Hubungan antara Privacy Concern, Familiaritas SSO, Faktor Demografi, Big Five Personality, dan Literasi Digital terhadap Kesadaran Keamanan Informasi pada Penggunaan Akun SSO di Kalangan Mahasiswa Universitas

Muhamad Nabil Fashhan[1], Candiwan[2]

[1,2]Prodi S1 Manajemen Bisnis Telekomunikasi dan Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom
[1]nabilfashan@student.telkomuniversity.ac.id, [2] candiwan@telkomuniversity.ac.id

Abstrak

Penelitian ini bertujuan untuk menganalisis hubungan antara faktor-faktor seperti kekhawatiran privasi (privacy concern), familiaritas dengan sistem Single Sign-On (SSO), karakteristik demografi, kepribadian Big Five, dan literasi digital terhadap kesadaran keamanan informasi dalam penggunaan akun SSO di kalangan mahasiswa. Sistem SSO, yang memungkinkan akses ke berbagai layanan digital dengan satu kali login, memberikan kemudahan namun juga menimbulkan risiko terkait keamanan informasi. Melalui survei yang melibatkan 384 mahasiswa, penelitian ini menggunakan pendekatan kuantitatif dengan analisis regresi berganda untuk menguji pengaruh masing-masing faktor terhadap kesadaran keamanan informasi. Hasil penelitian menunjukkan bahwa tingkat familiaritas dengan SSO, kekhawatiran privasi, dan literasi digital memiliki pengaruh positif terhadap kesadaran keamanan, sedangkan faktor-faktor demografi dan dimensi kepribadian Big Five berperan penting dalam membentuk perilaku keamanan informasi. Penelitian ini diharapkan dapat memberikan kontribusi dalam merancang kebijakan keamanan yang lebih baik di lingkungan pendidikan tinggi, serta meningkatkan kesadaran dan pemahaman mahasiswa terkait pentingnya perlindungan data pribadi mereka.

Kata kunci: *Kesadaran Keamanan, Single Sign-On (SSO), Kekhawatiran Privasi, Literasi Digital, Big Five Personality, Demografi*.

Abstract

This study aims to analyze the relationship between factors such as privacy concern, familiarity with the Single Sign-On (SSO) system, demographic characteristics, Big Five personality traits, and digital literacy on information security awareness in the use of SSO accounts among university students. The SSO system, which allows access to various digital services with a single login, provides convenience but also introduces risks related to information security. Through a survey involving 384 students, this research employs a quantitative approach with multiple regression analysis to test the impact of each factor on information security awareness. The results show that familiarity with SSO, privacy concern, and digital literacy positively influence security awareness, while demographic factors and Big Five personality traits play an important role in shaping information security behavior. This research is expected to contribute to the development of better security policies in higher education environments and increase students' awareness and understanding of the importance of protecting their personal data.

Keywords: Security Awareness, Single Sign-On (SSO), Privacy Concern, Digital Literacy, Big Five Personality, Demographics.

I. PENDAHULUAN

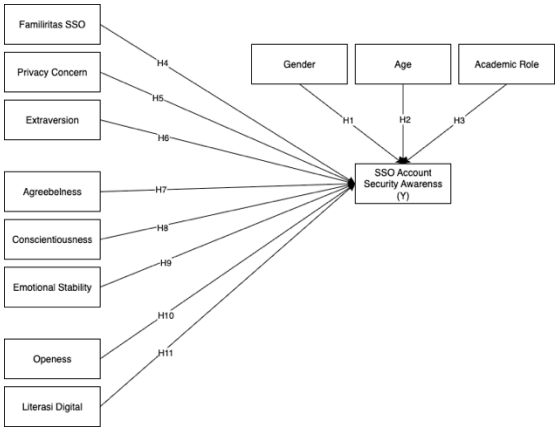
Single Sign-On (SSO) adalah mekanisme autentikasi yang memudahkan pengguna mengakses berbagai layanan digital melalui satu kali login. Di lingkungan perguruan tinggi, SSO digunakan untuk mengakses sistem pembelajaran, perpustakaan digital, dan portal akademik. Meski praktis, mekanisme ini menimbulkan tantangan keamanan, terutama terhadap data pribadi mahasiswa yang rentan disalahgunakan. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN, 2024), insiden kebocoran kredensial akun mahasiswa meningkat 25% dalam setahun terakhir. Survei awal terhadap 50 mahasiswa menunjukkan 60% responden belum memahami risiko penggunaan kata sandi yang sama di berbagai layanan, termasuk SSO. Kondisi ini mengindikasikan rendahnya kesadaran keamanan siber, yang dapat berdampak pada pencurian identitas, akses ilegal ke data akademik, dan kerusakan reputasi institusi.

