mereka menganggap perilaku target terlalu menantang atau berat. Temuan ini menunjukkan keamanan itu profesional harus memastikan bahwa semua perlindungan yang direkomendasikan mudah dan langsung bagi pengguna melaksanakan dan menggunakan. Kami percaya bahwa vendor teknologi keamanan cyber dan penulis kebijakan dapat menggunakan ini wawasan tentang safeguard effectiveness, self-efficacy, risk propensity, impulsivity, and effort cost to develop products, processes, and messages that more effectively encourage avoidance behavior [9].

Penelitian sebelumnya membahas tentang keamanan akun dari credential stuffing dengan password breach alerting oleh saat ekstensi Chrome meminta kredensial pada waktu login memperkirakan bahwa 1,5% dari kredensial yang 4 digunakan pada seluruh web rentan terhadap pencurian data kredensial berdasarkan hasil sampel 21 juta login [10]. Penelitian yang mengenai deteksi akun pengguna adalah berkoordinasi untuk mendeteksi serangan pencurian data yang aktif pada akun individual. Framework yang digunakan mengakomodasi

Journal of Information System Research (JOSH)
Volume 4, No. 3, April 2023, pp 1026−1032
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i3.3081

kecenderungan pengguna baru dari alternatif sebelumnya dan memastikan kompleksitas ekstraksi yang lebih tinggi untuk menangkap kemampuan dalam mengekstrak informasi yang cukup dari set offline [11].

Dalam observasi terdahulu dengan metode Technology Threat Avoidance Theory (TTAT) mengumpulkan evidensi sebanyak 152 responden pengguna komputer mengungkapkan adanya beberapa temuan utama seperti perceived threat, safeguard effectiveness, safeguard cost, self-efficacy influence avoidance motivation, perceived severity, dan perceived susceptibility. Ancaman yang dirasakan secara negatif memoderasi hubungan di antaranya safeguard effectiveness dan avoidance motivation [12].

Pada permasalahan tingkat kesadaran dan keamanan pada pengguna media sosial line. Pada faktor yang memengaruhi perilaku keamanan (security behavior) pada pengguna aplikasi tersebut adalah persepsi pengguna terhadap ancaman keamanan (perceived security threat). Dengan adanya sebuah ancaman keamanan ketika responden menggunakan dan menunjang aktivitas akan berpengaruh dengan perilaku keamanan dalam menjaga data privasi informasinya [13]. Penelitian sebelumnya mengenai analisis faktor personality threat terhadap phising attack menggunakan metode Technology Threat Avoidance Theory (TTAT) dalam hasil keterkaitan antar faktor yang sangat berpengaruh tersebut yaitu faktor behavioral intention dengan faktor self-efficacy – security awareness berdasarkan analisis data model penelitian kualitatif dan kuantitatif tersebut dengan menggunakan model faktor TTAT dan metode MANOVA [14].

Multivariate Analysis of Variance (MANOVA) hampir sama dengan one way Anova, memiliki lebih dari satu variabel dependen. Disimpulkan bahwa Multivariate Analysis of Variance (MANOVA) biasa digunakan pada dua kondisi utama, yaitu:

a. Terdapat beberapa korelasi variabel dependen, sedangkan hanya membutuhkan satu tes keseluruhan pada kumpulan variabel dibandingkan dengan tes individual.
b. Ingin mengetahui bagaimana variabel independent mempengaruhi pola variabel dependen.

Kelebihan dari Multivariate Analysis of Variance (MANOVA) adalah dapat digunakan untuk menganalisis pengaruh setiap variabel independen terhadap skala kategorik masing-masing variabel dependen secara individual, dimana variabel dependen memiliki skala kuantitatif [15].

Untuk mengatasi penyerangan keamanan tersebut, teknik seperti Multi-Factor Authentication (MFA) seharusnya dapat memberikan jaminan keamanan yang lebih tinggi. Multi-factor authentication (MFA) adalah salah satu cara untuk meningkatkan keamanan autentikasi dengan menggunakan dua atau lebih faktor yang berbeda saat masuk ke akun.

