ANALISIS KESADARAN *CYBER SECURITY* PADA KALANGAN PELAKU *E-COMMERCE* DI INDONESIA

Disusun Oleh:

N a m a : Galih Rahmadi
NIM : 16523077

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2020

HALAMAN PENGESAHAN DOSEN PEMBIMBING

ANALISIS KESADARAN *CYBER SECURITY* PADA KALANGAN PELAKU *E-COMMERCE* DI INDONESIA

TUGAS AKHIR

Disusun Oleh:

N a m a : Galih Rahmadi

NIM : 16523077

Yogyakarta, 24 Juli 2020

Pembimbing,

(Ahmad Munasir Rafie Pratama, ST., M.I.T., Ph.D)

HALAMAN PENGESAHAN DOSEN PENGUJI

ANALISIS KESADARAN CYBER SECURITY PADA KALANGAN PELAKU E-COMMERCE DI INDONESIA

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 24 Juli 2020

Tim Penguji

Ahmad Munasir Raf'ie Pratama, ST., M.I.T., Ph.D.

Anggota 1

Dr. Ing. Ridho Rahmadi, S.Kom., M.Sc.

Anggota 2

Sheila Nurul Huda, S.Kom., M.Cs.

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

(Dr. Raden Teduh Dirgahayu, S.T., M.Sc.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Galih Rahmadi

NIM : 16523077

Tugas akhir dengan judul:

ANALISIS KESADARAN *CYBER SECURITY* PADA KALANGAN PELAKU *E-COMMERCE* DI INDONESIA

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung resiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 24 Juli 2020

(Galih Rahmadi)

HALAMAN PERSEMBAHAN

Alhamdulillahirabbil'alamin

Karya sederhana ini saya persembahkan untuk:

Bapak dan Mama

Atas segala do'a, dukungan, cinta, kasih sayang dan jerih payah mereka. Yang saya ketahui dan tidak saya ketahui, yang saya sadari dan tidak saya sadari. Terima kasih, kesayanganku.

Adik-adikku

Atas semua do'a, dukungan, motivasi, kasih sayang, nasehat yang selalu ingin menjadikan penulis lebih baik dan bermanfaat bagi orang lain.

Seluruh Keluarga Besar

Terima kasih atas do'a, nasehat, dan bantuan yang telah diberikan selama ini.

HALAMAN MOTO

فَٱذۡكُرُونِيٓ أَذۡكُرۡكُمۡ وَٱشۡكُرُواْ لِي وَلَا تَكۡفُرُونِ

"Karena itu, ingatlah kalian kepada-Ku, niscaya Aku ingat (pula) kepada kalian; dan bersyukurlah kepada-Ku, dan janganlah kalian mengingkari (nikmat-Ku)."

Q.S Al Baqarah: 152

"I believe whatever doesn't kill you, simply makes you stronger."

The Joker Heath Ledger

"Why do we fall? So that we can learn to pick ourselves back up."

Galih Rahmadi

KATA PENGANTAR

Segala puji dan syukur tak terhingga kepada Allah *Subhanallahu wa ta'alla* yang Maha Agung dan Maha Pengasih atas nikmat dan rahmat-Nya, serta segala kekuatan, kemudahan dan kelancaran sehingga karya ini dapat terselesaikan dengan baik. Sholawat dan salam selalu tercurahkan kepada Nabi Muhammad *shallalluhu 'alaihi wa sallam*, keluarga, sahabat dan para pengikutnya.

Penulis menyadari bahwa dalam penyelesaian skripsi ini banyak pihak yang telah memberikan bantuan, bimbingan, dan dukungan. Oleh karena itu, dalam kesempatan ini perkenankan penulis mengucapkan terima kasih yang tak terhingga kepada:

1. Kedua orang tua tercinta (Bapak Zul Amri, S.H. dan Mama Nining Agustriana) dan Adik-adikku (Aulia Shaharani dan Humaira Rahadatul Aisy) yang tiada hentinya memberikan doa, cinta, kasih sayang, dukungan, motivasi, serta pengorbanan yang tak terhingga selama ini hingga skripsi dan masa perkuliahan ini dapat diselesaikan.
2. Bapak Dr. Raden Teduh Dirgahayu, S.T., M.Sc. selaku Ketua Program Studi Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.
3. Bapak Ahmad Munasir Raf'ie Pratama, ST., M.I.T., Ph.D. selaku Dosen Pembimbing Skripsi, atas segala bimbingan, waktu, dan pemikiran yang diberikan sejak sebelum skripsi ini dibuat, baik itu siang maupun malam, dan ketika sibuk dan juga senggang. Semoga Allah SWT membalas kebaikan Bapak sebagai amal jariyah, *Aamiin Yaa Rabbal 'aalamiin*.
4. Bapak Beni Suranto, S.T., M.Soft.Eng. selaku Dosen Pembimbing Akademik yang memberikan dukungan, motivasi, serta konsultasi yang berperan besar terhadap masa perkuliahan saya.
5. Seluruh dosen Program Studi Informatika Fakultas Teknologi Industri Universitas Islam Indonesia yang banyak memberikan ilmu, pelajaran, pengalaman, serta nasihat yang tak dapat terhitung jumlahnya. Semoga kebaikan Bapak/Ibu dosen dibalas oleh Allah SWT dengan balasan yang baik pula.
6. Kepada yang tersayang yang selalu memberikan semangat, doa, dukungan, motivasi, dan bantuan hingga skripsi ini dapat diselesaikan. Semoga Allah senantiasa memberikan kelancaran serta barokah-Nya pada setiap langkah dan segala urusan.
7. Kepada Sobat Batam (Rey, Iven, Gari, Faiz, Albab, Dina, Tiara, Rava) terima kasih atas waktu dan kebersamaan serta rasa persaudaraan yang telah tercipta selama penulis di Jogja.

Dukungan yang tiada habisnya kalian berikan memberikan kontribusi terhadap penelitian ini. Semoga kekeluargaan kita tetap terjalin dengan baik disusul dengan masa depan yang baik pula.

8. Teman-teman seperjuangan Skuy Living (Ahmad Padil, Aripin, Yoga, Rifqi, Rasyid, Astri, Afifah, Atikah) dan yang lainnya tak bisa penulis sebutkan satu per satu, terima kasih atas dukungan dan waktu kebersamaannya selama masa perkuliahan yang kemudian menjadikan Jogja semakin dirindukan. Semoga kesuksesan selalu mengiringi kalian semua.
9. Teman-teman Informatika UII angkatan 2016, atas segala bantuan dan kebersamaan selama masa perkuliahan. Semoga silaturahmi kita bisa tetap terjalin dengan baik.
10. Semua pihak yang telah membantu penulis dengan penuh keikhlasan, yang tidak dapat disebutkan satu persatu, terima kasih atas segala bantuan yang telah diberikan kepada penulis.

Pada akhirnya, penulis mengharapkan semoga skripsi ini dapat bermanfaat bagi penulis dan semua pihak yang berkenan menelaah di kemudian hari. Semoga Allah SWT memberikan limpahan rahmat, karunia dan balasan yang lebih baik atas kebaikan semua pihak yang secara langsung maupun tidak langsung membantu terwujudnya skripsi ini, Aamiin ya Rabbal alamin.

Yogyakarta, 24 Juli 2020

(Galih Rahmadi)

ABSTRAK

Hadirnya *e-commerce* di Indonesia sebagai aktivitas jual beli barang atau jasa melalui internet memungkinkan dapat terjadinya *cybercrime*. Ancaman terjadinya *cybercrime* merupakan hal yang dapat mengganggu aktivitas *e-commerce*, sehingga konsumen maupun pelaku usaha harus mampu melindungi dari ancaman tersebut dengan *cyber security*. Maka peneliti berusaha melakukan penelitian terkait faktor-faktor apa saja yang mempengaruhi kesadaran *cyber security* pada kalangan pelaku *e-commerce* terhadap ancaman *cybercrime*. Analisis data ini menggunakan sumber data primer dari hasil kuisioner yang dibagikan kepada pengguna *e-commerce.* Penelitian ini menggunakan teknik *Structural Equation Modeling* (SEM), untuk mengukur hubungan antar variabel laten berupa pengetahuan dan kesadaran *cyber security* dengan demografi pengguna *e-commerce*. Hasil penelitian menunjukkan bahwa variabel pengetahuan *cyber security* terdapat hubungan yang memiliki sifat signifikan terhadap kesadaran *cyber security* pelaku *e-commerce* dan variabel jenis kelamin memiliki hubungan bersifat signifikan terhadap pengetahuan *cyber security* yang secara tidak langsung berpengaruh pada kesadaran *cyber security.*

Kata kunci: *cyber security, e-commerce, structural equation modeling,* kesadaran.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era disrupsi ini memaksa pelaku usaha untuk selalu melakukan inovasi agar dapat beradaptasi terhadap kegiatan perdagangan pelaku *e-commerce* agar memberikan kelancaran dalam proses bisnis sehingga dapat bersaing secara kompetitif. Salah satu yang dilakukan pelaku usaha yaitu dengan menggunakan teknologi internet dalam proses bisnis sehingga membuat peralihan dari antar muka ke internet. Teknologi tersebut kita kenal dengan istilah *electronic commerce (e-commerce)* atau perdagangan elektronik. Karena adanya e-*commerce* membuat transaksi menjadi lebih interaktif, mudah, murah, dan cepat dalam mendapatkan produk atau jasa yang masyarakat inginkan. Hal ini lah yang dimanfaatkan pelaku usaha sehingga dapat menciptakan peluang bisnis yang signifikan, meningkatkan akses yang tanpa batas, dan konektivitas dengan skala yang lebih besar dalam lokal maupun skala global (Das, Tamhane, Vatterott, Wibowo, & Wintels, 2018).

Menurut data GlobalWebIndex (2019), pada Kuartal II 2019 bahwa 90 persen pengguna internet di Indonesia yang berusia antara 16 sampai 64 tahun melaporkan bahwa mereka pernah membeli produk dan layanan *e-commerce* hal ini membuat Indonesia menjadi tingkat pengguna *e-commerce* tertinggi di dunia (GlobalWebIndex, 2019). Berkembangnya *e-commerce* di Indonesia diprediksi bakal menyentuh angka 189,2 juta pada 2023, hal tersebut naik sekitar 25 persen dari tahun 2019 yang sebesar 112,1 juta pengguna (Statista, 2020).

Banyaknya pengguna *e-commerce* di Indonesia yang memanfaatkannya sebagai aktivitas pembelian atau penjualan produk melalui internet, karena pengguna dapat berkomunikasi dengan menyamarkan identitasnya, tanpa dibatasi oleh batas wilayah, dan bahkan lintas negara, sehingga hal tersebut dapat memungkinkan dapat terjadinya ancaman *cybercrime* (Amaliya, 2009). Ancaman terjadinya *cybercrime* merupakan hal serius yang dapat mengganggu aktivitas *e-commerce*. Maka, konsumen maupun pelaku usaha harus dapat melindungi dirinya dari ancaman tersebut dengan *cyber security.*

Cyber security yaitu sebagai mekanisme untuk mendeteksi celah keamanan komputer, mencegah ancaman kejahatan komputer, dan pemulihan kembali komputer atau perangkat yang telah terkena serangan siber (Bishop, 2003). Hal ini sangat dibutuhkan karena telah

berkembangnya penggunaan teknologi internet, khususnya pada *e-commerce* yang rentan terhadap *cybercrime*.

Pada dasarnya, *cyber crime* adalah salah satu bentuk kejahatan yang menargetkan kelemahan dari suatu komputer dengan memanfaatkan internet sebagai teknologi yang digunakan dengan tujuan untuk melakukan jenis kejahatan yang diinginkan pelaku. *Phising* merupakan salah satu jenis *cyber crime* yang sering terjadi pada korban e-commerce dengan cara menjebak korban dengan mengirimkan e-mail atau membuat tampilan *web* palsu yang menyerupai aslinya, sehingga pelaku *(phiser)* mendapatkan data atau informasi rahasia seperti e-mail, password, transaksi atau detail kartu kredit pelaku.

Di Indonesia untuk kasus *cybercrime* dapat dibuktikan oleh temuan Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri yang menerima 4.586 laporan sepanjang Januari-Desember 2019. Laporan soal penipuan online yang terjadi paling mendominasi nomor dua, yakni sebanyak 1.617 kasus (Direktorat Tindak Pidana Siber Bareskrim Polri, 2019). Korban pada *cybercrime* biasanya terjadi pada pengguna atau pelaku *e-commerce* itu sendiri yaitu pembeli dan penjual. Sehingga ini dapat dijadikan catatan penting terkait tingkat kesadaran akan *cyber security* di Indonesia.

Penciptaan malware yang paling berbahaya adalah ketika peretas (individu atau kelompok) membuat program perangkat lunak berbahaya dalam upaya untuk memenuhi tujuan kriminal spesifik demi keuntungan mereka sendiri atau kelompok. Peretas ini menciptakan virus komputer dan program trojan yang dapat mencuri kode akses ke rekening bank, mengiklankan produk atau layanan di komputer korban secara ilegal menggunakan sumber daya komputer yang terinfeksi untuk mengembangkan dan menjalankan kampanye spam, serangan jaringan terdistribusi (juga disebut serangan DDoS), dan pemerasan korban.

Karena banyaknya permasalahan dan kejahatan yang terjadi pada *e-commerce,* peneliti berupaya mencari faktor-faktor apa saja yang mempengaruhi kesadaran *cyber security* pada kalangan pelaku *e-commerce* di Indonesia dengan menyebarkan kuesioner secara daring, kemudian menggunakan metode statistik untuk melakukan analisis dengan teknik *structural equation modeling* (SEM) yang diharapkan mampu memberikan hasil berupa faktor-faktor tersebut.

1.2 Rumusan Masalah

Adapun rumusan masalah yang didapatkan dari latar belakang diatas adalah sebagai berikut:

a. Bagaimana tingkat kesadaran pelaku *e-commerce* di Indonesia dari kacamata *cyber security*?
b. Apa saja faktor-faktor yang mempengaruhi tingkat kesadaran *cyber security* pada kalangan pelaku *e-commerce* di Indonesia?

1.3 Tujuan Penelitian

Adapun tujuan melakukan penelitian ini, antara lain:

a. Untuk mengetahui tingkat kesadaran pelaku *e-commerce* di Indonesia dari kacamata *cyber security*
b. Untuk mengetahui faktor-faktor yang mempengaruhi tingkat kesadaran *cyber security* pada kalangan pelaku *e-commerce* di Indonesia

1.4 Manfaat Penelitian

Hasil penelitian diharapkan dapat memberikan manfaat dan kontribusi bagi pihak-pihak terkait, yaitu:

a. Sebagai bahan edukasi kesadaran bagi masyarakat, dalam melindungi diri dari ancaman kejahatan elektronik dengan *cyber security*.
b. Sebagai bahan kajian/literatur bagi penelitian yang lain untuk mengembangkan penelitian tentang kesadaran *cyber security* pada kalangan pelaku *e-commerce* atau penelitian yang terkait.

1.5 Batasan Masalah

Adapun batasan masalah dalam penelititan ini, yaitu:

a. Penelitian tidak merujuk ke suatu aplikasi e-commerce tertentu.
b. Survei disebarkan secara daring melalui media sosial sehingga ada potensi *sampling* bias.

BAB II
KAJIAN PUSTAKA

21 Electronic Commerce

2.1.1 Definisi *Electronic Commerce*

Definisi *electronic commerce* mendapatkan banyak perhatian dari para sarjana, peneliti dan mahasiswa. Karena banyaknya perbedaan tentang definisi itu sendiri, namun belum ada batasan untuk definisi e-commerce oleh para sarjana, peneliti dan penulis. Bagian ini akan fokus pada beberapa definisi e-commerce dan definisi peneliti tentang e-commerce.