Kesadaran keamanan informasi merupakan keterampilan penting untuk meminimalkan risiko serangan rekayasa sosial (Solomon et al., 2022). Persepsi keamanan berperan signifikan dalam membentuk kepercayaan pengguna terhadap platform digital (Candiwan & Rianda, 2024). Dalam konteks SSO, kombinasi persepsi keamanan yang rendah dan perilaku pengguna yang berisiko (seperti penggunaan kata sandi yang sama dan tidak melakukan log out) menjadi celah utama bagi serangan siber. Walaupun teknologi keamanan terus berkembang, faktor manusia tetap menjadi titik terlemah. Oleh karena itu, penelitian ini berfokus pada hubungan antara persepsi keamanan dan perilaku mahasiswa terhadap penggunaan SSO, untuk memberikan rekomendasi strategi edukasi keamanan siber yang lebih efektif di lingkungan perguruan tinggi.

II. TINJAUAN LITERATUR

2.1 Kerangka Berfikir

Penelitian ini mengadaptasi kerangka pemikiran Pratama et al. (2022) yang mengaitkan lima dimensi kepribadian *Big Five conscientiousness*, *openness*, *agreeableness*, *extraversion*, dan rendahnya *neuroticism* dengan perilaku keamanan informasi. Kelima dimensi tersebut berkontribusi positif terhadap kesadaran dan perilaku keamanan informasi. Berdasarkan kerangka tersebut, penelitian ini menguji pengaruh demografi, *privacy concern*, familiaritas *Single Sign-On* (SSO), *Big Five Personality*, dan literasi digital terhadap kesadaran keamanan akun SSO. Penambahan variabel literasi digital mengacu pada temuan Saritepeci et al. (2023) yang menunjukkan bahwa literasi digital meningkatkan pemahaman risiko digital dan mendorong perilaku perlindungan privasi online.



Gambar 2.1 Kerangka Pemikiran
Sumber: *(Pratama & Firmansyah, 2021)*

II. METODE

3.1 Populasi dan Sampel

Populasi dalam penelitian ini adalah pengguna Single Sign-On (SSO) di lingkungan universitas dengan target mahasiswa, sedangkan sampel merupakan bagian dari populasi yang dijadikan objek penelitian. Pengambilan sampel dilakukan dengan metode *non-probability sampling*, yaitu teknik yang tidak memberikan peluang yang sama bagi setiap anggota populasi untuk terpilih, mengingat tidak semua pengguna situs kampus mengakses setiap layanan berbasis SSO seperti sistem informasi akademik, perpustakaan digital, dan portal alumni. Kriteria responden meliputi mahasiswa aktif dan pengguna aktif SSO. Jumlah responden ditentukan menggunakan metode Bernoulli karena ukuran populasi yang luas dan tidak diketahui secara pasti. Dengan tingkat ketelitian 5% dan tingkat kepercayaan 95% (nilai Z = 1,96), serta nilai *p* dan *q* masing-masing sebesar 0,05, diperoleh jumlah sampel minimum sebanyak 384 responden.

3.2 Pengumpulan Data dan Sumber Data

Data yang dikumpulkan terdiri dari data primer dan data sekunder. Data primer berasal dari jawaban kuesioner responden, sementara data sekunder diperoleh dari studi literatur seperti jurnal ilmiah, buku, artikel, dan sumber relevan lainnya (Indrawati, 2015). Penelitian ini menggunakan teknik pengumpulan data kuesioner dalam bentuk *Google Form* yang disebarkan secara daring pada grup kampus atau langsung kepada individu yang sedang dalam masa perkuliahan. Penyebaran daring dilakukan untuk menjangkau target responden mahasiswa universitas. Jenis sumber data pada penelitian ini adalah data primer. Data primer berfokus pada informasi yang didapatkan langsung oleh peneliti yang berkaitan dengan variabel yang diteliti. Pada penelitian ini, sumber data primer yang digunakan adalah hasil dari penyebaran kuesioner yang didapatkan secara daring melalui *Google Form*.