Berdasarkan identifikasi masalah terkait pokok - pokok permasalahan tersebut yang berpengaruh kepada objek (mahasiswa dan karyawan) pada terjadinya ancaman cyber, penulis menetapkan tujuan pada penelitian ini sebagai; Mengetahui tingkat kesadaran dan pola perilaku pengguna media sosial berdasarkan pada model TTAT dam mengetahui faktor (self-efficacy (security awareness), avoidance behavior, avoidance motivation, dan behavioral intention) yang mempengaruhi tingkat kesadaran berdasarkan pada model TTAT terhadap objek (Mahasiswa dan karyawan) pengguna media sosial.

2. METODOLOGI PENELITIAN

Data yang terkumpul dianalisis secara kuantitatif menggunakan statistik deskriptif, sehingga perumusan hipotesis dapat disimpulkan terbukti atau tidak. Penelitian kuantitatif menekankan pada pengujian teori melalui pengukuran variabel penelitian dengan angka dan melakukan analisis data dengan prosedur statistik, menggunakan pendekatan deduktif yang bertujuan untuk menguji hipotesis. Metode penelitiannya menggunakan pengukuran yang terstandar atau menggunakan skala pengukuran data, penelitian yang dilakukan untuk menjawab pertanyaan dengan menggunakan rancangan yang terstruktur, sesuai dengan sistimatika penelitian ilmiah [16].

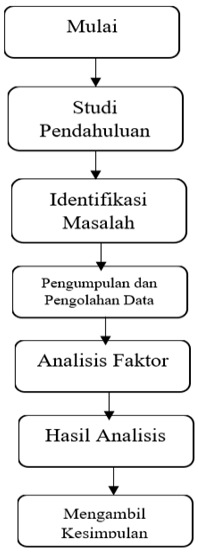
2.1 Tahapan Penelitian

Dalam melakukan penelitian ini langkah – langkah pelaksanaan dari awal sampai akhir, langkah – langkah ini didapat dari proses penelitian yang dilakukan oleh peneliti dari proses awal mulai sampai mendapatkan kesimpulan dari penelitian ini. Adapun langkah–langkahnya sebagai berikut:

a. literatur yang dilakukan untuk mengkaji dan secara teoritis menemukan metode yang digunakan dalam metode pemecahan masalah dengan menggunakan metode Technology Threat Avoidance Theory (TTAT). tersebut.
b. Tahap selanjutnya yaitu, Identifikasi masalah diperoleh dari hasil analisis penelitian lapangan dan data kuesioner. Hasil identifikasi masalah ini juga digunakan sebagai tujuan dari penelitian yang dilakukan.
c. Tahap ketiga, mengumpulkan data yang dibutuhkan untuk membantu mengidentifikasi masalah yang dirumuskan pada tahap kedua. Setelah data terkumpul, maka dilakukan pengolahan data yang digunakan pada tahap analisis.
d. Tahap selanjutnya ini berfokus pada tingkat keamanan rata-rata akun media sosial, menggunakan metode Technology Threat Avoidance Theory (TTAT) untuk menganalisis dan memberi peringkat pada hasil pembahasan masalah.
e. Dalam tahap terakhir penelitian ini, karakteristik responden yang dibutuhkan dapat dikaji dengan parameter seperti usia, jenis kelamin, platform media sosial yang sering digunakan dan status karyawan atau mahasiswa.

Journal of Information System Research (JOSH)
Volume 4, No. 3, April 2023, pp 1026−1032
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i3.3081

Untuk gambaran dari langkah-langkah tahapan ini dapat dilihat pada gambar 1.



Gambar 1. Tahapan Penelitian

2.2 Model yang Diusulkan

Dalam pengujian Multivariate Analysis Of Variance (MANOVA), untuk menganalisis indikator yang diperlukan untuk metode Technology Threat Avoidance Theory (TTAT) dengan menggunakan hasil perhitungan F test untuk uji signifikasi. Jika hasil signifikasi nya lebih kecil (sig <0,05), maka analisis dapat digunakan untuk menunjukkan keterikatan faktor antar variabel dependen dan independen, dan dapat dilakukan uji analisis faktor. Model analisis yang digunakan adalah Multivariate Analysis Of Variance (MANOVA). Model ini mengukur pengaruh variabel independen skala kuantitatif terhadap variabel dependen yang skala kategorik untuk menguji nilai variate dan signifikasi antar kelompok. Variabel Penelitian ini variabel dependen (Self-Efficacy) dan variabel independen (Avoidance motivation, avoidance behaviour, dan behavioural Intention).