Menurut Vladimir Zwass (1996), *Electronic commerce (E-commerce)* adalah pertukaran informasi dan transaksi bisnis demi mempertahankan hubungan bisnis melalui jaringan internet.

Menurut Roger Clarke, *Electronic Commerce* didefinisikan sebagai pelaksanaan perdagangan barang dan jasa, dengan bantuan alat telekomunikasi dan telekomunikasi.

Menurut Turban (2002), *Electronic Commerce* mempunyai tiga kegiatan utama yaitu: pemesanan dan pembayaran, pemenuhan pesanan, dan pengiriman ke pelanggan dengan menggunakan jaringan internet. Setiap kegiatan yang dilakukan dapat berupa fisik atau digital.

Menurut Dr. Anil Khurana mendefinisikan *Electronic Commerce* sebagai penggunaan komputer, internet dan perangkat lunak untuk mengirim dan menerima spesifikasi dan gambar produk; tawaran, pesanan pembelian, dan faktur; dan segala jenis data lain yang perlu dikomunikasikan kepada pelanggan, pemasok, karyawan, atau publik.

Dari beberapa definisi *Electronic Commerce* diatas, peneliti dapat menyimpulkan bahwa *e-commerce* merupakan suatu aktivitas yang menggunakan internet dan komputer atau perangkat genggam sebagai komponen utama. Dengan tujuan melakukan tawaran produk, transaksi jual-beli, hingga produk sampai ke tangan pembeli demi mempertahankan hubungan bisnis.

2.1.2 Jenis-Jenis *Electronic Commerce*

Turban (2002) mengatakan *E-commerce* diklasifikasikan berdasarkan jenis transaksi dan skala transaksi tersebut. Jenis-jenis utama dari *e-commerce* tersebut, yaitu:

a. Business-to-Business (B2B)

B2B adalah transaksi antar perusahaan, yang termasuk perdagangan grosir serta pembelian jasa perusahaan, sumber daya, teknologi, suku cadang dan komponen yang

diproduksi, dan peralatan modal. Ini juga mencakup beberapa jenis transaksi keuangan antara perusahaan, seperti asuransi, kredit komersial, obligasi, sekuritas, dan aset keuangan lainnya. Skala transaksinya sendiri, biasa sangat besar karena melibatkan beberapa perusahaan.

b. Consumer-to-Consumer (C2C)

Sebuah transaksi jual-beli yang melibatkan antara perseorangan dalam lingkup online. Jika kita ingin menjual sesuatu, yang harus dilakukan adalah memposting produk atau jasa di situs, memberikan detail produk dan harga, dan menunggu pelanggan yang berminat untuk membelinya. Pembeli menghubungi penjual melalui Internet dan kesepakatan berhasil ketika produk atau jasa sampai ke pembeli. Contoh implementasinya yaitu iklan baris atau lelang barang. C2C mengalami peningkatan karena sistem jualnya yang lebih mudah.

c. Business-to-Customer (B2C)

Setiap bisnis atau organisasi yang menjual produk atau jasa kepada konsumen melalui internet untuk konsumen. Ini memungkinkan konsumen untuk menelusuri katalog produk, memilih produk atau jasa dan menyelesaikan pesanan secara online. Selain retailer online, B2C telah berkembang untuk memasukkan layanan seperti perbankan online, layanan perjalanan, lelang online, informasi kesehatan dan situs perumahaan.

d. Business-to-Business-to-Consumer (B2B2C)

Dalam business-to-business-to-consumer (B2B2C), ketika perusahaan (B1) menjual produk ke perusahaan lain (B2). B2 kemudian menjual, atau memberikan, produk kepada individu yang mungkin adalah pelanggan atau karyawan B2 sendiri.

e. Consumer-to-Business E-commerce (C2B)

Ketika orang menggunakan Internet untuk menjual produk atau layanan kepada individu dan organisasi. Atau, individu menggunakan C2B untuk menawar produk atau layanan. Contohnya yaitu situs penjualan tiket traveloka.com

2.2 Cyber Security

2.2.1 Konsep *Cyber Security*

Faktor yang mempengaruhi kualitas layanan e-commerce yaitu keamanan. Kata kunci (password), kunci enkripsi, ser*tifikasi*, atau tanda tangan digital adalah cara untuk memberikan rasa nyaman dan aman dalam bertransaksi. Selain itu, seorang pengguna harus diberikan akses penuh untuk menjaga informasi dan data yang dipunya, sehingga individu dapat mengatur *e-commerce* pada aplikasinya (Park & Kim, 2006)

Menurut Bruce (1996), mengamankan komputer merupakan hal yang sangat vital untuk menjaga kerahasiaan informasi atau data yang ada pada komputer. Dalam melindungi komputer harus meliputi beberapa aspek keamanan, antara lain:

a. Confidentiality

Dalam menjaga kerahasiaan komputer harus mampu melindungi data atau informasi dengan sebuah kata sandi yang telah disandikan.

b. Authentication

Penerima pesan (komputer) harus memastikan bahwa seseorang yang melakukan pengambilan data atau informasi merupakan miliknya, bukanlah seorang yang menyamar untuk menyusup atau mencuri data atau informasi tersebut. Sehingga untuk memastikannya, perlu dilakukan autentifikasi keaslian, data, dan sebagainya.

c. Integrity

Perlindungan dari bentuk usaha untuk mengubah data secara tidak sah. Untuk menjaganya, sistem harus mampu mengenali dari usaha manipulasi data atau informasi dari pihak-pihak yang tidak bertanggung jawab, antara lain penghapusan, penyisipan, pendistribusian data lain ke data yang asli.

d. Non Repudiation

Dalam pengiriman data atau informasi, pengirim seharusnya tidak dapat menyangkal bahwa individu yang mengirim, begitu juga sebaliknya.

2.2.2 Kategori Cyber Security

Cyber Security merupakan praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari ancaman yang juga dikenal sebagai keamanan teknologi informasi. Istilah ini berlaku dalam berbagai konteks, dari bisnis ke komputasi *mobile*, dan dapat dibagi menjadi beberapa kategori umum, yaitu:

a. *Network security* adalah praktik mengamankan jaringan komputer dari penyusup, baik penyerang yang ditargetkan atau *malware*.
b. *Application Security* berfokus pada menjaga perangkat lunak dan perangkat bebas dari ancaman. Aplikasi yang dikompromikan dapat memberikan akses ke data yang dirancang untuk dilindungi. Keamanan yang berhasil dimulai pada tahap desain, jauh sebelum program atau perangkat digunakan.
c. *Information security* melindungi integritas dan privasi data, baik dalam penyimpanan maupun dalam perjalanan.

d. *Operational security* mencakup proses dan keputusan untuk menangani dan melindungi aset data. Izin yang dimiliki pengguna saat mengakses jaringan dan prosedur yang menentukan bagaimana dan di mana data dapat disimpan atau dibagikan semuanya termasuk dalam cakupan ini.
e. *Disaster recovery and business continuity* menentukan bagaimana organisasi merespons insiden keamanan cyber atau peristiwa lain apa pun yang menyebabkan hilangnya operasi atau data. Kebijakan *disaster recovery* menentukan bagaimana organisasi mengembalikan operasi dan informasinya untuk kembali ke kapasitas operasi yang seperti sebelumnya. *business continuity* adalah rencana ketika sebuah organisasi tersebut jatuh pada saat mencoba untuk beroperasi tanpa sumber daya tertentu.
f. *End-user education* membahas faktor keamanan cyber yang paling tidak dapat diprediksi: orang. Siapa pun dapat secara tidak sengaja memperkenalkan virus ke sistem yang dinyatakan aman dengan tidak mengikuti praktik keamanan yang benar. Mengajarkan pengguna untuk menghapus lampiran email yang mencurigakan, tidak mencolokkan drive USB yang tidak dikenal, dan berbagai pelajaran penting lainnya yang sangat penting untuk keamanan organisasi mana pun.

2.2.3 Ancaman Terhadap *Cyber Security*

Ketika pencipta malware yang paling berbahaya adalah saat peretas dan kelompok peretas membuat program perangkat lunak berbahaya dalam upaya untuk memenuhi tujuan kriminal spesifik demi keuntungan mereka sendiri atau organisasi. Penjahat dunia maya ini menciptakan virus komputer dan program Trojan yang dapat mencuri kode akses ke rekening bank, mengiklankan produk atau layanan di komputer korban secara ilegal menggunakan sumber daya komputer yang terinfeksi untuk mengembangkan dan menjalankan kampanye spam, serangan jaringan terdistribusi (juga disebut serangan DDoS), dan pemerasan korban.

Menurut situs kaspersky, ancaman yang dilawan oleh *Cyber Security* ada tiga, adalah:

a. *Cybercrime* termasuk aktor tunggal atau kelompok yang menargetkan sistem untuk keuntungan finansial atau menyebabkan gangguan.
b. *Cyber attack* seringkali melibatkan pengumpulan informasi yang bermotivasi penyerangan secara politik.
c. *Cyberterror* yang dimaksudkan untuk melemahkan sistem elektronik yang menyebabkan kepanikan atau ketakutan.

Metode umum yang digunakan penyerang untuk mengontrol komputer atau jaringan termasuk virus, worm, spyware, trojans, dan ransomware. Virus dan worm dapat mereplikasi diri sendiri dan merusak file atau sistem, sementara spyware dan Trojans sering digunakan untuk pengumpulan data secara sembunyi-sembunyi. Ransomware menunggu kesempatan untuk mengenkripsi semua informasi pengguna dan menuntut pembayaran untuk mengembalikan akses ke pengguna. Kode berbahaya sering menyebar melalui lampiran email yang tidak diminta atau unduhan yang tampak sah yang sebenarnya membawa muatan malware.

Ancaman *cyber security* memengaruhi semua industri, apapun ukurannya. Industri yang melaporkan serangan cyber paling banyak dalam beberapa tahun terakhir adalah layanan kesehatan, manufaktur, keuangan, dan pemerintah. Beberapa sektor ini lebih menarik bagi penjahat dunia maya karena mereka mengumpulkan data keuangan dan medis, tetapi semua bisnis yang menggunakan jaringan dapat ditargetkan untuk data pelanggan, spionase perusahaan, atau serangan pelanggan.

2.3 Kesadaran dan Pengetahuan *Cyber Security*

Kesadaran *cyber security* adalah tingkat pemahaman pengguna tentang pentingnya menjaga keamanan informasi dan tanggung jawab mereka serta melakukan kontol terhadap keamanan informasi yang memadai demi melindungi data dan jaringan (Shaw, Chen, Harris, & Huang, 2009). Individu harus peduli terhadap segala akses dan keamanan, karena demi menjaga *e-commerce* dari berbagai ancaman seperti peretas (*hacker),* pencurian *password* atau nomor kartu kredit, atau menghindari kegagalan sistem.

Karena Individu atau pelaku *e-commerce* dengan pengetahuan *cyber security* yang baik, akan lebih sadar *cyber security* karena individu mampu mengetahui jenis kejahatan yang biasanya terjadi pada *e-commerce*. Selain itu, individu juga mampu mengetahui kriteria untuk jenis *password* yang kuat dan aman. Yang lebih menarik, individu mampu mengetahui dalam hal melindungi diri dari ancaman yang berkaitan dengan transaksi (Rhee, Kim, & Ryu, 2009). Berdasarkan uraian diatas, berikut hipotesis penelitian:

H1: Pengetahuan *cyber security e-commerce* memiliki pengaruh signifikan terhadap kesadaran *cyber security e-commerce*

24 Faktor Demografi

Menurut Kamus Besar Bahasa Indonesia pengertian demografi merupakan ilmu tentang suatu populasi berdasarkan faktor usia, ras, agama dan jenis kelamin. Data demografi mengacu pada informasi sosial-ekonomi yang dinyatakan secara statistik, juga termasuk pekerjaan, pendidikan, pendapatan, tingkat perkawinan, tingkat kelahiran, kematian, dan lain-lain. Pemerintah, perusahaan, dan penelitian menggunakan demografi untuk mempelajari lebih lanjut tentang karakteristik populasi untuk banyak tujuan, termasuk mencari tahu pengetahuan individu melalui karakteristik demografi.

Salah satu bagian penting dari studi demografi yaitu komposisi penduduk. Lebih dari itu, demografi memiliki karateristik yang kemudian dikelompokkan di bawah ini:

a. Karakteristik demografi, yakni umur, jumlah wanita subur, jenis kelamin, dan jumlah anak.
b. Karakteristik sosial adalah status perkawinan dan tingkat pendidikan.
c. Karakteristik ekonomi, antara lain pendapatan per bulan, status pekerjaan, lapangan pekerjaan, sektor pekerjaan, dan kegiatan penduduk yang aktif secara ekonomi,

Faktor demografi ini terdiri dari berbagai unsur yang dipengaruhi oleh lingkungan sosialnya. Peneliti coba mengambil beberapa aspek demografi yang akan dijadikan sebagai faktor terhadap pengaruh pengetahuan *cyber security*.

a. Usia

Lamanya waktu seorang individu hidup yaitu terhitung sejak lahir sampai dengan sekarang. Usia terbagi menjadi dua jenis yaitu usia biologis dan usia mental. Usia biologis adalah proses biologis di mana manusia mengalami dan mencapai tahap pematangan biologis. Usia biologis dapat dilihat sebagai proses biologis yang relatif objektif di mana seseorang menjadi lebih tua dan memahami perkembangan biologis ketika mencapai usia tertentu. Usia mental adalah tingkat kemampuan individu, biasanya sebagaimana ditentukan oleh tes kecerdasan dan kontrol emosi. Berdasarkan hal tersebut peneliti mengembangkan hipotesis:

H2: Usia memiliki pengaruh signifikan terhadap pengetahuan *cyber security e-commerce*

b. Jenis Kelamin

Jenis kelamin adalah kondisi fisik biologis dari dua jenis manusia, yakni laki-laki dan perempuan dan merupakan bawaan dari lahir sehingga melekat pada manusia. Jenis kelamin merupakan pemberian dari Tuhan yang tidak bisa kita hindarkan. Berdasarkan hal tersebut peneliti mengembangkan hipotesis:

H3: Jenis kelamin memiliki pengaruh signifikan terhadap pengetahuan *cyber security e-commerce*

c. Pendidikan

Tingkat pendidikan adalah suatu kondisi ketika individu telah menjalani pendidikan secara formal yang dipakai pemerintah. Di Indonesia ada tiga jenjang pendidikan yakni tingkat dasar dari SD hingga SMP, sedang yaitu SMA, dan perguruan tinggi. Berdasarkan hal tersebut peneliti mengembangkan hipotesis:

H4: Pendidikan terakhir memiliki pengaruh signifikan terhadap pengetahuan *cyber security e-commerce*

d. Pendapatan

Pendapatan adalah jumlah semua pendapatan individu yang diwujudkan dalam bentuk uang dan barang. Berdasarkan hal tersebut peneliti mengembangkan hipotesis:

H5: Pendapatan rendah memiliki pengaruh signifikan terhadap pengetahuan *cyber security e-commerce*

H6: Pendapatan tinggi memiliki pengaruh signifikan terhadap pengetahuan *cyber security e-commerce*

e. Sektor Pekerjaan

Menurut Soekidjo (2003) pekerjaan merupakan cara bertahan hidup yang dilakukan manusia untuk memperoleh pendapatan. Berdasarkan hal tersebut peneliti mengembangkan hipotesis:

H7: Sektor pekerjaan memiliki pengaruh signifikan terhadap pengetahuan *cyber security e-commerce*

f. Domisili

Kitab Undang-Undang Hukum Perdata mengatakan bahwa domisili merupakan tempat yang dijadikan tempat tinggal untuk hidup sebagai kediamannya. Sedangkan menurut Kamus Besar Bahasa Indonesia pengertian domisili adalah tempat tinggal yang legal dari seseorang atau tempat tinggal resmi. Sementara daerah asal adalah merupakan tempat kelahiran dari suatu individu. Berdasarkan hal tersebut peneliti mengembangkan hipotesis:

H8: Domisili memiliki pengaruh signifikan terhadap pengetahuan *cyber security e-commerce*

H9: Daerah asal memiliki pengaruh signifikan terhadap pengetahuan *cyber security e-commerce*

25 *Exploratory Factor Analysis* (EFA)

Dalam statistik multivariat, exploratory factor analysis (EFA) adalah metode statistik yang digunakan untuk membentuk faktor dari variabel yang banyak. EFA adalah teknik analisis dalam analisis faktor yang bertujuan untuk mengidentifikasi hubungan yang mendasari antar variabel tersebut (Norris & Lecavalier, 2009). Pada umumnya EFA digunakan oleh para peneliti ketika mengembangkan variabel (variabel adalah kumpulan pertanyaan yang digunakan untuk mengukur topik penelitian tertentu) dan berfungsi untuk mengidentifikasi serangkaian variabel latenyang didasari oleh sejumlah variabel. Ketika peneliti tidak memiliki hipotesis tentang faktor atau pola dari variabel yang diukur, maka pemilihan EFA sangat tepat (Finch & West, 1997). Variabel terukur adalah atribut dari seseorang yang dapat diamati dan diukur. Contoh variabel yang diukur dapat berupa tinggi fisik, berat badan, dan denyut nadi manusia. Para peneliti biasanya memiliki jumlah variabel terukur yang besar, kemudian diasumsikan terkait dengan sejumlah kecil faktor "tidak teramati". Peneliti harus berhati-hati dalam mempertimbangkan jumlah variabel yang ingin diukur untuk dimasukkan ke dalam analisis (Finch & West, 1997). Analisis akan lebih akurat ketika masing-masing faktor telah terwakilkan oleh beberapa variabel terukur dalam analisis.