3.3 Teknik Analisis Data

3.3.1 Analisis Deskriptif

Analisis deskriptif merupakan teknik statistik yang digunakan untuk menjelaskan atau mendeskripsikan data yang telah dikumpulkan tanpa menarik kesimpulan inferensial. Dalam penelitian ini, analisis dilakukan untuk mengetahui pengaruh *privacy concern*, familiaritas Single Sign-On (SSO), demografi, *Big Five Personality*, dan literasi digital terhadap kesadaran keamanan informasi pada penggunaan akun SSO di kalangan mahasiswa. Instrumen penelitian memuat pernyataan dengan lima opsi jawaban yang dapat dipilih responden. Nilai kumulatif diperoleh dari total jawaban responden pada setiap item, sedangkan persentase dihitung dengan membagi nilai kumulatif dengan frekuensi, kemudian dikalikan 100%. Kategori penilaian terdiri dari: Sangat Tidak Baik (20%–36%), Tidak Baik (>36%–52%), Cukup Baik (>52%–68%), Baik (>68%–84%), dan Sangat Baik (>84%–100%). Skor total setiap variabel dihitung dengan menjumlahkan respon “sangat setuju”, “setuju”, “cukup setuju”, “tidak setuju”, dan “sangat tidak setuju”, sedangkan skor ideal diasumsikan jika seluruh responden memilih “sangat setuju”.

3.3.2 Uji Asumsi Klasik

Uji asumsi klasik diperlukan sebelum analisis regresi linear berganda, terdiri dari uji normalitas, uji multikolinearitas, dan uji heteroskedastisitas. Uji Normalitas Data: Bertujuan memastikan data sampel berasal dari populasi yang terdistribusi normal, karena hasil uji statistik (t atau f) akan disajikan sebagai parameter populasi. Kriteria normalitas terpenuhi jika hasil pengujian tidak signifikan pada taraf signifikan tertentu (α), atau jika data menyebar di

sekitar diagonal dan histogram menunjukkan pola terdistribusi normal. Uji Multikolinearitas: Bertujuan mengetahui hubungan signifikan antar variabel bebas. Korelasi tinggi antar variabel independen akan mengurangi keyakinan terhadap hasil pengujian. Pengujian dilakukan dengan memeriksa nilai VIF dan koefisien antar variabel bebas. Regresi bebas multikolinearitas jika VIF kurang dari 10 dan nilai toleransi lebih dari 0,1.

3.3.3 Analisis Regresi Berganda

Analisis regresi berganda berfungsi sebagai analisis untuk mencari hubungan antara dua atau lebih variabel independent (X1,X2,X3,..Xn) terhadap variabel independent (Y) secara bersamaan. Analisis regresi berganda diperlukan jika bertujuan memprediksi suatu kondisi (kenaikan atau penurunan) variabel dependen, jika dua atau lebih variabel independent menjadi faktor prediksi. Penelitian ini menggunakan enam prediktor yaitu, Age (X1), Gender (X2), Academic Role (X3), Privacy Concern (X4), SSO Familiarity (X5), Big Five Personality (X6) dan literasi digital (X7). Sehingga persamaan regresi yang digunakan sebagai berikut:

$$Y = \alpha + \beta1X1 + \beta2X2 + \beta3X3 + \beta4X4 + \beta5X5 + \beta6X6 + \beta7X7 +$$

3.3.4 Uji Hipotesis

Hipotesis merupakan dugaan sementara yang sifatnya di sebuah kejadian pada suatu fenomena, namun diharuskan untuk diberi bukti maupun diuji kebenarannya dengan empiris (Bambang et al., n.d.; Nugroho & Haritanto, 2022).

3.3.4.1 Uji t

Uji t digunakan untuk menguji signifikansi dari koefisien pada regresi linear berganda. Untuk pengambilan keputusan, hipotesis dapat dilakukan dengan membandingkan nilai statistik dari uji t (thitung) terhadap nilai kritis t (tkritis). Pengambilan keputusan pada uji t dapat dijelaskan sebagai:

1. Jika | thitung | ≤ | tkritis |, maka H0 diterima dan H1 ditolak
2. Jika | thitung | > | tkritis |, maka H0 ditolak dan H1 diterima

Pengambilan keputusan terhadap hipotesis uji t juga dapat dilakukan dengan cara membandingkan nilai probabilitas dari uji t dengan tingkat signifikansi yang digunakan. Berikut ini adalah syarat pengambilan keputusan yang berdasarkan nilai probabilitas :

1. Jika nilai probabilitas ≥ tingkat signifikansi, maka H0 diterima dan H1 ditolak.
2. Jika nilai probabilitas < tingkat signifikansi, maka H0 ditolak dan H1 diterima

3.3.4.2 Uji F

Uji simultan (F) digunakan untuk menguji apakah persamaan regresi linear yang diperoleh benar-benar bermakna atau mampu menjelaskan bahwa variabel bebas secara simultan atau bersamaan mempengaruhi variabel tidak bebas. Pengambilan keputusan hipotesis dapat dilakukan dengan cara membandingkan nilai probabilitas dari uji F dengan tingkat signifikansi yang digunakan. Berikut ini adalah syarat pengambilan keputusan yang berdasarkan pendekatan nilai probabilitas:

1. Jika nilai probabilitas ≥ tingkat signifikansi, maka H_0 diterima dan H_1 ditolak.
2. Jika nilai probabilitas < tingkat signifikansi, maka H_0 ditolak dan H_1 diterima.