2.3 Pengumpulan Data

Dari 81 kuesioner yang disebarkan, sebanyak 15 data kuesioner tidak dapat digunakan dikarenakan data berakibat tidak normal dan 1 data kuesioner yang memiliki jawaban ganda. Dengan demikian jumlah kuesioner yang dapat diolah sebanyak 65 data eksemplar kuesioner.

Tabel 1. Data Primer yang dihasilkan

Kuesioner	Jumlah	Presentase (%)
Kuesioner yang disebarkan	81	**100**
Kuesioner yang tidak digunakan	16	**19.7**
Kuesioner yang dapat digunakan	65	**80.3**

Berdasarkan 65 data responden yang diolah, diperoleh informasi mengenai struktur respoden sebagai acuan dalam melihat karakteristik respoden yang menjadi sampel penelitian. Struktur kuesioner dalam penelitian ini diantaranya: jenis kelamin, usia, status dan sosial media yang sering digunakan oleh responden. Secara rinci stuktur responden ini diringkas pada tabel 2.

Tabel 2. Struktur Responden

Keterangan	Jumlah (Orang)	Presentase (%)
Jenis Kelamin :		
Laki – Laki	**29**	**44.6**
Perempuan	**36**	**56.4**
Usia :		
17 – 20 tahun	**16**	**24.6**
21 – 25 tahun	**35**	**53.8**
26 – 30 tahun	**6**	**9.20**
31 – 35 tahun	**1**	**1.50**
>36 tahun	**7**	**10.7**
Status :		
Karyawan	**33**	**50.8**

Journal of Information System Research (JOSH)
Volume 4, No. 3, April 2023, pp 1026−1032
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i3.3081

Keterangan	Jumlah (Orang)	Presentase (%)
Mahasiswa	**32**	**49.2**
Media sosial yang sering digunakan:		
Instagram	**51**	**63**
Facebook	**29**	**35**
WhatsApp	**65**	**80.2**
Twitter	**22**	**27.2**
Lainnya	**12**	**15**

2.3 Analisis Data

Berdasarkan pada mahasiswa dan karyawan yang menjadi tujuan ingin dicapai dari penelitian, analisis data membantu mengidentifikasi faktor-faktor yang mempengaruhi tingkat kesadaran pengguna media sosial terhadap MFA. Menganalisis data menggunakan metode MANOVA dalam analisis faktorial memerlukan beberapa pengujian pada penelitian ini.

a. Uji Normalisasi dimaksudkan untuk memeriksa apakah nilai residual terdistribusi normal. Uji normalisasi dapat diukur dengan Kolmogorov-Smirnov test (K-S test) untuk menentukan tingkat signifikasi. Dalam menentukan apakah nilai Asymp. Sig (2-tailed) residual lebih besar dari >0.05, maka data berdistribusi normal. Sedangkan, jika nilai Asymp. Sig (2-tailed) lebih kecil dari <0,05, maka data tidak berdistribusi normal [17].
b. Uji Reliabilitas menyatakan reliabilitas untuk mengukur suatu kuesioner yang merupakan indikator dari variabel atau konstruktur. pengambilan keputusan untuk pengujian reliabilitas yaitu suatu konstruk atau variabel dikatakan reliabel jika memberikan nilai Cronbach's Alpha> 0,70 [18].
c. Uji Koefisien Determinasi menjelaskan tentang besarnya pengaruh dari seluruh variabel independen terhadap variabel dependen. Pengujian ini dilakukan untuk menjelaskan besaran proporsi variasi dari variabel dependen yang dijelaskan oleh variabel independen [19].
d. Multivariate tests dapat diartikan sebagai tes yang dirancang untuk dapat melihat dan memperhitungkan hasil dari beberapa variabel dependen sekaligus secara bersamaan.
e. Tests of Between-Subjects Effects merupakan hasil keluaran untuk meguji hipotesis penelitian.