EFA didasarkan pada model faktor umum (Norris & Lecavalier, 2009). Dalam model ini, variabel manifes dinyatakan sebagai fungsi dari faktor umum, faktor unik, dan kesalahan pengukuran. Setiap faktor unik hanya memengaruhi satu variabel manifes dan tidak menjelaskan korelasi antara variabel manifes. Faktor-faktor umum mempengaruhi lebih dari satu variabel manifes dan "*factor loadings*" adalah nilai yang diukur dalam pengaruh faktor umum pada variabel manifes. Untuk prosedur EFA, kami lebih tertarik untuk mengidentifikasi faktor-faktor umum dan variabel manifes terkait.

Pada saat melakukan analisis, EFA akan mengasumsikan bahwa indikator/variabel yang diukur dapat dikaitkan dengan faktor apa pun. Saat mengembangkan hipotesis, peneliti harus menggunakan EFA terlebih dahulu sebelum melakukan *Confirmatory Factor Analysis* (CFA) (Worthington & Whittaker, 2006). EFA sangat penting untuk menentukan faktor/konstruksi yang mendasari serangkaian variabel yang diukur; sementara CFA memungkinkan peneliti untuk menguji hipotesis bahwa ada hubungan antara variabel yang diamati dan variabel laten. EFA mengharuskan peneliti untuk membuat sejumlah keputusan penting tentang bagaimana melakukan analisis atau hiptesis karena tidak ada metode yang ditetapkan.

2.6 *Structural Equation Modeling* (SEM)

2.6.1 Konsep SEM

Structural Equation Modeling disingkat SEM merupakan teknik analisis statistik multivariat yang digunakan untuk menganalisis hubungan struktural. Teknik ini adalah kombinasi dari analisis faktor konfirmatori, analisis jalur, analisis regresi berganda. SEM biasanya digunakan untuk menganalisis hubungan struktural antara variabel yang diukur dan variabel laten. Metode ini lebih disukai oleh peneliti karena menutupi keterbatasan yang ada pada model analisis sebelumnya yang sudah secara luas digunakan, selain itu analisis dapat saling terkait dalam melakukan analisis tunggal. Pada analisis ini, dua jenis variabel yang digunakan adalah variabel endogen dan variabel eksogen. Variabel endogen setara dengan variabel dependen dan variabel independen. (Prihandini & Sunaryo, 2011).

Menurut Ghozali (2008), SEM merupakan model persamaan struktural teknik analisis multivariat yang dapat menguji hubungan kompleks antar variabel secara *recursive dan non-recursive* hingg peneliti mendapatkan seluruh hasil mengenai suatu model. Tidak seperti analisis multivariate biasa (regresi berganda dan analisis faktor). SEM dapat melakukan pengujian secara bersama-sama SEM dapat melakukan analisis pengujian dengan bersamaan yang tidak bisa dilakukan analisis multivariate biasa (analisis faktor dan analisis regresi berganda) yaitu: model struktural yang mengukur model structural antara hubungan variabel independen dengan variabel dependen, serta perhitungan model yang mengukur hubungan antara variabel indikator dengan variabel laten. Dengan digabungkannya pengujian model struktural dan pengukuran tersebut memungkinkan peneliti untuk menguji kesalahan pengukuran (*measurement error*) sebagai bagian yang tak terpisahkan dari *structural equation model* dan melakukan analisis faktor bersamaan dengan pengujian hipotesis (Bollen, 1989).

Dengan demikian SEM adalah salah satu teknik analisis multivariat yang digunakan untuk menganalisis hubungan antar variabel yang lebih kompleks dibandingkan dengan analisis regresi berganda dan analisis faktor. Menurut Mustika (2014) berikut ini adalah konsep dan istilah-istilah yang terdapat dalam SEM:

a. Model jalur adalah penggambaran yang dilakukan dengan mengunakan diagram, dalam diagram terdapat hubungan antara, variabel perantara, variabel bebas, dan variabel terikat. Untuk menggambarkan hubungan antar variabel disimbolkan dengan anak panah. Hubungan kausalitas yang terjadi antar variabel disimbolkan dengan anak panah tunggal. Sedangkan untuk menunjukkan interalasi antar variabel digunakan anak panah ganda.

b. Variabel eksogen merupakan variabel yang faktor eksternal yang mempengaruhinya, pada diagram tidak ada anak panah yang menuju variabel tersebut.
c. Variabel endogen adalah variable yang memiliki anak panah yang menuju langsung ke variabel tersebut. Variabel yang termasuk diantaranya adalah variabel perantara dan variabel terikat.
d. Variabel laten merupakan variabel yang tidak dapat diukur secara langsung. Pada umumnya variabel ini akan diukur terlebih dahulu manifesnya. Dalam variabel laten dibagi menjadi 2, yaitu:
    11. Variabel laten eksogen adalah variabel bebas yang mempengaruhi variabel terikat,
    12. Variabel laten endogen adalah variabel terikat yang dipengaruhi oleh variabel bebas
e. Variabel manifest adalah variabel yang mengukur atau menentukan jumlah variabel laten. Dalam beberapa variabel manifest memiliki satu variabel laten.
f. Koefisien regresi standar atau koefisien jalur, atau biasa disebut dengan beta (β) variabel terikat, biasanya menunjukkan pengaruh secara langsung dalam beberapa model jalur tertentu.
g. Analisis faktor penegasan merupakan analisis factor yang didapat dari sebuah teknik keberlanjutan dimana pengujian hipotesis *factor loadings* dan interkorelari dilakukan.

2.6.2 Karakteristik SEM

Menurut Ghozali dan Fuad (2008), karakteristik dari SEM *(Structural Equation Modeling)* sebagai berikut:

a. SEM adalah teknik analisis data multivariate interdependensi dan depensi yang dikombinasikan, yakni analisis jalur dan *Confirmatory Factor Analysis* (CFA).
b. Variabel laten adalah variabel yang dianalisis, namu tidak dapat dilakukan analisis secara langsung, sehingga harus diukur melalui indikator-indikator atau variabel manifest.
c. Menghasilkan model bukanlah tujuan dari SEM. Tetapi SEM mengkonfirmasi model berdasarkan teori, yakni *structural model* dan *measurement model*.

BAB III
METODOLOGI PENELITIAN

3.1 Jenis Penelitian

Penelitian dilakukan dengan menggunakan jenis penelitian deskriptif dengan pendekatan kuantitatif. Menurut Sugiyono (2016) penelitian deskriptif adalah penelitian yang dilakukan untuk mengetahui hubungan antara dua variabel atau lebih. Pada penelitian ini, penelitian deskriptif digunakan untuk menjelaskan tentang pengaruh pengetahuan *cyber security* dan demografi terhadap kesadaran *cyber security* para pelaku *e-commerce* di Indonesia.

Pendekatan kuantitatif digunakan untuk mendapatkan informasi dari populasi atau sampel tertentu dengan melakukan analisis data menggunakan alat statistik dan instrumen penelitian sebagai alat pengumpulan data, dengan tujuan untuk melakukan pengujian terhadap hipotesis yang telah ditentukan (Sugiyono, 2016).

3.2 Definisi Operasional Variabel

Variabel penelitian adalah kumpulan sesuatu yang dapat berbentuk apa saja dan ditetapkan oleh peneliti untuk memperoleh suatu informasi, kemudian informasi akan digunakan untuk ditarik kesimpulannya (Sugiyono, 2016). Pada penelitian ini menggunakan dua variabel yaitu variabel dependen (terikat) dan variabel independen (bebas). Berikut penjelasan dari masing-masing variabel adalah sebagai berikut:

3.2.1 Variabel Dependen

Variabel dependen adalah variabel terikat yang dipengaruhi oleh variabel bebas. Dalam penelitian ini, variabel terikat yang digunakan yaitu kesadaran *cyber security* (Ksd). Kesadaran merupakan keadaan sadar akan sesuatu yang secara langsung mengetahui, memahami, dan menyadari peristiwa yang membuatnya harus melakukan sesuatu (Chalmers, 1997). Berikut definisi operasional variabel kesadaran *cyber security* pada tabel di bawah ini:

Tabel 3.1 Tabel Definisi Operasional Variabel Kesadaran

Variabel	Simbol	Indikator	Jenis Data
Kesadaran *cyber security*	K_1	Saya sadar untuk mengabaikan email yang mengandung *phising*	Ordinal
	K_2	Saya sadar untuk melindungi diri dari *cybercrime*	Ordinal

	K_3	Saya sadar untuk mengantisipasi dari kejahatan *carding*	Ordinal
	K_4	Saya sadar untuk tidak memberikan informasi pribadi (e-mail, username, password)	Ordinal
	K_5	Saya sadar *Two-Factor Authentication* (2FA) berguna melindungi akun dari pembobolan	Ordinal
	K_6	Saya sadar untuk melindungi dari *phising, cybercrime, social engineering*	Ordinal
	K_7	Saya sadar untuk mengakses situs *e-commerce* yang menggunakan HTTPS/SSL	Ordinal
	K_8	Saya sadar untuk menjaga kartu debit atau kredit dari pencurian	Ordinal
	K_9	Saya sadar untuk menggunakan *password* yang kuat	Ordinal
	K_10	Saya sadar untuk menggunakan *password* yang unik	Ordinal
	K_11	Saya sadar untuk menyimpan *password* pada platform yang aman	Ordinal
	K_12	Saya sadar untuk menggunakan *e-commerce* saat menggunakan jaringan publik	Ordinal
	K_13	Saya sadar untuk menyimpan data transaksi *e-commerce* dengan baik	Ordinal
	K_14	Saya sadar untuk mengakses akun bank pada saat menggunakan jaringan publik	Ordinal

3.2.2 Variabel Independen

Variabel independen merupakan variabel bebas yang mempengaruhi variabel dependen atau terikat secara positif atau negatif. Variabel independen yang digunakan dalam penelitian ini adalah demografi dan pengetahuan *cyber security* (Png).

Data demografi merupakan komponen sosial yang berhubungan dengan individu yang mempengaruhi tingkah laku dan pola pikir dari individu. Adapun definisi operasional variabel demografi akan dijelaskan pada tabel di bawah ini:

Tabel 3.2 Tabel Definisi Operasional Variabel Demografi

Variabel	Simbol	Indikator	Jenis Data
Usia	Umr	Umur	Rasio
Jenis kelamin	Sex	Pria	Nominal
		Wanita	
Pendidikan terakhir	pnd	Pendidikan tinggi (DIII, S1, S2, S3)	Ordinal
		Pendidikan menengah (SD, SMP)	
Pendapatan rendah	P_r	Pendapatan rendah (dibawah Rp.5 juta/bulan)	Nominal
Pendapatan tinggi	P_t	Pendapatan tinggi (diatas Rp.5 juta/bulan)	Nominal
Sektor pekerjaan	Sk_	Bekerja	Nominal
		Tidak bekerja	
Domisili	Dms	Jawa	Nominal
		Luar Jawa	
Daerah asal	Dsl_	Jawa	Nominal
		Luar Jawa	

Pengetahuan merupakan kumpulan satu informasi yang individu dapatkan dari suatu pengalaman atau sejak lahir, sehingga membuat individu menjadi tahu akan sesuatu (Reber & Reber, 2010). Berikut definisi operasiona variabel pengetahuan *cyber security* yang digunakan adalah sebagai berikut:

Tabel 3.3 Tabel Definisi Operasional Variabel Pengetahuan

Variabel	Simbol	Indikator	Jenis Data
Pengetahuan *cyber security*	P_1	Saya tahu apa itu *phising*	Ordinal
	P_2	Saya tahu apa itu *cybercrime*	Ordinal
	P_3	Saya tahu apa itu *Carding*	Ordinal
	P_4	Saya tahu apa itu *social engineering*	Ordinal
	P_5	Saya tahu apa itu *two-factor authentication*	Ordinal
	P_6	Saya tahu bagaimana melindungi dari *phising*, *cyber*crime, dan *social engineering*	Ordinal
	P_7	Saya tahu situs *e-commerce* yang aman	Ordinal

	P_8	Saya tahu jika kartu debit dan kredit bisa dicuri	Ordinal
	P_9	Saya tahu bagaimana *password* yang kuat	Ordinal
	P_10	Saya tahu bagaimana *password* yang unik	Ordinal
	P_11	Saya tahu untuk menyimpan *password* baik secara fisik maupun digital	Ordinal
	P_12	Saya tahu kerentanan melakukan transaksi pada jaringan publik	Ordinal
	P_13	Saya tahu untuk tidak menyimpan data transaksi	Ordinal
	P_14	Saya tahu untuk tidak mengakses akun bank pada saat menggunakan jaringan publik	Ordinal

3.3 Populasi dan Sampel

Menurut Sugiyono (2016) populasi adalah obyek atau subjek wilayah secara umum yang memiliki kualitas dan karakteristik tertentu yang akan dipelajri oleh peneliti untuk menarik kesimpulan. Pada penelitian ini populasinya adalah pengguna *e-commerce* di Indonesia.

Sampel merupakan keseluruhan objek yang diteliti dan merupakan bagian dari populasi yang dianggap mewakili kesuluruhan populasi (Sugiyono, 2016). Metode dari pemilihan sampel untuk penelitian ini adalah *non probability sampling*, yakni teknik pengambilan sampel dengan tidak memberikan peluang yang sama untuk menjadi sampel bagi tiap populasi. Metode pengambilan sampel menggunakan *purposive sampling* berdasarkan kriteria yang ditentukan oleh peneliti, yakni individu yang pernah menggunakan *e-commerce* dan berusia minimal 13 tahun.