3.3.4.3 Uji Koefisien Determinasi

Menurut Nugroho & Haritanto (2019) pengujian ini dilakukan untuk melihat besaran bagian dari jumlah semua macam elemen dependen yang dideskripsikan pada variabel independen dalam penelitian ini. Apabila koefisien determinasi (R^2) kecil, artinya variabel independen memberikan sedikit atau bahkan tidak ada penjelasan terhadap variasi variabel dependen. Sebaliknya, apabila koefisien determinasi besar maka variabel independen memperlihatkan hampir semua hal tentang bagaimana variabel dependen menjelaskan. Berikut adalah persamaannya:

$$KD = R^2 \text{ x } 100\%$$

Keterangan:
KD = berapa jauh macam variabel terikat dinyatakan oleh elemen bebas.
R^2 = Kuadrat Koefesien Korelasi.

III. HASIL DAN PEMBAHASAN

4.1 Statistik Deskritptif

Analisis deskriptif bertujuan untuk memberikan gambaran data yang telah dikumpulkan dari responden. Kategori penilaian skor variabel didasarkan pada rentang persentase.

Tabel 4.1 Hasil Analisis Deskriptif Variabel

Variabel	Rata-rata Skor	Persentase (%)	Kategori Penilaian
Privacy Concern	4.18	83.6	Baik
Familiaritas SSO	4.21	84.2	Sangat Baik
Big Five Personality	3.95	79	Baik
Literasi Digital	4.35	87	Sangat Baik
Kesadaran Keamanan (Y)	4.28	85.6	Sangat Baik

Sumber: Olah Data Peneliti, 2024

Berdasarkan Tabel 4.3, secara umum seluruh variabel penelitian berada pada kategori "Baik" hingga "Sangat Baik." Variabel Literasi Digital menunjukkan persentase tertinggi (87.0%), yang mengindikasikan bahwa responden memiliki pemahaman yang sangat baik terkait teknologi digital. Variabel dependen, Kesadaran Keamanan Informasi (Security

Awareness), juga berada dalam kategori "Sangat Baik" (85.6%), yang menunjukkan bahwa mahasiswa secara umum telah memiliki pengetahuan, sikap, dan perilaku yang positif terkait keamanan akun SSO mereka.

4.2 Uji Asumsi Klasik

Sebelum menarik kesimpulan dari hasil regresi linear berganda, perlu dipastikan bahwa model regresi memenuhi tiga asumsi klasik, yaitu normalitas residual, tidak adanya multikolinearitas, dan tidak adanya heteroskedastisitas.

4.2.1 Uji Normalitas

Hasil Uji normalitas residual dilakukan menggunakan Kolmogorov-Smirnov. Hasil uji menunjukkan nilai D = 0.02512 dengan p-value = 0.9687. Karena p-value lebih besar dari 0.05, maka distribusi residual dianggap normal. Hal ini mengindikasikan bahwa model tidak melanggar asumsi normalitas, dan residual menyebar dengan pola mendekati distribusi normal. Distribusi residual yang normal penting untuk menjamin validitas uji signifikansi dalam model regresi (A. Ghasemi, 2012).

4.2.2 Uji Multikolinearitas

Pengujian multikolinearitas dilakukan dengan melihat nilai Variance Inflation Factor (VIF). Semua nilai VIF dalam model berada di bawah 2, dengan nilai tertinggi pada variabel literasi digital (2.25).

```
vif(model)

##                       GVIF Df GVIF^(1/(2*Df))
## gender            1.040685  1        1.020140
## age               1.026072  1        1.012952
## roles             1.048042  2        1.011800
## familiarity       1.476842  1        1.215254
## privacy           1.786905  1        1.336752
## literacy          2.249312  1        1.499771
## extraversion      1.023459  1        1.011662
## agreeableness     1.018043  1        1.008981
## conscientiousness 1.016660  1        1.008296
## emotionalstability 1.031072  1        1.015417
## openness          1.046255  1        1.022866
```

Gambar 4.1 VIF Model

Sumber: Diolah Penulis (2024)

Nilai-nilai VIF tersebut jauh di bawah ambang batas kritis 10 sebagaimana disarankan oleh (Joseph F. Hair et al., 2010) dan GVIF(1/2df) di bawah 2 (John Fox & Georges Monette, 1992). Dengan demikian, tidak ditemukan adanya multikolinearitas antar variabel independen.