3. HASIL DAN PEMBAHASAN

Pada metode pelaksanaan mengenai tahapan-tahapan penelitian yang dilaksanakan pada penelitian ini proses selanjutnya adalah persiapan analisis dan pengujian faktor untuk mengetahui variabel apa saja yang memiliki pengaruh terhadap tingkat kesadaran pengguna media sosial menggunakan metode Multivariate Analysis of Variance (MANOVA) dan metode faktor Technology Threat Avoidance Theory (TTAT).

3.1 Uji Analisis Faktor

Sebelum melakukan pengujian pada analisis faktor model TTAT melakukan pengujian pada hasil pengumpulan data kuesioner online meliputi: uji normalisasi, perhitungan Kaiser-Mayer Olkin Measure of Sampling Adequacy (KMO MSA) dan Bartlett's test, uji reliabilitas dan uji koefisien determinasi.

a. Uji Normalisasi
   Uji normalisasi dilakukan untuk mengetahui apakah data kuesioner tersebut berdistribusi normal atau tidak, berdasarkan hasil tersebut Asymp.Sig (2-tailed) adalah 0.200 lebih besar dari >0.05 yang artinya data tersebut terdistribusi normal, maka pengujian dapat dilanjutkan.

Tabel 3. Hasil kalkulasi Uji Normalisasi

One-Sample Kolmogorov-Smirnov Test	
N	**65**
Asymp. Sig. (2-tailed)	**,200c,d**

b. Perhitungan Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO MSA) dan Bartlett's test.
   Pada perhitungan asumsi analisis faktor (self-efficacy (security awareness), avoidance behaviour, avoidance motivation dan behavioural intention) menunjukkan hasil KMO MSA sebesar 0.702 lebih besar dari >0.60 dan nilai Bartlett's (Sig.) 0,00 < 0.05 maka faktor tersebut memenuhi persyaratan.

Tabel 4. Hasil Kalkulasi KMO dan Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		**,702**
Bartlett's Test of Sphericity	Approx. Chi-Square	**126,705**
	Df	**6**

Journal of Information System Research (JOSH)
Volume 4, No. 3, April 2023, pp 1026−1032
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i3.3081

KMO and Bartlett's Test	
Sig.	**,000**

c. Uji Reliabilitas
Dalam perhitungan reabilitas dapat mengikuti perhitungan Cronbach's Alpha, dengan tolak ukur nilai >0.7 dihitung masing-masing konstruktur untuk mengukur konsistensi kuesioner item. Hal tersebut menunjukan data yang dianalisis sangat reliabel [20].

Tabel 5. Hasil Kalkulasi Cronbach's Alpha

Konstruktur Item Kuesioner	Cronbach's Alpha (>0,70)
Self-Efficacy	**0.736**
Avoidance Motivation	**0.889**
Avoidance Behaviour	**0.729**
Behavioural Intention	**0.805**

d. Uji Koefisien Determinasi (R2)
Pada pengujian ini untuk mengukur kemampuan model tentang besarnya pengaruh dari seluruh variabel independen terhadap variabel dependen. Nilai Adjusted R Square sebesar 0,746 yang artinya kemampuan variabel (faktor) dependen dan variabel (faktor) independen memiliki korelasi kuat .

Tabel 6. Hasil Kalkulasi Koefisien Determinasi

Model Summary	
R	**,871**
R Square	**,758**
Adjusted R Squared	**,746**

3.2 Uji Manova

a. Perhitungan Multivariate Tests
Perhitungan ini menggunakan proses perhitungan pada pengumpulan data set kuesioner bersumber pada faktor model TTAT mencakup faktor (variabel) dependen dan faktor (variabel) independen. Pada kalkulasi perhitungan uji multivariate, adanya pengaruh yang signifikan dari variabel dependen (self efficacy) dengan perolehan nilai signifikansi 0.000 (sig <0.05) pada semua variabel independen (avoidance motivation, avoidance behaviour, dan behavioral intention) maka, hasil uji multivariet dengan model TTAT diterima.