Penentuan jumlah sampel pada penelitian ini, menggunakan *margin of error* 5% dan tingkat *confidence level* 95% dengan data populasi pengguna *e-commerce* di Indonesia 122 juta maka jumlah sampel yang rekomendasikan adalah 384 sampel.

3.4 Teknik Pengumpulan Data

Sumber data yang digunakan pada penelitian ini menggunakan data primer yang diperoleh secara langsung oleh peneliti dengan cara menyebarkan kuesioner. Kuesioner merupakan teknik pengumpulan yakni memberikan daftar pertanyaan atau pernyataan kepada responden untuk dijawabnya secara langsung (Sugiyono, 2016). Kuesioner dirancang agar bisa

menjawab kesadaran *cyber security* dengan dengan tipe pernyataan atau pertanyaan positif, sehingga responden tinggal memilih jawaban yang telah diberikan. Untuk pilihan jawaban yang diajukan menggunakan skala likert. Menurut Sugiyono (2016) skala likert digunakan sebagai alat ukur persepsi, sikap, dan pendapat seseorang atau kelompok terhadap fenomena social. Berikut skala likert yang digunakan pada penelitian ini:

Tabel 3.4 Skala Likert Kuesioner

No	Keterangan	Skor
1	Sangat setuju	5
2	Setuju	4
3	Netral	3
4	Tidak setuju	2
5	Sangat tidak setuju	1

3.5 Hasil Uji Instrumen Penelitian

Data kuesioner yang dimiliki peneliti terlebih dahulu dilakukan pengujian untuk melihat keakuratan dan ketepatan dari data penelitian yang dimiliki sebelum melakukan suatu analisis. Untuk dapat mengukur sejauh mana ketepatan dalam mengumpulkan data peneliti menggunakan uji validitas dan untuk menilai tingkat konsistensi dari mengumpulkan data yang dilakukan peneliti menggunakan uji reliabilitas.

3.5.1 Uji Validitas

Dilakukan uji validitas agar konsep penelitian benar-benar dapat diukur secara akurat, memberikan hasil data yang memiliki kaitan erat, dan menjalankan peran dari indikator seperti yang diinginkan (Heale & Alison, 2015)

Uji validitas penelitian ini menggunakan metode *bivariate pearson* yaitu melakukan perbandingan hasil *degree of freedom* (df) dan nilai pada r tabel. Indikator pada variabel dikatakan valid apabila nilai r tabel kurang dari nilai *degree of freedom* (df) yang bernilai positif (Sugiyono, 2016). Pada penelitian ini terdiri dari 383 responden dengan 28 variabel, sehingga r tabel untuk signifikansi 5% dengan n=383 adalah 0,098. Berikut tabel hasil pengujian validitas:

Tabel 3.5 Hasil Uji Validitas

Variabel	Indikator	r Hitung n=383	r Tabel	Hasil
Pengetahuan *cyber security* (Png)	P_1	0,692	0,098	valid
	P_2	0,639	0,098	valid

	P_3	0,634	0,098	valid
	P_4	0,658	0,098	valid
	P_5	0,617	0,098	valid
	P_6	0,734	0,098	valid
	P_7	0,714	0,098	valid
	P_8	0,595	0,098	valid
	P_9	0,756	0,098	valid
	P_10	0,725	0,098	valid
	P_11	0,554	0,098	valid
	P_12	0,702	0,098	valid
	P_13	0,488	0,098	valid
	P_14	0,652	0,098	valid
Kesadaran *cyber security* (Ksd)	K_1	0,657	0,098	valid
	K_2	0,793	0,098	valid
	K_3	0,787	0,098	valid
	K_4	0,681	0,098	valid
	K_5	0,610	0,098	valid
	K_6	0,776	0,098	valid
	K_7	0,712	0,098	valid
	K_8	0,757	0,098	valid
	K_9	0,795	0,098	valid
	K_10	0,697	0,098	valid
	K_11	0,746	0,098	valid
	K_12	0,448	0,098	valid
	K_13	0,637	0,098	valid
	K_14	0,330	0,098	valid

Berdasarkan hasil uji validitas pada Tabel 3.5 terhadap 383 responden, 28 indikator penelitian memiliki nilai diatas r tabel yaitu 0,098 sehingga data dapat dikatakan valid

3.5.2 Uji Reliabilitas

Uji reliabilitas merupakan berkaitan dengan seberapa konsisten alat ukur pada penelitian sehingga alat ukur tersebut dapat dipercaya dan dipergunakan (Heale & Alison, 2015).

Untuk menguji reliabilitas data dilakukan dengan membandingkan nilai Cronbach Alpha 28 indikator penelitian dari 383 responden. Standar batas *cronbach's alpha* untuk indikator

yang akan digunakan penelitian ini yaitu > 0,70 (George & Mallery, 2003). Berikut hasil pengujian pada tabel berikut:

Tabel 3.6 Hasil Uji Reliabilitas

Variabel	***Cronbach's Alpha***	**Standar *Cronbach Alpha's***	**Hasil**
Pengetahuan *cyber security* (Png)	0,91	0,70	Reliabel
Kesadaran *cyber security* (Ksd)	0,92	0,70	Reliabel

Setelah dilakukan pengujian pada Tabel 3.6, didapatkan hasil uji reliabilitas *cronbach's alpha* pada masing-masing variabel dengan nilai diatas dari 0,70 maka semua pernyataan pada penelitian ini dinyatakan reliabel.

3.6 Teknik Analisis Data

Dalam memahami suatu bentuk data, maka diperlukan penyederhaan dengan melakukan analisis. Tujuannya adalah agar data dapat dibaca dengan mudah dan dipahami. Untuk mendapat hasil analisis yang akurat tentang hasil hipotesis, maka peneliti memilih metode kuantitatif sehingga data yang berbentuk angka tersebut diolah dengan menggunakan metode statistik. Analisis data menggunakan program Rstudio.

3.6.1 Analisis Faktor

Metode analisis faktor yang digunakan adalah *Exploratory Factor Analysis* (EFA). EFA digunakan peneliti untuk menilai hubungan antara variabel indikator dan mereduksi data kedalam satu kelompok atau beberapa kelompok tanpa mengurangi informasi dari kumpulan data tersebut (Supranto, 2004).

Pemilihan analisis EFA dikarenakan peneliti dihadapkan pada kondisi tidak memiliki informasi awal atau hipotesis terkait data yang aka diolah, sehingga peneliti harus mengelompokkan indikator yang dibentuk kedalam beberapa variabel laten.

Pada awalnya dilakukan identifikasi kecukupan data dengan uji *Kaiser-Mayer-Olkin* (KMO), *Measure of Sampling Adequacy* (MSA) dan Bartlett's dengan syarat nilai MSA dan KMO lebih dari 0,5 (Widarjono, 2010). Kemudian, analisis faktor dilakukan dengan melihat *factor loadings* dari setiap item yang diamati memiliki nilai cut-off lebih dari 0,3 dan tidak

memiliki efek cross-loading. Jika telah memenuhi kriteria tersebut, direkomendasikan untuk melakukan analisis lebih lanjut (Hair Jr, Black, Babin, & Anderson, 2009).

3.6.2 Analisis Deskriptif

Analisis deskriptif merupakan analisis yang berdasarkan jawaban kuesioner yang diberikan kepada responden untuk menggambarkan karakteristik responden itu sendiri seperti jenis kelamin, usia, pekerjaan, pendidikan terakhir, pendapatan, daerah asal, domisili, dan pengetahuan *cyber security*.

3.6.3 Analisis Structural Equation Modeling

Metode analisis data yang digunakan dalam penelitian ini adalah *Structural Equation Modeling* (SEM). SEM merupakan teknik statistik yang memungkinkan serangkaian hubungan antara satu atau lebih variabel independen (IV) dan satu atau lebih variabel dependen (DV), baik kontinu maupun diskrit, yang kemudian dianalisis. Baik IV maupun DV dapat menjadi faktor atau variabel yang diukur. *Structural Equation Modeling* (SEM) juga disebut sebagai pemodelan kausal, analisis kausal, pemodelan persamaan simultan, analisis struktur kovarian, analisis jalur, atau analisis faktor konfirmatori (Ullman & Bentler, 2003). Dalam melakukan analisis SEM terdapat tujuh tahap dalam permodelan SEM menurut Ghozali (2011) yaitu:

a. Spesifikasi model

Langkah ini merupakan suatu kegiatan untuk mengembangkan suatu model terhadap rumusan masalah pada penelitian, sehingga untuk mendukung hubungan antar variabel-variabel, maka harus berdasarkan landasan teori yang kuat dan model yang jelas.

b. Identifikasi model

Tahap ini merupakan langkah yang penting untuk mengidentifikasi suatu model, jika model tidak dapat diidentifikasi, maka model tersebut tidak dapat dilakukan perhitungan atau mengestimasi suatu model. Identifikasi model dilakukan dengan cara menghitung nilai *degree of freedom (df)*. Jika df pada model bernilai lebih dari 0 atau positif, maka model dapat dilakukan perhitungan atau estimasi model.

c. Estimasi model

Estimasi model dilakukan setelah menentukan estimasi model pada tahap identifikasi model. Estimasi model yang biasa digunakan adalah *maximum likelihood* (ML).

d. Evaluasi model

Setelah estimasi dilakukan, maka langkah selanjutnya adalah mengevaluasi model dan melakukan interpretasi terhadap hasil. Tahap ini bertujuan untuk mengevaluasi model secara

keseluruhan. Untuk melakukan tingkat kecocokan model antara variabel dengan data, maka dilakukan dengan menilai 'fit' model secara keseluruhan dengan kriteria *Goodness of Fit* (GOF). Uraian di bawah akan menjelaskan bagaiaman menilai kriteria GOF*:*

1. CMIN/DF

   Merupakan indikator untuk menilai tingkat kesesuain model. CMIN/DF merupakan hasil bagi antara chi-square dibagi dengan *degree of* freedom (df). Ukuran yang menyatakan fit adalah nilai ratio < 5,0 (Wheaton, Muthen, Alwin, & Summers, 1977)

2. SRMR (*Standardized Root Mean Square Residual*)

   SRMR adalah ukuran kecocokan absolut dan didefinisikan sebagai perbedaan standar antara korelasi yang diamati dan korelasi yang diprediksi.

3. RMSEA (*The Root Mean Square Error of Approximation*)

   Root mean square error of approximation (RMSEA) yaitu indeks kecocokan absolut, karena menilai sejauh mana model yang dihipotesiskan dengan model yang sempurna. Nilai RMSEA yang biasanya digunakan adalah 0,05-0,08 sehingga dapat dikatakan *good fit* (MacCallum, Browne, & Sugawara, 1996).

4. CFI (*Comparative Fit Index*)

   CFI adalah indikator untuk menganalisis model fit dengan memeriksa perbedaan antara data dan model yang dihipotesiskan, sambil menyesuaikan untuk masalah ukuran sampel yang melekat dalam uji chi-squared model fit sehingga direkomendasikan nilai untuk CFI adalah > 0,80 (Hu & Bentler, 1999).

5. TLI (*Tucker Lewis Index*)

   TLI merupakan indikator *incremental fit index* yaitu dengan menguji *baseline model* dengan model yang diuji. Nilai TLI dikatakan fit apabila memiliki nilai > 0,80 (Marsh, Balla, & McDonald, 1988).

e. Modifikasi model

Modifikasi model merupakan langkah selanjutnya setelah melakukan uji kecocokan. Model dilakukan modifikasi jika hasil uji kecocokan dirasa belum 'fit', sehingga dilakukan modifikasi model agar mendapatkan hasil uji yang diinginkan.

3.7 Pengujian Hipotesis

Pengujian hipotesis yang dilakukan adalah menjawab rumusan masalah pada penelitian ini. Untuk melihat apakah hipotesis diterima atau tidak, yakni dengan melihat nilai probabilitas (p) kurang dari ≤0,05 (Chandio, 2011). Langkah-langkah pengujiannya sebagai berikut:

a. Menentukan hipotesis:

   H0: bi = 0, artinya variabel independen tidak memiliki pengaruh signifikan dengan variabel dependen

   H1: bi ≠ 0, artinya variabel independen memiliki pengaruh signifikan terhadap variabel dependen

b. Menentukan *Level of Significant* (α) 5%, degree of freedom (df) = n – 2 (dengan n = jumlah responden) dan pengujian dua sisi, maka pada penentuan t-tabel menggunakan α/2.

c. Kriteria pengujian:

   1. H0 gagal tolak bila: t hitung ≤ t-tabel
   2. H0 ditolak bila: t hitung > t-tabel
   3. Probabilitas ≥ *Level of Significant* = 0,05. Maka H0 gagal tolak, H1 ditolak
   4. Probabilitas < *Level of Significant* = 0,05. Maka H0 ditolak, H1 gagal tolak

d. Melakukan perhitungan sesuai dengan pendekatan (alat) statistika yang dipergunakan yaitu dengan menggunakan program Rstudio.

e. Pengambilan kesimpulan t-hitung dengan *Level of Significant* untuk menentukan H1 dan H0 diterima atau tidak.

BAB IV
ANALISIS DATA DAN PEMBAHASAN

41 Analisis Faktor

4.1.1 Faktorisasi Pengetahuan *Cyber Security*

Peneliti akan melakukan reduksi variabel pengetahuan *cyber security*. Hasil faktorisasi dari analisis EFA kemudian digunakan peneliti untuk uji lanjut. Langkah pertama untuk analisis EFA adalah pengecekan layak tidaknya kumpulan data yang digunakan dalam penelitian ini untuk dilakukan faktorisasi, menggunakan uji *Kaiser-Mayer-Olkin* (KMO), *Measure of Sampling Adequacy* (MSA) dan *Bartlett's*. Hasil uji KMO dan Bartlett's untuk data pengetahuan umum sebagai berikut:

Gambar 4.1 Uji KMO dan Bartlett's Pengetahuan

```
> uji_bart(pengetahuan) ##uji Bartlett's

        Bartlett's test of sphericity

data:  pengetahuan
Khi-squared = 2867, df = 91, p-value < 2.2e-16

> kmo(pengetahuan) ## Uji KMO
$KMO
[1] 0.9119781
```

Pada Gambar 4.1 diperoleh KMO = 0,91 dengan tingkat signifikan 0,05, maka gagal tolak $\square_o$ karena KMO(0,91)>$\square$(0,05), dengan menggunakan tingkat kepercayaan 95% dapat disimpulkan sebagai jumlah data yang dimiliki telah cukup untuk difaktorkan. Selanjutnya peneliti melakukan uji Bartlett's, uji ini digunakan untuk mengetahui apakah ada hubungan antar variabel dalam kasus multivariat.. Berdasarkan hasil pada Gambar 1 diperoleh nilai p-*value* atau nilai *sig* adalah 0,000. Maka tolak $\square_o$ karena p-*value* (0,000) < $\square$(0,05), sehingga dengan tingkat kepercayaan 95% maka dapat disimpulkan analisis multivariat layak digunakan analisis EFA untuk data pengetahuan umum ini. Selanjutnya peneliti melakukan pengecekan MSA (Tabel 4.1) untuk melihat variabel mana saja yang dapat digunakan dalam penelitian ini. Jika nilai MSA ≥0,5 maka variabel tersebut dapat digunakan dalam analisis ini.