4.2.3 Uji Heteroskedastisitas

Untuk mendeteksi heteroskedastisitas, dilakukan visualisasi grafik antara nilai residual dan fitted values. Grafik menunjukkan pola sebaran residual yang menyebar acak di sekitar garis nol tanpa pola tertentu. Ini mengindikasikan bahwa variansi residual bersifat homogen (homoskedastisitas). Hal ini menunjukkan bahwa asumsi homoskedastisitas terpenuhi dan regresi yang dilakukan bebas dari masalah heteroskedastisitas (Gujarati & Porter, 2009).

4.3 Pengujian Hipotesis

4.3.1 Uji t

Berdasarkan hasil pengujian *Ordinal Least Square* (OLS), sebagian besar hipotesis penelitian ini diterima, meskipun terdapat beberapa yang ditolak karena tidak memenuhi kriteria signifikansi statistik ($p > 0,05$). Variabel usia (H2) dan *roles* (H3) terbukti berpengaruh signifikan terhadap kesadaran keamanan akun Single Sign-On (SSO). Temuan ini mengindikasikan bahwa perbedaan usia dan peran akademik berkontribusi pada tingkat kesadaran keamanan, di mana individu yang lebih muda dan memiliki peran aktif, seperti staf, cenderung menunjukkan kesadaran yang lebih tinggi. Selanjutnya, variabel *familiarity* (H4), *privacy concern* (H5), dan literasi digital (H13) juga berpengaruh signifikan dan positif terhadap kesadaran keamanan, mendukung asumsi teoritis sebelumnya. Literasi digital muncul sebagai prediktor penting dalam memahami risiko dan menerapkan praktik keamanan yang tepat pada sistem SSO, sejalan dengan temuan Saritepeci et al. (2023) dan GÖLDAĞ (2021).

Sementara itu, dimensi kepribadian *Big Five* menunjukkan hasil yang beragam. *Extraversion* (H6) dan *agreeableness*(H7) tidak berpengaruh signifikan terhadap kesadaran keamanan, sedangkan *conscientiousness* (H8) berpengaruh positif dan signifikan ($p = 0,002$), yang menunjukkan bahwa individu dengan tingkat *conscientiousness* tinggi cenderung lebih berhati-hati dan sadar akan keamanan akun. *Emotional stability* (H9) berpengaruh positif namun hanya mendekati signifikansi ($p = 0,048$), sehingga memerlukan kajian lebih lanjut, sedangkan *openness* (H10) tidak berpengaruh signifikan.

Uji interaksi menunjukkan bahwa *agreeableness* × *privacy concern* (H11) dan *conscientiousness* × *privacy concern*(H12) berpengaruh signifikan, dengan nilai $p < 0,05$ pada keduanya. Secara keseluruhan, hasil ini memperkuat bahwa literasi digital, tingkat familiaritas terhadap SSO, serta faktor usia dan peran akademik berperan penting dalam membentuk kesadaran keamanan informasi. Namun, tidak semua dimensi kepribadian memberikan pengaruh signifikan, sehingga membuka peluang penelitian lanjutan untuk mengeksplorasi hubungan ini secara lebih mendalam.

4.4 Pembahasan Hasil Penelitian

4.4.1 Age (Usia) Berpengaruh terhadap Security Awareness

Hasil analisis menunjukkan bahwa usia berpengaruh signifikan terhadap kesadaran keamanan informasi pada penggunaan akun Single Sign-On (SSO) di kalangan mahasiswa (koefisien -0,331; $p = 0,018 < 0,05$). Mahasiswa yang

lebih muda cenderung memiliki kesadaran keamanan lebih tinggi dibandingkan yang lebih tua. Hal ini sejalan dengan Shillair (2015) yang menyatakan bahwa faktor demografis memengaruhi kepercayaan, kesadaran risiko, dan efektivitas adopsi praktik keamanan daring. Meskipun literasi digital pada usia muda umumnya lebih baik, risiko privasi sering diabaikan; sebaliknya, usia yang lebih tua cenderung lebih waspada namun menghadapi keterbatasan teknis. Temuan ini menegaskan pentingnya mempertimbangkan usia dalam merancang strategi edukasi keamanan siber yang tepat sasaran.