Tabel 7. Hasil Kalkulasi Multivariate Tests

Multivariate Tests	
F	**4,322**
Sig.	**,000**

b. Tests of Between-Subjects Effects
Pada uji tests of between–subjects effect atau uji multivariate analysis of variance (MANOVA) di proses setelah kalkulasi uji multivariate pada faktor (variabel) dependen dan faktor (variabel) independen pada metode TTAT.

Tabel 8. Tests of Between-Subjects Effects

Tests of Between-Subjects Effects		
Variabel Independen	Variabel Dependen	Sig (<0,005)
Avoidance Motivation	Self-efficacy	**0,000**
Advoidance Behaviour	Self-efficacy	**0,029**
Behavioural Intention	Self-efficacy	**0,000**

Berdasarkan hasil tabel diatas menunjukkan, apakah ada faktor yang mempengaruhi faktor self-efficacy terhadap faktor lainnya:

1. Pada faktor Avoidance Motivation (variabel independen) dengan nilai Sig. 0.000 lebih kecil <0.05, maka berpengaruh terhadap faktor Self-efficacy (variabel dependen).
2. Pada faktor Avoidance Behaviour (variabel independen) memperoleh nilai Sig. 0.029 lebih besar > 0.05, maka tidak berpengaruh pada faktor Self-efficacy.
3. Pada faktor Behavioural Intention (variabel independen) di peroleh nilai Sig. 0.000 lebih kecil < 0.05, maka berpengaruh terhadap faktor Self-efficacy.

Journal of Information System Research (JOSH)
Volume 4, No. 3, April 2023, pp 1026−1032
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i3.3081

3.3 Hasil Implementasi

Berdasarkan perhitungan dalam uji manova pada tests of between – subject effect, dalam keterkaitan faktor advoidance motivation mempengaruhi faktor self-efficacy (security awareness) merupakan perilaku untuk menghindari kejadian yang tidak di inginkan dari para responden terhadap pencurian dan ancaman terhadap data privasi tanpa adanya penggunaan multi-factor authentication. Ada juga faktor yang berkaitan lainnya yaitu faktor behavioural intention juga memperngaruhi faktor self-efficacy (security awareness) dimana faktor kepercayaan diri atau perilaku niat dari responden terhadap pengamanan data privasi dengan pengamanan multi-factor authentication hal tersbut juga berdasarkan pada faktor avoidance behaviour dari setiap responden. Behavioural intention dipengaruhi oleh safe-guard cost yang meliputi waktu, keresahan, dan usaha lainnya. Hasil penelitian ini sama dengan yang dilakukan sebelumnya oleh [14].

4. KESIMPULAN

Berdasarkan hasil penelitian tingkat kesadaran dan faktor yang mempengaruhi para pengguna media sosial terhadap Multi-Factor Authentication (MFA). Penerapan metode penelitian kuantitatif berupa data yang dapat digunakan dalam analisis faktor tingkat kesadaran ini berdasarkan pengumpulan data kuesioner online dengan menggunakan metode Multivariate Analysis of Variance (MANOVA). Dari hasil kalkulasi uji MANOVA pada test of between–subject test menunjukan bahwa faktor yang memiliki keterkaitan pada metode Technology Avoidance Thread Theory (TTAT) adalah faktor avoidance motivation yang mempengaruhi faktor self-efficacy (security awareness) secara signifikan dengan kalkulasi (r^2 = 0.499 dan sig. 0.000) dan faktor behavioural intention juga mempengaruhi faktor self-efficacy (security awareness) yaitu dengan kalkulasi (r^2 = 0,427 dan Sig. 0.000).