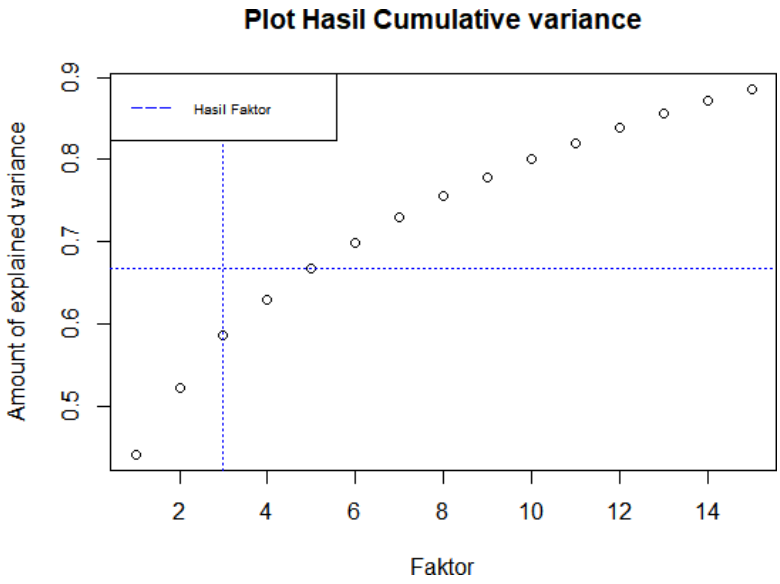
Tabel 4.1 Hasil MSA 383 Variabel Pengetahuan

No	Variabel	MSA	Hasil
1	Pengetahuan_1	0,90791	Signifikan
2	Pengetahuan_2	0,953283	Signifikan

No	Variabel	MSA	Hasil
3	Pengetahuan_3	0,911543	Signifikan
4	Pengetahuan_4	0,928158	Signifikan
5	Pengetahuan_5	0,968155	Signifikan
6	Pengetahuan_6	0,889329	Signifikan
7	Pengetahuan_7	0,949857	Signifikan
8	Pengetahuan_8	0,94364	Signifikan
9	Pengetahuan_9	0,848548	Signifikan
10	Pengetahuan_10	0,843734	Signifikan
11	Pengetahuan_11	0,960996	Signifikan
12	Pengetahuan_12	0,906052	Signifikan
13	Pengetahuan_13	0,943472	Signifikan
14	Pengetahuan_14	0,91508	Signifikan

Hasil Tabel 4.1 Hasil MSA 383 Variabel Pengetahuan menunjukan dari 14 variabel yang diuji keseluruhan signifikan, maka setelah diketahui, data tersebut cukup untuk diimplementasikan dan layak digunakan maka selanjutnya peneliti melakukan reduksi 14 variabel. Kemudian peneliti menentukan jumlah faktor yang merepresentasikan dari masing-masing item dengan menggunakan screeplot. Berikut hasil screeplot tersebut.

Gambar 4.2 Screeplot Variabel Pengetahuan



Hasil pada Gambar 4.2 menunjukan pola atau faktor yang cocok untuk data penelitian ini adalah nfaktor=3 sehingga peneliti kemudian mereduksi 14 variabel kedalam 3 faktor menggunakan EFA. Hasil analisis EFA dengan tiga faktor sebagai berikut.

Tabel 4.2 Hasil Faktorisasi Variabel Pengetahuan

Variabel	***Loadings Factor 1***	***Loadings Factor 2***	***Loadings Factor 3***
Pengetahuan_1	**0,734**	0,234	0,164
Pengetahuan_2	0,360	**0,400**	0,366
Pengetahuan_3	**0,747**	0,143	0,155
Pengetahuan_4	**0,594**	0,168	0,324
Pengetahuan_5	**0,487**	0,267	0,245
Pengetahuan_6	**0,835**	0,184	0,205
Pengetahuan_7	**0,592**	0,300	0,310
Pengetahuan_8	0,244	0,398	**0,423**
Pengetahuan_9	0,249	**0,861**	0,279
Pengetahuan_10	0,235	**0,841**	0,260
Pengetahuan_11	0,223	**0,471**	0,323
Pengetahuan_12	0,169	0,409	**0,734**
Pengetahuan_13	0,315	0,146	**0,421**
Pengetahuan_14	0,281	0,257	**0,611**
SS loadings	**3,299**	**2,542**	**2,007**
proportion	**0,236**	**0,182**	**0,143**

Dari tabel Tabel 4.2 diatas dapat dilihat faktor yang terbentuk beserta *item-item* pembentuk dan nilai *factor loadings*-nya. *Factor loadings* merupakan hasil yang terbentuk karena terdapat korelasi antar item dengan faktor. Jika dilihat dari Tabel 4.2 nilai *loadings* masing-masing faktor sudah memenuhi nilai minimum yang disarankan yaitu 0,3 (Hair Jr, Black, Babin, & Anderson, 2009). Berikut hasil dan penamaan faktor-faktor yang terbentuk:

Tabel 4.3 Hasil Faktorisasi yang Terbentuk

Faktor 1 (P_1)	
P_1	Saya tahu apa itu *phising*
P_3	Saya tahu apa itu *Carding*
P_4	Saya tahu apa itu *social engineering*
P_5	Saya tahu apa itu *two-factor authentication*

P_6	Saya tahu bagaimana melindungi dari *phising*, *cyber*crime, dan *social engineering*
P_7	Saya tahu situs *e-commerce* yang aman
Faktor 2 (P_2)	
P_9	Saya tahu bagaimana *password* yang kuat
P_10	Saya tahu bagaimana *password* yang unik
P_11	Saya tahu untuk menyimpan *password* baik secara fisik maupun digital
P_2	Saya tahu apa itu *cybercrime*
Faktor 3 (P_3)	
P_8	Saya tahu jika kartu debit dan kredit bisa dicuri
P_12	Saya tahu kerentanan melakukan transaksi pada jaringan publik
P_13	Saya tahu untuk tidak menyimpan data transaksi
P_14	Saya tahu untuk tidak mengakses akun bank pada saat menggunakan jaringan publik

Hasil faktorisasi pada Tabel 4.6 selanjutnya akan digunakan sebagai variabel laten pada analisis kuantitatif *Structural Equation Modeling* (SEM). Pada P_1 merupakan representasi dari pengetahuan umun tentang keamanan, P_2 merupakan representasi dari pengetahuan akan keamanan password, dan P_3 adalah representasi dari pengetahuan akan risiko transaksi e-commerce

4.1.2 Faktorisasi Kesadaran *Cyber Security*

Selanjutnya peneliti melakukan faktorisasi pada data kesadaran umum, dengan banyak responden adalah 383 dan 14 variabel. Hasil uji KMO dan Bartlett's untuk data kesadaran umum sebagai beriut:

```
> uji_bart(Kesadaran_umum) ##uji Bartlett's

        Bartlett's test of sphericity

data:  Kesadaran_umum
Khi-squared = 3436.9, df = 91, p-value < 2.2e-16

> kmo(Kesadaran_umum) ## Uji KMO
$KMO
[1] 0.9200175
```

Gambar 4.3 Uji KMO dan Bartlett's Kesadaran

Pada Gambar 4.3 diperoleh KMO = 0,92 dengan tingkat signifikan 0,05, maka gagal tolak $\square_o$ karena KMO(0,92)>$\square$(0,05), dengan menggunakan tingkat kepercayaan 95% dapat disimpulkan sebagai jumlah data yang dimiliki telah cukup untuk difaktorkan. Selanjutnya

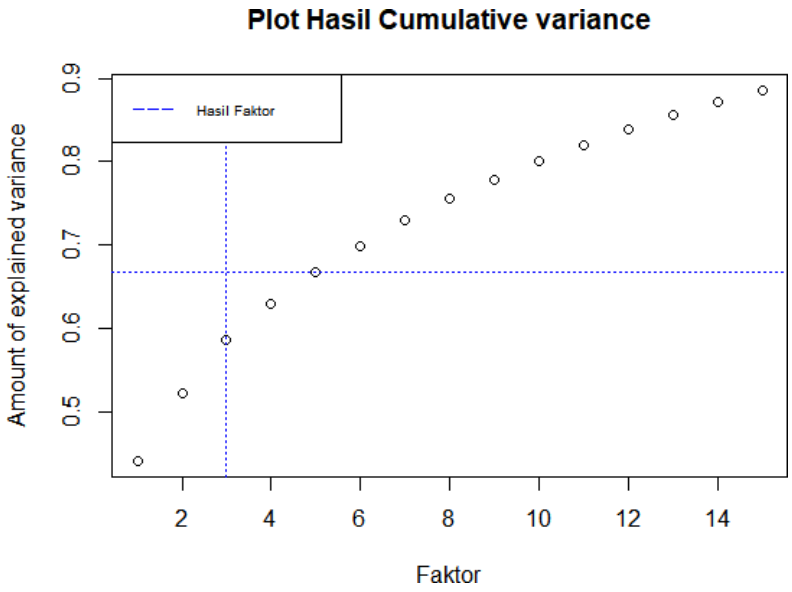
peneliti melakukan uji Bartlett's, uji ini digunakan untuk mengetahui apakah ada hubungan antar variabel dalam kasus multivariat. Berdasarkan hasil pada Gambar 4.3 diperoleh nilai p-*value* atau nilai *sig* adalah 0,000. Maka tolak $\square_o$ karena p-*value* (0,000) < $\square$(0,05), sehingga dengan tingkat kepercayaan 95% maka dapat disimpulkan analisis multivariat layak digunakan analisis EFA untuk data kesadaran umum ini. Selanjutnya peneliti melakukan pengecekan MSA (Tabel 6) untuk melihat variabel mana saja yang dapat digunakan dalam penelitian ini. Jika nilai MSA ≥0,5 maka variabel tersebut dapat digunakan dalam analisis ini.

Tabel 4.4 Hasil MSA 383 Variabel Kesadaran

No	Variabel	MSA	Hasil
1	kesadaran_umum_1	0,94523	Signifikan
2	kesadaran_umum_2	0,931214	Signifikan
3	kesadaran_umum_3	0,938917	Signifikan
4	kesadaran_umum_4	0,922209	Signifikan
5	kesadaran_umum_5	0,936293	Signifikan
6	kesadaran_umum_6	0,919614	Signifikan
7	kesadaran_umum_7	0,921465	Signifikan
8	kesadaran_umum_8	0,955013	Signifikan
9	kesadaran_umum_9	0,90582	Signifikan
10	kesadaran_umum_10	0,929232	Signifikan
11	kesadaran_umum_11	0,966856	Signifikan
12	kesadaran_umum_12	0,775051	Signifikan
13	kesadaran_umum_13	0,961736	Signifikan
14	kesadaran_umum_14	0,708886	Signifikan

Hasil Tabel 4.4 menunjukan dari 14 variabel yang diuji keseluruhan signifikan, maka setelah diketahui, data tersebut cukup untuk diimplementasikan dan layak digunakan maka selanjutnya peneliti melakukan reduksi 14 variabel. Kemudian peneliti menentukan jumlah faktor yang merepresentasikan dari masing-masing item dengan menggunakan screeplot. Berikut hasil screeplot tersebut.

Gambar 4.4 Screeplot Variabel Kesadaran



Hasil pada Gambar 4.4 menunjukan pola atau faktor yang cocok untuk data penelitian ini adalah nfaktor=3 sehingga peneliti kemudian mereduksi 14 variabel kedalam 3 faktor menggunakan EFA. Hasil analisis EFA dengan tiga faktor sebagai berikut.

Tabel 4.5 Hasil Faktorisasi Variabel Kesadaran

Variabel	***Loadings Factor 1***	***Loadings Factor 2***	***Loadings Factor 3***
Kesadaran_1	0,270	**0,662**	0,106
Kesadaran _2	0,585	**0,592**	0,047
Kesadaran _3	0,424	**0,671**	0,146
Kesadaran _4	**0,663**	0,388	0,035
Kesadaran _5	0,379	**0,425**	0,162
Kesadaran _6	0,325	**0,792**	0,105
Kesadaran _7	0,300	**0,674**	0,242
Kesadaran _8	**0,678**	0,434	0,140
Kesadaran _9	**0,879**	0,317	0,160
Kesadaran _10	**0,689**	0,270	0,176
Kesadaran _11	**0,490**	0,475	0,241
Kesadaran _12	0,125	0,191	**0,787**
Kesadaran _13	0,431	0,362	**0,431**
Kesadaran _14	0,087	0,053	**0,884**

SS loadings	**3,530**	**3,416**	**1,853**
proportion	**0,252**	**0,244**	**0,132**

Dari Tabel 4.5 diatas dapat dilihat faktor yang terbentuk beserta *item-item* pembentuk dan nilai *factor loadings*-nya. *Factor loadings* merupakan hasil yang terbentuk karena terdapat korelasi antar item dengan faktor. Jika dilihat dari Tabel 4.5 nilai *loadings* masing-masing faktor sudah memenuhi nilai minimum yang disarankan yaitu 0,3 (Hair Jr, Black, Babin, & Anderson, 2009). Berikut hasil dan penamaan faktor-faktor yang terbentuk:

Tabel 4.6 Hasil Faktorisasi yang Terbentuk

Faktor 1 (K_1)	
K_1	Saya sadar untuk mengabaikan email yang mengandung *phising*
K_2	Saya sadar untuk melindungi diri dari *cybercrime*
K_3	Saya sadar untuk mengantisipasi dari kejahatan *carding*
K_5	Saya sadar *Two-Factor Authentication* (2FA) berguna melindungi akun dari pembobolan
K_6	Saya sadar untuk melindungi dari *phising*, *cybercrime*, *social engineering*
K_7	Saya sadar untuk mengakses situs *e-commerce* yang menggunakan HTTPS/SSL
Faktor 2 (K_2)	
K_4	Saya sadar untuk tidak memberikan informasi pribadi (e-mail, username, password)
K_8	Saya sadar untuk menjaga kartu debit atau kredit dari pencurian
K_9	Saya sadar untuk menggunakan *password* yang kuat
K_10	Saya sadar untuk menggunakan *password* yang unik
K_11	Saya sadar untuk menyimpan *password* pada platform yang aman
Faktor 3 (K_3)	
K_12	Saya sadar untuk menggunakan *e-commerce* saat menggunakan jaringan publik
K_13	Saya sadar untuk menyimpan data transaksi *e-commerce* dengan baik
K_14	Saya sadar untuk mengakses akun bank pada saat menggunakan jaringan publik

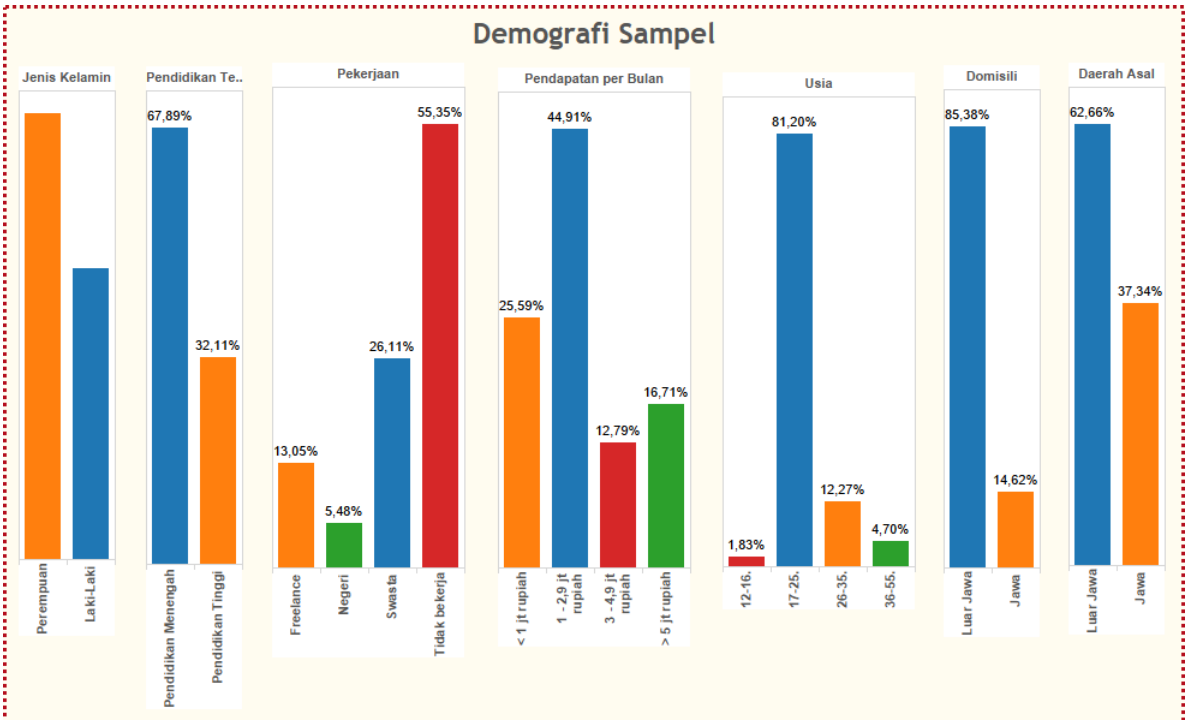
Hasil faktorisasi pada Tabel 4.6 selanjutnya akan digunakan sebagai variabel laten pada analisis kuantitatif *Structural Equation Modeling* (SEM).). Pada K_1 merupakan representasi dari kesadaran untuk menjaga diri dari segala jenis kejahatan siber, K_2 merupakan representasi dari kesadaran untuk menjaga diri dari pencurian dan kata sandi, dan K_3 adalah representasi dari kesadaran untuk menjaga diri saat melakukan transaksi e-commerce.