4.5.3 Academic Role (Peran Akademik) Berpengaruh terhadap Security Awareness

Peran dalam organisasi terbukti berpengaruh signifikan terhadap kesadaran keamanan informasi (*security awareness*), dengan koefisien 0,696 dan p-value 0,045. Hubungan positif ini menunjukkan bahwa semakin jelas dan terstruktur peran individu, semakin tinggi kesadaran mereka akan pentingnya menjaga keamanan informasi. Temuan ini selaras dengan Lebek et al. (2014) yang menyatakan bahwa definisi peran yang baik meningkatkan perilaku keamanan informasi melalui pemahaman tanggung jawab dan konsekuensi tindakan terkait pengelolaan informasi organisasi.

4.5.4 Familiaritas Single Sign-On (SSO) Berpengaruh terhadap Security Awareness

Hasil penelitian menunjukkan bahwa familiaritas terhadap Single Sign-On (SSO) berpengaruh signifikan terhadap kesadaran keamanan informasi (koefisien 0,095; $p = 0,018 < 0,05$). Meskipun pengaruhnya relatif kecil, hasil ini menunjukkan bahwa semakin tinggi pemahaman dan pengalaman individu menggunakan SSO, semakin besar kesadaran mereka dalam menjaga keamanan informasi. Temuan ini konsisten dengan Hadlington (2017) yang menyatakan bahwa faktor psikologis dan perilaku, termasuk pengalaman dengan teknologi keamanan seperti SSO, berkontribusi pada peningkatan kesadaran keamanan siber.

4.7.5 Privacy Concern Berpengaruh terhadap Security Awareness

Privacy concern atau kekhawatiran terhadap privasi berpengaruh signifikan terhadap kesadaran keamanan informasi (koefisien 0,081; $p = 0,017 < 0,05$). Meskipun pengaruhnya relatif kecil, hasil ini menunjukkan bahwa individu dengan kepedulian tinggi terhadap perlindungan data pribadi cenderung lebih sadar dan waspada terhadap isu keamanan informasi. Temuan ini konsisten dengan Solove (2008) yang menegaskan bahwa kesadaran akan risiko penyalahgunaan data pribadi mendorong perilaku yang lebih hati-hati dan bertanggung jawab dalam menjaga keamanan informasi.

4.7.6 Extraversion Berpengaruh terhadap Security Awareness

Hasil analisis menunjukkan bahwa dimensi kepribadian extraversion tidak berpengaruh signifikan terhadap kesadaran keamanan informasi (koefisien -1,149; $p = 0,654 > 0,05$), sehingga hipotesis ditolak. Artinya, tingkat ekstraversi seseorang tidak terbukti memengaruhi kesadaran keamanan mereka. Meski demikian, arah hubungan negatif ini sejalan dengan temuan Pratama et al. (2022) yang menunjukkan bahwa individu dengan ekstraversi tinggi cenderung lebih terbuka dan aktif secara sosial, sehingga lebih rentan terhadap risiko keamanan akibat kebiasaan berbagi informasi secara bebas.

4.7.7 Agreeableness Berpengaruh terhadap Security Awareness

Agreeableness tidak berpengaruh signifikan terhadap kesadaran keamanan informasi (koefisien -16,446; $p = 0,071 > 0,05$), sehingga hipotesis ditolak. Meski demikian, arah hubungan negatif sejalan dengan temuan Pratama et al. (2022) yang menyatakan bahwa individu dengan agreeableness tinggi cenderung mudah percaya dan ingin membantu, sehingga berpotensi mengurangi kewaspadaan terhadap risiko keamanan informasi. Pola ini mendukung logika teoritis bahwa sifat terlalu kooperatif dapat menjadi kerentanan dalam konteks keamanan informasi.

4.7.8 Conscientiousness Berpengaruh terhadap Security Awareness

Berdasarkan hasil penelitian, conscientiousness berpengaruh signifikan terhadap kesadaran keamanan informasi (koefisien 15,300; $p = 0,002 < 0,05$), sehingga hipotesis diterima. Individu dengan conscientiousness tinggi—disiplin, bertanggung jawab, dan berhati-hati—memiliki kesadaran keamanan lebih baik. Temuan ini selaras dengan Shappie et al. (2020) yang menyatakan bahwa conscientiousness meningkatkan kepatuhan terhadap kebijakan keamanan, kehati-hatian dalam mengelola data, dan motivasi menghindari kesalahan yang berpotensi membahayakan sistem informasi. Karakteristik ini berkontribusi penting dalam membentuk perilaku aman dalam penggunaan teknologi informasi di lingkungan organisasi.