REFERENCES

[1] C. Mutia Annur, “Jumlah Pengguna Internet di Indonesia (2018-2022),” databoks.katadata.co.id, 2022. https://databoks.katadata.co.id/datapublish/2022/03/23/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022.
[2] R. Nafi’ah, “Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce,” Cyber Secur. dan Forensik Digit., vol. 3, no. 1, pp. 7–13, 2020, doi: 10.14421/csecurity.2020.3.1.1980.
[3] R. Mahmud, “Pencurian Identitas Kategori & Kasus,” Cyber Secur. dan Forensik Digit., vol. 2, no. 1, pp. 38–42, 2019, doi: 10.14421/csecurity.2019.2.1.1421.
[4] S. Widup and V. Communications, “2020 Verizon Data Breach Investigations Report,” 2020, doi: 10.13140/RG.2.2.21300.48008.
[5] S. S. Gupta, A. Thakral, and T. Choudhury, “Social Media Security Analysis of Threats and Security Measures,” 2018 Int. Conf. Adv. Comput. Commun. Eng., no. June, pp. 01–06, 2018, doi: 10.1109/iccomm.2018.8430168.
[6] H. Liang and Y. Xue, “Avoidance of information technology threats: A theoretical perspective,” MIS Q. Manag. Inf. Syst., vol. 33, no. 1, pp. 71–90, 2009, doi: 10.2307/20650279.
[7] F. A. Aloul, “The Need for Effective Information Security Awareness,” J. Adv. Inf. Technol., vol. 3, no. 3, pp. 116–123, 2012, doi: 10.4304/jait.3.3.176-183.
[8] B. A. Sara D. Boysen, “ANALYZING THREAT PERCEPTIONS IN THE CONTEXT OF FITNESS DATA: REFINING THE THREAT CALCULUS IN TECHNOLOGY THREAT AVOIDANCE THEORY,” 2018.
[9] D. K. Young, P. Barrett, A. J. Mcleod, and D. Carpenter, “Refining Technology Threat Avoidance Theory Refining Technology Threat Avoidance Theory,” 2019, doi: 10.17705/1CAIS.04422.
[10] K. Thomas et al., “Protecting accounts from credential stuffing with password breach alerting,” Proc. 28th USENIX Secur. Symp., pp. 1555–1571, 2019.
[11] K. C. Wang and M. K. Reiter, “Detecting stuffing of a user’s credentials at her own accounts,” Proc. 29th USENIX Secur. Symp., pp. 2201–2218, 2020.
[12] H. Liang and Y. Xue, “Understanding security behaviors in personal computer usage: A threat avoidance perspective,” J. Assoc. Inf. Syst., vol. 11, no. 7, pp. 394–413, 2010, doi: 10.17705/1jais.00232.
[13] I. A. Afandi, A. Kusyanti, and N. H. Wardani, “Analisis Hubungan Kesadaran Keamanan , Privasi Informasi , Perilaku Keamanan Pada Para Pengguna Media Sosial Line,” J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 1, no. 9, pp. 783–792, 2017.
[14] K. Saidi and Y. Prayudi, “Analisis Indikator Utama Dalam Information Security - Personality Threat Terhadap Phishing Attack Menggunakan Metode Technology Threat Avoidance Theory (TTAT),” Justindo, vol. 6, no. 1, pp. 21–30, 2021.
[15] H. Unimus, “ANOVA dan MANOVA,” in ANOVA dan MANOVA, 2022, p. 1.
[16] M. M. Dr. Ratna Wijayanti Daniar Paramita, S.E., Cf. Noviansyah Rizal, S.E., M.M., Ak, CA, and M. M. Riza Bahtiar Sulistyan, S.E., METODE PENELITIAN KUANTITATIF, 3rd ed. Lumajang, Jawa Timur: WIDYA GAMA PRESS STIE WIDYA GAMA LUMAJANG, 2021.
[17] I. Ghozali, Aplikasi Analisis Multivariate dengan Program IBM SPSS 25. Semarang: Badan Penerbit Universitas Diponegoro, 2018.
[18] S. Arikunto, Prosedur Penelitian Suatu Pendekatan Praktik. Jakarta: PT. Rineka Cipta, 2010.
[19] S. Raharjo, “Panduan Analisis Faktor dan Interpretasi dengan SPSS Lengkap," SPSS Indonesia,” https://www.spssindonesia.com, 2018. https://www.spssindonesia.com/2018/12/analisis-faktor-dan-interpretasi-spss.html (accessed Jun. 20, 2022).
[20] 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, doi: 10.1016/j.chb.2014.05.046.