4.2 Analisis Deskriptif

4.2.1 Analisis Karateristik Responden

Setelah melakukan penyebaran kuesioner ke berbagai media sosial, maka terkumpul sebanyak 383 responden untuk dianalisis. Berikut gambar yang menampilkan kumpulan karateristik dari responden:

Gambar 4.5 Rincian Demografi Sampel



Sampel merupakan data pengisi kuisioner yang terdiri dari 383 responden pelaku *e-commerce*, serta variabel demografi yang berjumlah tujuh variabel yaitu jenis kelamin, pendidikan terakhir, pekerjaan, penghasilan, usia, domisili, dan daerah asal. Dapat dilihat dari grafik diatas, pada variabel jenis kelamin terlihat bahwa jumlah sampel perempuan lebih banyak daripada laki-laki yaitu sebanyak 60,57% sedangkan laki-laki sebanyak 39,43%.

Selanjutnya beralih ke variabel pendidikan terakhir. Pendidikan dikategorikan menjadi dua yaitu pendidikan menengah dan pendidikan tinggi. Sampel tertinggi adalah orang-orang yang memiliki pendidikan menengah yaitu sebesar 67,89% sedangkan pendidikan tinggi sebesar 32,11%.

Selanjutnya adalah variabel kategori pekerjaan. Terdapat empat kategori yaitu swasta, *freelance* atau pekerja lepas, pegawai negeri, dan tidak bekerja. Untuk presentasenya tertingginya adalah kategori tidak bekerja sebanyak 55,35%, swasta sebanyak 26,11%, *freelance* sebanyak 13,05%, dan pegawai negeri sebanyak 5,48%.

Selanjutnya adalah variabel selanjutnya yaitu adalah pendapatan perbulan. Pendapatan perbulan digolongkan menjadi empat yaitu kurang dari 1 juta, 1 – 2,9 juta, 3 – 4,9 juta, dan lebih dari 5 juta. Presentasenya berturut-turut adalah 29,59%, 44,91%, 16,71%, dan 12,79%. Untuk sampel terbanyak adalah orang-orang dengan pendapatan 1- 2,9 juta. Sampel yang memiliki pendapatan tertinggi adalah sebanyak 12,79% dan yang memiliki pendapatan terendah adalah sebesar 29,59%.

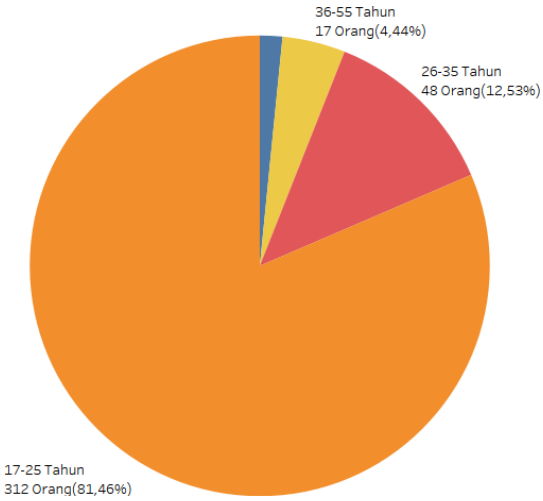
Selanjutnya adalah variabel usia. Mayoritas sampel berusia 17 – 25 tahun dengan presentase sebesar 81,20%, selanjutnya terbanyak kedua, ketiga, keempat, dan kelima secara berturut-turut adalah sebagai berikut: usia 26 – 35 tahun sebesar 12,27%, usia 36 – 55 tahun sebesar 4,70%, dan usia 12 – 16 tahun sebesar 1,83%.

Selanjutnya adalah variabel domisili atau tempat tinggal. Variabel ini dikategorikan menjadi dua yaitu Jawa dan luar Jawa. Dari sampel yang ada, sampel terbanyak adalah orang-orang yang berdomisili di luar Jawa yaitu sebanyak 85,38% sedangkan yang berdomisili di Jawa hanya sebesar 14,62%. Kemudian variabel terakhir adalah variabel daerah asal. Variabel ini juga dibagi menjadi dua yaitu Jawa dan luar Jawa. Untuk variabel daerah asal, mayoritas sampel adalah orang-orang yang berasal dari luar Jawa yaitu sebanyak 62,66% sedangkan untuk orang yang berasal dari Jawa sebanyak 37,34%.

4.2.1.1 Usia Responden

Persentase responden menurut usia dapat dilihat pada gambar sebagai berikut:

Gambar 4.6 Responden Menurut Usia

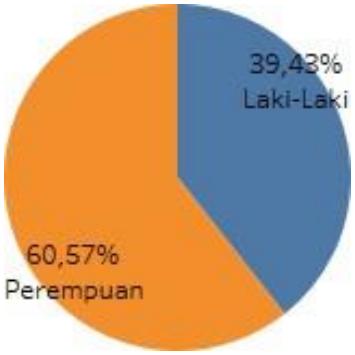


Pada Gambar 4.6 dapat dilihat sebagian besar usia responden dalam penelitian ini adalah 17-25 tahun dengan jumlah responden 312 orang atau memiliki persentase sebesar 81,46 persen, sedangkan responden 26-35 tahun berjumlah 48 orang atau 12,53 persen. Kemudian, sebagian kecil responden berusia 36-55 tahun dengan jumlah 17 orang atau 4,44 persen dan 13-16 tahun berjumlah 6 orang dengan persentase 1,57 persen.

4.2.1.2 Jenis Kelamin Responden

Berikut persentase jenis kelamin responden dapat dilihat pada gambar sebagai berikut:

Gambar 4.7 Responden Menurut Jenis Kelamin

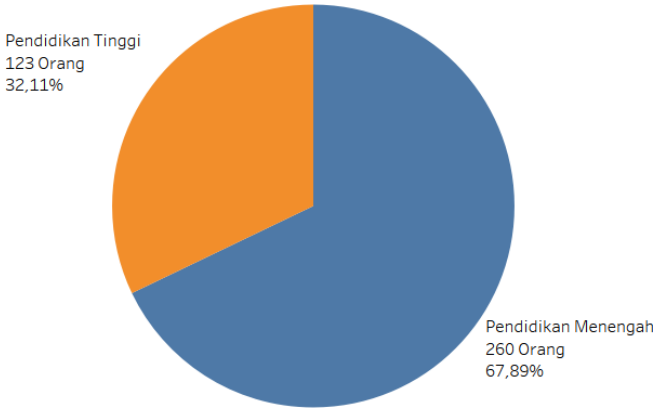


Berdasarkan Gambar 4.7 menunjukkan bahwa sebagian besar responden dalam penelitian ini adalah perempuan dengan jumlah responden 232 orang atau memiliki persentase sebesar 60,57 persen, sedangkan responden laki-laki berjumlah 151 orang atau 39,43 persen.

4.2.1.3 Pendidikan Terakhir Responden

Berikut persentase pendidikan terakhir responden dapat dilihat pada gambar sebagai berikut

Gambar 4.8 Responden Menurut Pendidikan Terakhir

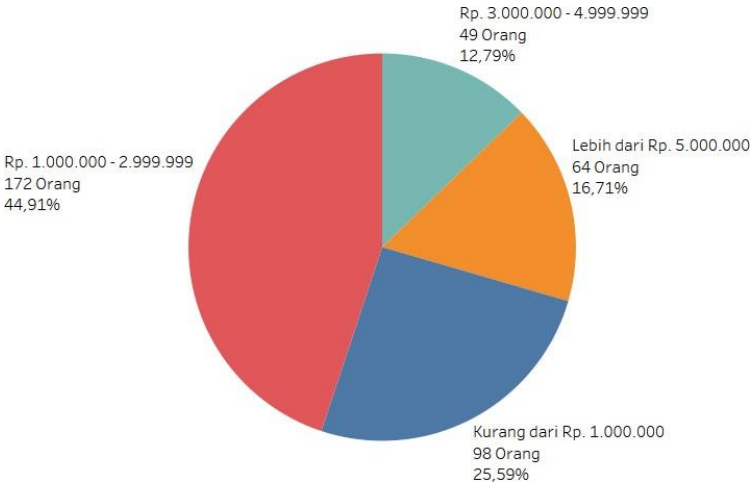


Pada Gambar 4.8 bisa dilihat dalam penelitian ini banyak pendidikan terakhir dari responden adalah pendidikan menengah dengan jumlah responden 260 orang atau memiliki persentase sebesar 67,89 persen, sedangkan responden pendidikan tinggi berjumlah 123 orang atau 32,11 persen.

4.2.1.4 Pendapatan Bulanan Responden

Berikut persentase pendapatan bulanan responden dapat dilihat pada gambar sebagai berikut:

Gambar 4.9 Responden Menurut Pendapatan per Bulan

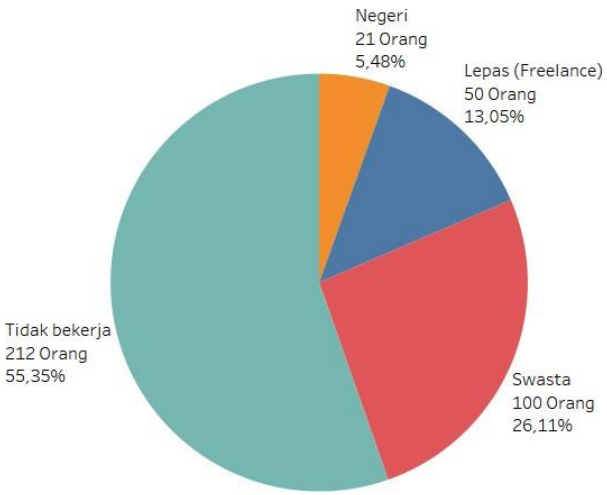


Berdasarkan Gambar 4.9 menunjukkan bahwa sebagian besar pendapatan bulanan responden dalam penelitian ini adalah 1–2,9 juta dengan jumlah responden 172 orang atau memiliki persentase sebesar 44,91 persen, selanjutnya responden dengan pendapatan bulanan dibawah 1 juta berjumlah 98 orang atau 25,59 persen. Kemudian, responden dengan pendapatan diatas 5 juta berjumlah 64 orang atau 16,71 persen dan responden dengan pendapatan 3-4,9 juta berjumlah 49 orang atau 12,79 persen.

4.2.1.5 Sektor Pekerjaan Responden

Berikut persentase sektor pekerjaan responden dalam penelitian dapat dilihat pada gambar di bawah ini:

Gambar 4.10 Responden Menurut Sektor Pekerjaan

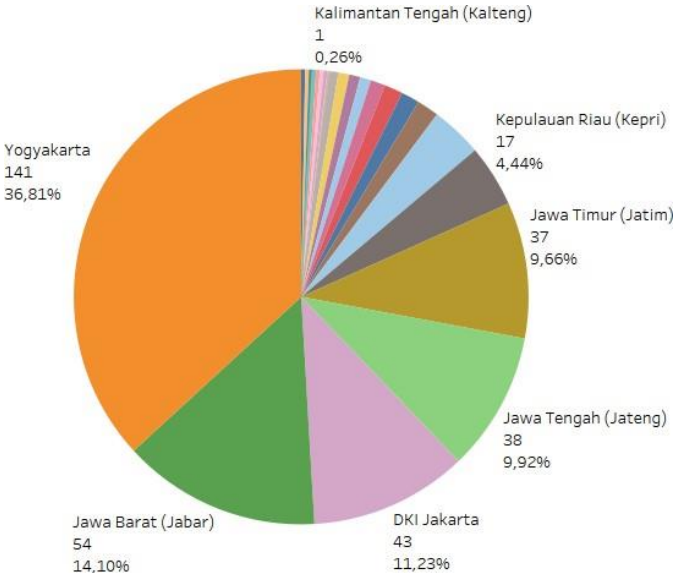


Berdasarkan Gambar 4.10 sebagian besar dari responden adalah tidak bekerja dengan jumlah responden 212 orang atau memiliki persentase sebesar 55,35 persen, selanjutnya responden pada sektor swasta berjumlah 100 orang atau 26,11 persen. Kemudian, sektor pekerja lepas dengan jumlah responden 50 orang atau memiliki persentase sebesar 13,05 persen dan sektor negeri berjumlah 21 orang atau 5,48 persen.