4.7.9 Emotional Stability Berpengaruh terhadap Security Awareness

Hasil analisis menunjukkan bahwa emotional stability berpengaruh signifikan terhadap kesadaran keamanan informasi (koefisien 1,427; $p = 0,048 < 0,05$), sehingga hipotesis diterima. Individu yang tenang, tidak mudah cemas, dan mampu mengelola stres cenderung memiliki kesadaran lebih tinggi terhadap keamanan informasi. Temuan ini sejalan dengan Russell et al. (2017) yang menunjukkan bahwa stabilitas emosional berhubungan positif dengan kepatuhan terhadap kebijakan keamanan. Individu yang stabil secara emosional lebih rasional dalam menghadapi risiko, mengikuti prosedur keamanan, dan menghindari tindakan impulsif yang dapat memicu pelanggaran, sehingga menjadi prediktor penting perilaku sadar keamanan di organisasi maupun penggunaan teknologi digital sehari-hari.

4.7.10 Openness Berpengaruh terhadap Security Awareness

Penelitian ini juga menunjukkan bahwa variabel openness berpengaruh negatif terhadap kesadaran keamanan (koefisien –1,348) namun tidak signifikan secara statistik ($p = 0,069 > 0,05$), sehingga hipotesis ditolak. Temuan ini sejalan dengan Moutafi et al. (2006) yang menjelaskan bahwa keterbukaan terdiri dari berbagai aspek, seperti ide, tindakan, fantasi, perasaan, dan nilai-nilai, di mana tidak semua aspek berkontribusi positif terhadap hasil kognitif atau perilaku adaptif. Arah negatif dalam penelitian ini dapat disebabkan oleh aspek keterbukaan tertentu, seperti fantasi atau toleransi terhadap ambiguitas, yang membuat individu cenderung lebih permisif dan kurang waspada terhadap ancaman digital, sehingga menurunkan tingkat kesadaran keamanan.

V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini bertujuan untuk menganalisis pengaruh privacy concern, familiaritas terhadap sistem Single Sign-On (SSO), faktor demografi, Big Five Personality, dan literasi digital terhadap kesadaran keamanan informasi (security awareness) pada mahasiswa pengguna akun SSO universitas. Sebanyak 384 responden berpartisipasi, mewakili pengguna layanan digital kampus seperti portal akademik, e-learning, dan email institusional. Fokus penelitian ini adalah mengkaji peran faktor internal (kepribadian) dan eksternal (literasi digital, persepsi privasi) dalam memengaruhi kewaspadaan terhadap risiko keamanan digital.

Hasil penelitian menunjukkan bahwa variabel usia, peran dalam organisasi, familiaritas SSO, conscientiousness, emotional stability, dan literasi digital berpengaruh positif terhadap kesadaran keamanan, meskipun tidak seluruhnya signifikan secara statistik. Mahasiswa yang lebih muda, memiliki peran organisasi yang jelas, dan terbiasa menggunakan SSO cenderung lebih sadar terhadap risiko keamanan. Sifat conscientious dan kestabilan emosi juga berkontribusi pada perilaku yang lebih patuh terhadap prosedur keamanan.

Sementara itu, extraversion, agreeableness, openness, dan privacy concern tidak berpengaruh signifikan secara langsung terhadap security awareness. Namun, interaksi antara privacy concern dengan sifat kepribadian tertentu seperti conscientiousness dan agreeableness menunjukkan potensi meningkatkan kewaspadaan, khususnya saat kepercayaan terhadap sistem menjadi faktor penting.

Literasi digital menjadi faktor paling signifikan, mencakup kemampuan teknis sekaligus kesadaran kritis dalam melindungi data pribadi. Temuan ini menegaskan perlunya strategi edukasi keamanan siber yang mengintegrasikan peningkatan literasi digital, pemahaman peran organisasi, dan kesadaran risiko berbasis profil demografis serta karakter pengguna.

5.2 Saran

Berdasarkan hasil penelitian, disarankan agar lembaga pendidikan tinggi menyelenggarakan program literasi digital yang menekankan aspek keamanan informasi, mencakup keterampilan teknis dan kesadaran kritis terhadap perlindungan data pribadi. Peningkatan pemahaman mengenai sistem autentikasi seperti Single Sign-On (SSO) dapat dilakukan melalui sosialisasi dan pelatihan berbasis pengalaman langsung, sehingga mahasiswa dapat memahami risiko dan praktik aman secara lebih kontekstual.

Selain itu, strategi peningkatan kesadaran keamanan informasi dapat mengintegrasikan materi yang relevan dengan berbagai tipe kepribadian, manajemen stres, dan pembinaan disiplin kepatuhan kebijakan keamanan. Edukasi ini sebaiknya juga disertai dengan penjelasan peran dan tanggung jawab individu dalam organisasi untuk menumbuhkan perilaku digital yang aman.

Untuk penelitian selanjutnya, disarankan mengeksplorasi peran mediasi atau moderasi variabel kepribadian, memperluas populasi sampel ke pengguna umum di luar lingkungan akademik, serta mengombinasikan metode kualitatif dan kuantitatif untuk mendapatkan pemahaman lebih mendalam tentang persepsi pengguna terhadap keamanan informasi. Penelitian ini diharapkan memberikan kontribusi akademik dalam memahami faktor-faktor yang memengaruhi kesadaran keamanan informasi pada sistem otentikasi terpusat, serta menjadi pijakan dalam merancang strategi intervensi berbasis perilaku dan psikologi pengguna.

Daftar Pustaka

Bambang, D. A., Jarkawi, S., Primadewi, K., Habibah, U., Lounggina, T., Peny, L., Pratama, K., Derry, R., Wiena, N., Abdul, S., Zulfiah, W., Bambang, L., Firdaus, S., & Dharta, Y. (n.d.). *METODE PENELITIAN KUANTITATIF*. https://penerbitzaini.com/

Candiwan, C., & Rianda, L. M. (2024). Transactions at Your Fingertips: Influential Factors in Information Security Behavior for Mobile Banking Users. *International Journal of Safety and Security Engineering*, *14*(3), 795–806. https://doi.org/10.18280/ijsse.140312

Candiwan, Kencana Sari, P., & Pertiwi Sudirman, B. (2023). *Differences in Information Security Behavior of Smartphone Users in Indonesia Using Pearson's Chi-square and Post Hoc Test*. *13*(2).

Daniel J. Solove. (2008). A Taxonomy of Privacy. *University of Pennsylvania Law Review*.

GÖLDAĞ, B. (2021). Üniversite Öğrencilerinin Dijital Okuryazarlık Düzeyleri İle Dijital Veri Güvenliği Farkındalık Düzeyleri Arasındaki İlişkinin İncelenmesi. *E-International Journal of Educational Research*. https://doi.org/10.19160/e-ijer.950635

Gujarati, & Porter. (2009). *Basic Econometrics*.

Hadlington, L. (2017). *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours*. *3*(7).

Indrawati, Ph. D. (2015). *Metode Penelitian Manajemen dan Bisnis: Konvergensi Teknologi Komunikasi dan Informasi*.

John Fox, & Georges Monette. (1992). Generalized collinearity diagnostics. *Journal of the American Statistical Association*.

Joseph F. Hair, William C. Black, Barry J. Babin, & Rolph E. Anderson. (2010). *Multivariate Data Analysis*.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Moutafi, Joanna, & Adrian. (2006). *What facets of openness and conscientiousness predict fluid intelligence score?*

Nugroho, A. S., & Haritanto, W. (2022). *Metode Penelitian Kuantitatif dengan Pendekatan Statistika: Teori, Implementasi & Praktik dengan SPSS*. Penerbit Andi.

Pratama, A. R., & Firmansyah, F. M. (2021). Until you have something to lose! Loss aversion and two-factor authentication adoption. *Applied Computing and Informatics*. https://doi.org/10.1108/aci-12-2020-0156

Pratama, A. R., Firmansyah, F. M., & Rahma, F. (2022). Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality. *PeerJ Computer Science*, *8*. https://doi.org/10.7717/PEERJ-CS.918

Russell, J. D., Weems, C. F., Ahmed, I., & Richard III, G. G. (2017). Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. *Journal of Cyber Security Technology*, *1*(3–4), 163–174. https://doi.org/10.1080/23742917.2017.1345271

Saritepeci, M., Durak, H. Y., Kırs¸ehir, K., Ufer, N., & Uslu, A. (2023). *The role of digital literacy and digital data security awareness in online privacy concerns: a multi-group analysis with gender*. https://doi.org/10.1108/OIR

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 475–480. https://doi.org/10.1037/ppm0000247

Shillair, R. ; C. S. R. ; T. H. Y. S. ; A. S. ; L. R. ; R. N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*.

Siagian, H., Tarigan, Z. J. H., Basana, S. R., & Basuki, R. (2022). The effect of perceived security, perceived ease of use, and perceived usefulness on consumer behavioral intention through trust in digital payment platform. *International Journal of Data and Network Science*, *6*(3), 861–874. https://doi.org/10.5267/j.ijdns.2022.2.010

Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R., & Shabtai, A. (2022). Contextual security awareness: A context-based approach for assessing the security awareness of users. *Knowledge-Based Systems*, *246*. https://doi.org/10.1016/j.knosys.2022.108709