4.2.1.6 Domisili dan Daerah Asal Responden

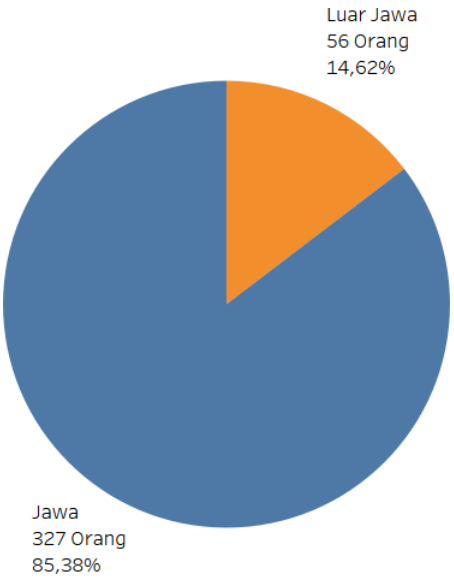
Berikut persentase domisili dan daerah asal responden dapat dilihat pada gambar sebagai berikut:

Gambar 4.11 Responden Menurut Domisili



Setelah melakukan penyebaran kuesioner berdasarkan Gambar 4.11 didapatkan total provinsi dari 383 responden yaitu 23 provinsi dengan mayoritas responden berdomisili Yogyakarta, Jawa Barat, DKI Jakarta, Jawa Tengah, dan Jawa Timur dengan total mayoritas 81,72 persen karena keberagaman itu, maka peneliti melakukan kategorisasi menjadi Jawad dan luar Jawa (Sumatera, Kalimantan, Sulawesi, dll). Berikut hasil kategorisasi domisili pada gambar berikut:

Gambar 4.12 Kategorisasi Domisili

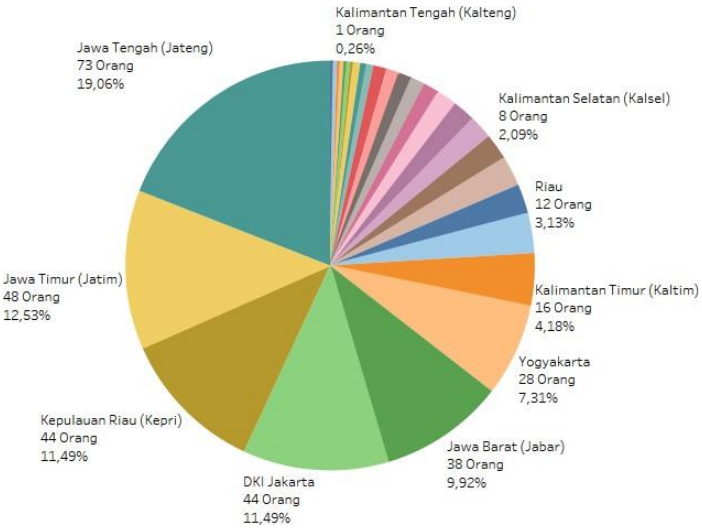


Berdasarkan Gambar 4.12 menunjukkan bahwa sebagian besar responden dalam penelitian ini adalah berdomisili di Jawa dengan jumlah responden 327 orang atau memiliki

persentase sebesar 85,38 persen, selanjutnya responden dengan domisili luar Jawa berjumlah 56 orang atau 14,62 persen.

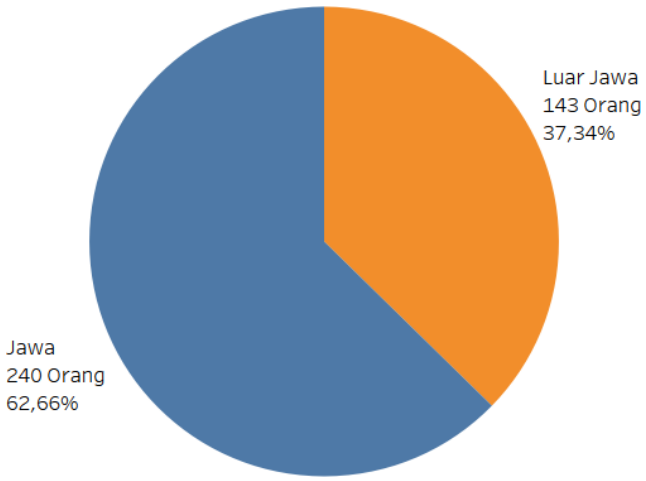
Persentase responden menurut daerah asal dapat dilihat pada tabel sebagai berikut:

Gambar 4.13 Responden Menurut Daerah Asal



Setelah melakukan penyebaran kuesioner berdasarkan Gambar 4.13 didapatkan total provinsi dari 383 responden yaitu 29 provinsi dengan mayoritas responden berasal dari provinsi Jawa Tengah, Jawa Timur, Kepulauan Riau, DKI Jakarta dan Jawa Barat dengan total mayoritas provinsi berasal dari Jawa dengan persentase 60,73 persen karena keberagaman itu, maka peneliti melakukan kategorisasi menjadi Jawa dan luar Jawa (Sumatera, Kalimantan, Sulawesi, dll). Berikut hasil kategorisasi domisili pada gambar berikut:

Gambar 4.14 Kategorisasi Daerah Asal



Berdasarkan Gambar 4.14 menunjukkan bahwa sebagian besar responden dalam penelitian ini adalah daerah asal dari Jawa dengan jumlah responden 240 orang atau memiliki

persentase sebesar 62,66 persen, selanjutnya responden dengan daerah asal luar Jawa berjumlah 143 orang atau 37,34 persen.

4.2.2 Analisis Deskriptif Variabel Penelitian

Dalam analisis deskriptif variabel penelitian ini akan menejelaskan tentang seberapa tinggi tingkat penilaian responden terhadap variabel pengetahuan *cyber security* dan kesadaran *cyber security*. Berdasarkan jawaban didapatkan dari responden, maka dilakukan perhitungan agar dapat melakukan analisis deskriptif dari jawaban yang diberikan responden. Penilaian ini dilakukan atas dasar sebagai berikut:

Skor penilaian terendah adalah 1

Skor penilaian tertinggi adalah 5

$$\text{Interval} = \frac{5-1}{5} = 0{,}8 \qquad (4.1)$$

Berdasarkan rumus diatas maka dilakukan penetuan batasan penilaian terhadap masing masing variabel penelitian, berikut penilaian tersebut:

1,00 - 1,8 = sangat tidak setuju

1,81 - 2,60 = tidak setuju

2,61 - 3,41 = netral

3,42 - 4,22 = setuju

4,23 - 5,00 = sangat setuju

4.2.2.1 Analisis Deskriptif Pengetahuan Kejahatan (P_1)

Dari kumpulan pertanyaan yang diberikan kepada responden dapat dijelaskan distribusi penilaian responden terhadap pengetahuan umum tentang keamanan (P_1). Berikut tabel distribusi:

Tabel 4.7 Hasil Analisis Deskriptif Pengetahuan Kejahatan

Item	Indikator	Rata-rata	Keterangan
P_1	Saya tahu apa itu *phising*	3,25	Netral
P_3	Saya tahu apa itu *Carding*	3,06	Netral
P_4	Saya tahu apa itu *social engineering*	3,34	Netral
P_5	Saya tahu apa itu *two-factor authentication*	3,60	Setuju

P_6	Saya tahu bagaimana melindungi dari *phising*, *cyber*crime, dan *social engineering*	2,99	Netral
P_7	Saya tahu situs *e-commerce* yang aman	3,34	Netral
Rata-rata		3,23	Netral

Dari tabel diatas, dapat dilihat hasil distribusi rata-rata bahwa tingkat pengetahuan umum tentang keamanan (P_1) adalah netral. Artinya, pelaku *e-commerce* masih belum sepenuhnya tahu tentang pengetahuan umum keamanan.

4.2.2.2 Analisis Deskriptif Pengetahuan Password (P_2)

Dari kumpulan pertanyaan yang diberikan kepada responden dapat dijelaskan distribusi penilaian responden terhadap pengetahuan tentang mengamankan password (P_2). Berikut tabel distribusi:

Tabel 4.8 Hasil Analisis Deskriptif Pengetahuan *Password*

Item	Indikator	Rata-rata	Keterangan
P_9	Saya tahu bagaimana *password* yang kuat	4,15	Setuju
P_10	Saya tahu bagaimana *password* yang unik	4,09	Setuju
P_11	Saya tahu untuk menyimpan *password* baik secara fisik maupun digital	3,89	Setuju
P_2	Saya tahu apa itu *cybercrime*	4,22	Setuju
Rata-rata		4,09	Setuju

Dari tabel diatas, dapat dilihat hasil distribusi rata-rata bahwa tingkat pengetahuan mengamankan *password* (P_2) adalah setuju, maka pelaku *e-commerce* sudah mengetahui bagaimana cara mengamnakan *password*-nya.

4.2.2.3 Analisis Deskriptif Pengetahuan Transaksi (P_3)

Dari kumpulan pertanyaan yang diberikan kepada responden dapat dijelaskan distribusi penilaian responden terhadap pengetahuan tentang risiko transaksi *e-commerce* (P_3). Berikut tabel distribusi:

Tabel 4.9 Hasil Analisis Deskriptif Pengetahuan *Password*

Item	Indikator	Rata-rata	Keterangan
P_8	Saya tahu jika kartu debit dan kredit bisa dicuri	4,05	Setuju
P_12	Saya tahu kerentanan melakukan transaksi pada jaringan publik	4,04	Setuju
P_13	Saya tahu untuk tidak menyimpan data transaksi	3,17	Netral
P_14	Saya tahu untuk tidak mengakses akun bank pada saat menggunakan jaringan publik	3,81	Setuju
Rata-rata		3,76	Setuju

Dari tabel diatas, dapat dilihat hasil distribusi rata-rata bahwa tingkat pengetahuan risiko transaksi *e-commerce* (P_3) adalah setuju, maka pelaku *e-commerce* sudah mengetahui risiko yang terjadi saat bertransaksi di *e-commerce.*

4.2.2.4 Analisis Deskriptif Kesadaran Kejahatan (K_1)

Dari kumpulan pertanyaan yang diberikan kepada responden dapat dijelaskan distribusi penilaian responden terhadap kesadaran untuk menjaga diri dari segala jenis kejahatan siber (K_1). Berikut tabel distribusi:

Tabel 4.10 Hasil Analisis Deskriptif Kesadaran Kejahatan

Item	Indikator	Rata-rata	Keterangan
K_1	Saya sadar untuk mengabaikan email yang mengandung *phising*	3,91	Setuju
K_2	Saya sadar untuk melindungi diri dari *cybercrime*	4,28	Sangat setuju
K_3	Saya sadar untuk mengantisipasi dari kejahatan *carding*	3,98	Setuju
K_5	Saya sadar *Two-Factor Authentication* (2FA) berguna melindungi akun dari pembobolan	3,96	Setuju
K_6	Saya sadar untuk melindungi dari *phising, cybercrime, social engineering*	4,00	Setuju
K_7	Saya sadar untuk mengakses situs *e-commerce* yang menggunakan HTTPS/SSL	3,80	Setuju
Rata-rata		3,99	Setuju

Dari tabel diatas, dapat dilihat hasil distribusi rata-rata bahwa tingkat kesadaran untuk menjaga diri dari segala jenis kejahatan siber (K_1) adalah setuju. Artinya, pelaku *e-commerce* sudah menyadari untuk menjaga dirinya dari segala jenis kejahatan siber.

4.2.2.5 Analisis Deskriptif Kesadaran Password dan Pencurian (K_2)

Dari kumpulan pertanyaan yang diberikan kepada responden dapat dijelaskan distribusi penilaian responden terhadap kesadaran untuk menjaga diri dari pencurian dan kata sandi (K_2) Berikut tabel distribusi:

Tabel 4.11 Hasil Analisis Deskriptif Kesadaran *Password* dan Pencurian

Item	Indikator	Rata-rata	Keterangan
K_4	Saya sadar untuk tidak memberikan informasi pribadi (e-mail, username, password)	4,44	Sangat setuju
K_8	Saya sadar untuk menjaga kartu debit atau kredit dari pencurian	4,29	Sangat setuju
K_9	Saya sadar untuk menggunakan *password* yang kuat	4,39	Sangat setuju
K_10	Saya sadar untuk menggunakan *password* yang unik	4,17	Setuju
K_11	Saya sadar untuk menyimpan *password* pada platform yang aman	4,05	Setuju
Rata-rata		4,27	Sangat setuju

Dari tabel diatas, dapat dilihat hasil distribusi rata-rata bahwa tingkat kesadaran untuk menjaga diri dari pencurian dan kata sandi (K_2) adalah sangat setuju. Artinya, pelaku *e-commerce* sudah menyadari untuk menjaga diri dari pencurian dan kata sandinya agar tidak terjaadi pembobolan akun.

4.2.2.6 Analisis Deskriptif Kesadaran Transaksi (K_3)

Dari kumpulan pertanyaan yang diberikan kepada responden dapat dijelaskan distribusi penilaian responden terhadap kesadaran untuk menjaga diri saat melakukan transaksi *e-commerce* (K_3). Berikut tabel distribusi:

Tabel 4.12 Hasil Analisis Deskriptif Kesadaran Kejahatan

Item	Indikator	Rata-rata	Keterangan
K_12	Saya sadar untuk menggunakan *e-commerce* saat menggunakan jaringan publik	3,47	Setuju

K_13	Saya sadar untuk menyimpan data transaksi *e-commerce* dengan baik	3,86	Setuju
K_14	Saya sadar untuk mengakses akun bank pada saat menggunakan jaringan publik	3,23	Netral
Rata-rata		3,52	Setuju

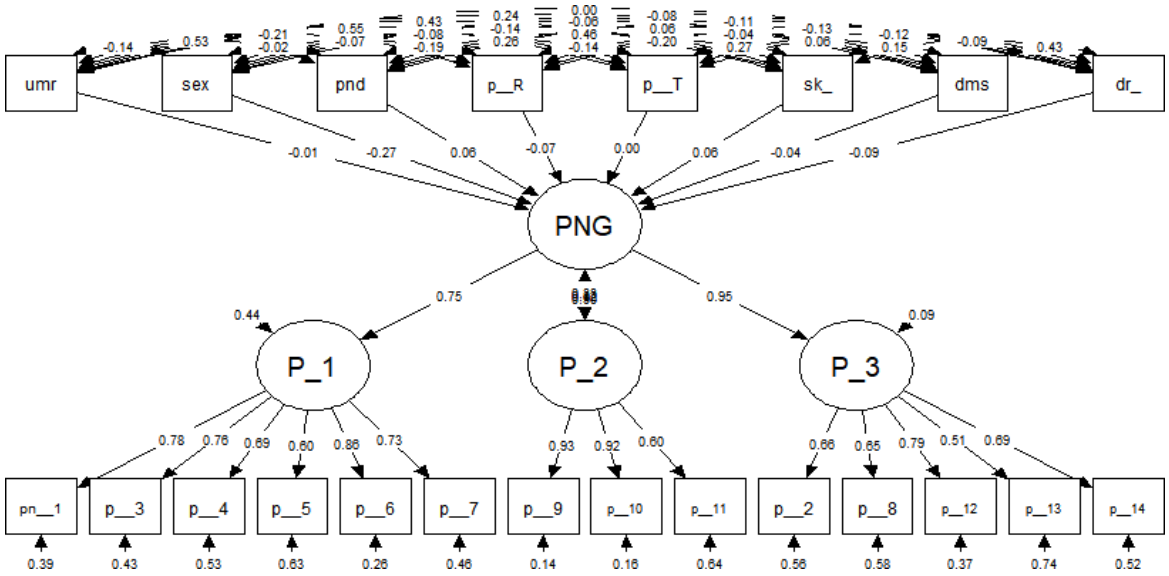
Dari tabel diatas, dapat dilihat hasil distribusi rata-rata bahwa tingkat kesadaran untuk menjaga diri saat melakukan transaksi *e-commerce* (K_3) adalah setuju. Artinya, pelaku *e-commerce* sudah menyadari untuk menjaga diri saat melakukan transaksi agar tidak terjadi risiko yang tidak diinginkan.

4.3 Analisis Kuantitatif

4.3.1 Menguji Model Struktural

Suatu model dapat diterima atau ditolak, maka kita harus menentukannya dengan mengukur model *goodness of fit* antara variabel laten dengan indikator. Jika suatu model diterima maka kita bisa menggunakan metode *Structural Equation Mode*ling (SEM) untuk melakukan interpretasi terhadap model yang telah diterima (Holgado-Tello, Chacon-Moscoso, Barbero-Garcia, & Vila-Abad, 2010). Berikut model structural untuk demografi terhadap pengetahuan:

Gambar 4.15 Output Model Diagram Demografi Terhadap Pengetahuan



Berdasarkan hasil model pada Gambar 4.15 Output Model Diagram Demografi Terhadap Pengetahuan, maka selanjutnya dilakukan pengujian terhadap model dengan menggunakan kriteria sebagai berikut:

Tabel 4.13 Hasil Uji Goodness of Fit Demografi Terhadap Pengetahuan

Indikator	Standar	Hasil	Keterangan
CMIN/DF	< 5,0	2,52	Fit
SRMR	< 0,08	0,05	Fit
RMSEA	< 0,08	0,06	Fit
CFI	> 0,80	0,90	Fit
TLI	> 0,80	0,89	Fit

Dapat dilihat pada Tabel 4.13, model penelitian ini merupakan penelitian dengan model good fit.

CMIN/DF akan menunjukkan hasil the minimum sample discrepancy function yang dibagi dengan degree of freedom. Hasil CMIN/DF pada penelitian ini adalah 2,52. Nilai tersebut sudah sesuai dengan kriteria yaitu < 5,00 (Wheaton, Muthen, Alwin, & Summers, 1977) hal ini menunjukkan bahwa model penelitian ini fit.

SRMR (*Standardized Root Mean Square Residual*) didefinisikan sebagai perbedaan antara korelasi yang diamati dan model yang menyatakan matriks korelasi dengan nilai kurang dari 0,08 (Hu & Bentler, 1999). Pada penelitian ini nila SRMR yang didapat adalah 0,05 sehingga dikatakan model fit.

RMSEA (*The Root Mean Square of Aprroximation*) adalah indeks yang digunakan untuk mengkompenasi chi-square dalam sampel yang besar. Nilai RMSEA yang lebih kecil atau sama dengan 0,08 (MacCallum, Browne, & Sugawara, 1996) merupakan indeks yang dapat diterima modelnya. Nilai RMSEA penelitian ini adalah 0,06. Model penelitian ini menunjukkan model yang fit.

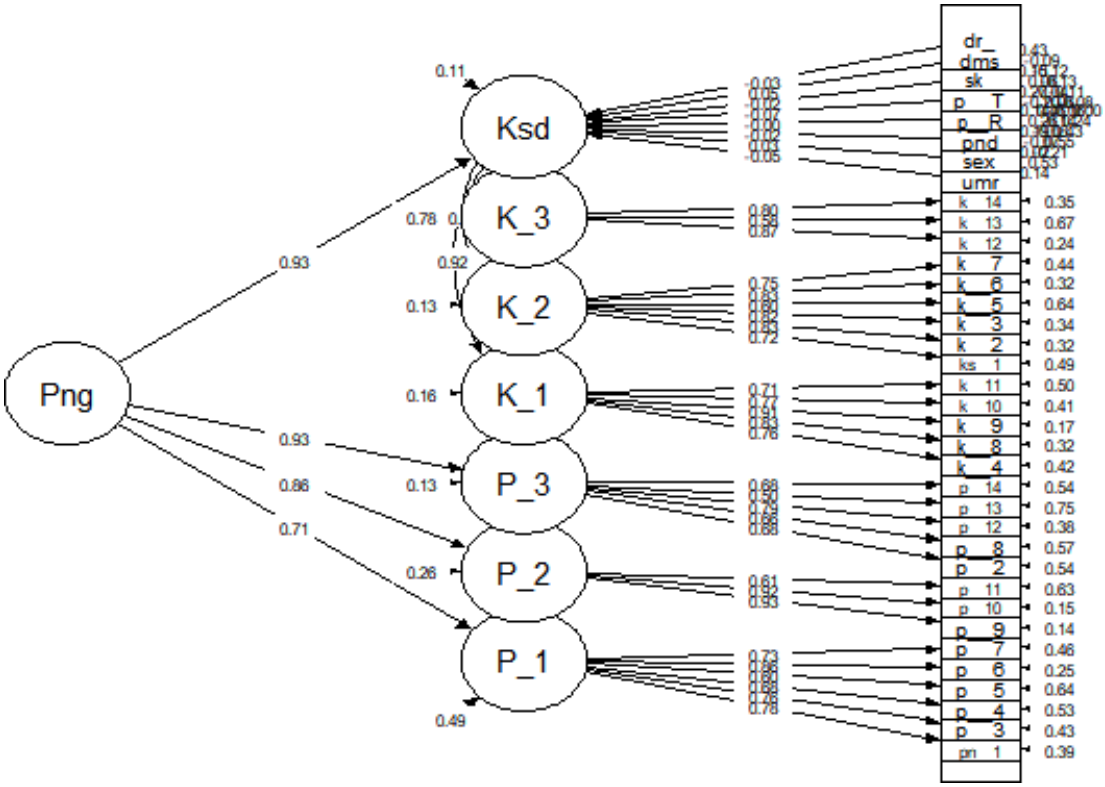
CFI (*Comperative Fit Index*) adalah indeks yang relatif tidak berpengaruh terhadap seberapa besar sampel dan kerumitan model. Nilai CFI pada penelitian ini adalah 0,90. Nilai tersebut sesuai dengan kriteria yaitu > 0,80 (Hu & Bentler, 1999) hal ini mengindikasikan tingkat marginal fit.

TLI (*Tucker Lewis Index*) merupakan sebuah model yang diujikan terhadap baseline model dengan membandingkan *alternative fit index*. Hasil dari TLI pada penelitian ini adalah 0,89. Nilai tersebut sesuai dengan kriteria yaitu > 0,80 (Marsh, Balla, & McDonald, 1988) hal ini menunjukkan bahwa model penelitian ini marginal fit.

Berdasarkan keseluruhan pengukuran goodness of fit, semua indeks menunjukkan model penelitian yang baik. Berarti model yang diajukan dalam penelitian ini dapat diterima karena telah memenuhi kriteria fit.

Selanjutnya peneliti akan melakukan uji model pengetahuan dan demografi terhadap kesadaran Berikut model structural:

Gambar 4.16 Output Model Diagram Pengetahuan dan Demografi Terhadap Kesadaran



Berdasarkan hasil model pada Gambar 4.16, maka selanjutnya dilakukan pengujian terhadap model dengan menggunakan kriteria sebagai berikut:

Tabel 4.14 Hasil Uji Goodness of Fit Pengetahuan dan Demografi Terhadap Kesadaran

Indikator	Standar	Hasil	Keterangan
CMIN/DF	< 5,0	3,51	Fit
SRMR	< 0,08	0,09	Acceptable fit
RMSEA	< 0,08	0,08	Fit
CFI	> 0,80	0,81	Fit
TLI	> 0,80	0,79	Marginal fit

Dapat dilihat pada tabel Tabel 4.14, model penelitian ini merupakan penelitian dengan model good fit.

CMIN/DF akan menunjukkan hasil the minimum sample discrepancy function yang dibagi dengan degree of freedom. Hasil CMIN/DF pada penelitian ini adalah 3,51. Nilai tersebut sudah sesuai dengan kriteria yaitu < 5,00 (Wheaton, Muthen, Alwin, & Summers, 1977) hal ini menunjukkan bahwa model penelitian ini fit.

SRMR (*Standardized Root Mean Square Residual*) didefinisikan sebagai perbedaan antara korelasi yang diamati dan model yang menyatakan matriks korelasi dengan nilai kurang dari 0,08 (Hu & Bentler, 1999). Pada penelitian ini nila SRMR yang didapat adalah 0,09 dengan kriteria acceptable fit karena mendekati 0,08.

RMSEA (*The Root Mean Square of Aprroximation*) adalah indeks yang digunakan untuk mengkompenasi chi-square dalam sampel yang besar. Nilai RMSEA yang lebih kecil atau sama dengan 0,08 (MacCallum, Browne, & Sugawara, 1996) merupakan indeks yang dapat diterima modelnya. Nilai RMSEA penelitian ini adalah 0,08. Model penelitian ini menunjukkan model yang fit.

CFI (*Comperative Fit Index*) adalah indeks yang relatif tidak berpengaruh terhadap seberapa besar sampel dan kerumitan model. Nilai CFI pada penelitian ini adalah 0,81. Nilai tersebut sesuai dengan kriteria yaitu > 0,80 (Hu & Bentler, 1999) hal ini mengindikasikan tingkat marginal fit.

TLI (*Tucker Lewis Index*) merupakan sebuah model yang diujikan terhadap baseline model dengan membandingkan *alternative fit index*. Hasil dari TLI pada penelitian ini adalah 0,79. Nilai tersebut sesuai dengan kriteria yaitu > 0,80 (Marsh, Balla, & McDonald, 1988) hal ini menunjukkan bahwa model penelitian ini marginal fit.

Berdasarkan keseluruhan pengukuran goodness of fit, semua indeks menunjukkan model penelitian yang baik. Berarti model yang diajukan dalam penelitian ini dapat diterima karena telah memenuhi kriteria fit.

4.3.2 Pengujian Hipotesis

Parameter penilaian *estimate coefficient* merupakan hal yang krusial dalam hal melakukan uji hipotesis (Chandio, 2011). *Estimate coefficient* digunakan untuk melakukan evaluasi pemodelan hipotesis. Ketika pengujian probabilitas (p) memiliki nilai kurang dari ≤0,05 dan nilai dari *critical ratio* (C.R) mempunyai nilai lebih dari 1,96 maka hipotesis dapat dikatakan diterima dan dapat dilakukan interpretasi hasil. Berikut tabel di bawah memperlihatkan hasil dari pengujian *structural model*:

Tabel 4.15 Hasil Uji Hipotesis Demografi Terhadap Pengetahuan

Index	Estimate	C.R	P
Umur > Png	-0,001	-0,075	0,940
Jenis kelamin (Perempuan) > Png	0,438	4,690	****
Pendidikan (Tinggi)> Png	0,103	0,906	0,365
Pendapatan_bln_R > Png	-0,128	-1,252	0,211
Pendapatan_bln_T > Png	0,006	0,027	0,978
Sektor _job (bekerja) > Png	0,089	0,875	0,382
Domisili (luar Jawa) > Png	-0,094	-0,678	0,498
Daerah_asal (luar Jawa) > Png	-0,154	1,518	0,129

Berdasarkan hasil uji hipotesis pada Tabel 4.15 dapat diambil kesimpulan bahwa:

1. Ada hubungan antara jenis kelamin dan pengetahuan *cyber security e-commerce* dinyatakan dengan hubungan bersifat signifikan, karena nilai dari *critical ratio (C.R)* adalah 4,690, kemudian *estimate* juga menghasilkan nilai sebesar 0,438, dan probabilitas (p) memiliki nilai kurang ≤0,001.

Tabel 4.16 Hasil Uji Hipotesis Pengetahuan dan Demografi Terhadap Kesadaran

Index	Estimate	C.R	P
Ksd > Png	0,718	10,851	****
Ksd > Umur	-0,006	-1,160	0,246
Ksd > Jenis kelamin (Perempuan)	0,032	0,829	0,407
Ksd > Pendidikan (Tinggi)	-0,028	-0,560	0,576
Ksd > Pendapatan_bln_R	-0,003	-0,073	0,941
Ksd > Pendapatan_bln_T	-0,167	-1,729	0,084
Ksd > Sektor _job (bekerja)	-0,018	-0,413	0,679
Ksd > Domisili (luar Jawa)	0,091	1,487	0,137
Ksd > Daerah_asal (luar Jawa)	0,042	-0,940	0,347

Berdasarkan hasil uji hipotesis pada Tabel 4.16 dapat diambil kesimpulan bahwa:

1. Kesadaran *cyber security* berpengaruh pada pengetahuan *cyber security* dinyatakan terdapat hubungan signifikan, hal ini berdasarkan nilai *critical ratio (C.R)* sebesar 10,851, nilai *estimate* adalah 0,718, dan probabilitas (p) memiliki nilai ≤ 0,001.

44 Pembahasan

Dari hasil analisis deskriptif variabel kesadaran bahwa, responden memiliki tingkat kesadaran untuk menjaga diri dari pencurian dan kata sandi (K_1) dengan tingkat kesadaran 4,27 (sangat sadar), sementara kesadaran untuk menjaga diri dari segala jenis kejahatan siber (K_2) responden memiliki tingkat kesadaran 3,99 (sadar), dan untuk kesadaran dalam menjaga diri saat melakukan transaksi *e-commerce* (K_3) adalah 3,52 (sadar).

Setelah melakukan analisis, maka peneliti akan melakukan pembahasan terkait faktor demografi yang terdapat jenis kelamin, usia, domisili, daerah asal, pendapatan, pekerjaan, dan pendidikan terakhir dan pengaruh pengetahuan terhadap kesadaran *cyber security*.

Analisis yang dilakukan oleh peneliti, menemukan bahwa jenis kelamin merupakan faktor yang mempengaruhi pengetahuan *cyber security* pengguna *e-commerce* dinyatakan dengan pengaruh yang signifikan, dengan nilai dari *critical ratio (C.R)* adalah 4,690, kemudian *estimate* nilai sebesar 0,438, dan probabilitas (p) H0 ditolak dengan nilai kurang ≤0,05. Hal ini diperkuat dengan penelitian serupa oleh Garbarino & Strahilevitz (2004) yang menemukan bahwa perempuan merasakan tingkat risiko yang secara signifikan memiliki resiko lebih tinggi dalam belanja online. Beberapa penelitian juga menunjukkan bahwa perbedaan jenis kelamin dalam penggunaan teknologi, perempuan telah terbukti memiliki tingkat masalah privasi yang lebih tinggi dalam penyebaran informasi mereka ketimbang laki-laki (Chai, Das, & Rao, 2014). Oleh karena itu, hal ini mengungkapkan bahwa laki-laki memiliki perbedaan pengetahuan *cyber security* yang lebih tinggi dibandingkan perempuan.

Individu dengan pengetahuan yang baik secara tidak langsung juga akan mempengaruhi kesadaran *cyber security*. Hal ini diperkuat dengan temuan hasil di mana memiliki pengaruh yang signifikan pada analisis yang dilakukan dengan nilai *estimate* sebesar 0,718, kemudian nilai *critical ratio (C.R)* adalah 10,851, dan probabilitas (p) H0 ditolak dengan nilai kurang ≤ 0,05. Sehingga individu biasanya lebih mengetahui jenis kejahatan yang biasanya terjadi pada *e-commerce*. Selain itu, individu juga mampu mengetahui kriteria untuk jenis *password* yang kuat dan aman. Yang lebih menarik, individu mampu mengetahui dalam hal melindungi diri dari ancaman yang berkaitan dengan risiko transaksi (Rhee, Kim, & Ryu, 2009).

Selanjutnya pada analisis yang dilakukan, ternyata usia tidak terbukti sebagai faktor yang mempengaruhi pengetahuan *cyber security*, hal ini diperkuat dengan temuan pada uji hipotesis dengan *estimate* bernilai sebesar 0,438, kemudian nilai dari *critical ratio (C.R)* adalah 4,690, dan probabilitas (p) H0 gagal tolak dengan nilai lebih dari > 0,05. Dengan hasil uji seperti itu, maka dinyatakan bahwa usia tidak memiliki memiliki pengaruh yang signifikan terhadap

tingkat pengetahuan *cyber security* individu. Hal ini bisa terjadi, karena pengetahuan yang dimiliki individu berbeda karena tiap individu memiliki usia bervariasi sehingga pengalaman yang didapat tentunya juga berbeda pula. Sebuah teori juga mengatakan, bahwa usia mempengaruhi proses berpikir dan daya tangkap manusia, semakin tua usia maka semakin baik juga mentalnya, akan tetapi hal tersebut tidak berlaku ketika umur belasan tahun yang perkembangannya sedikit lambat (Settersten, Richard A., & Angel, 2011). Sehingga, usia seseorang tidak berpengaruh pada pengetahuan maupun kesadaran *cyber security*.

Kemudian, analisis dilakukan dengan melihat pengaruh faktor pendidikan terhadap pengetahuan dan kesadaran *cyber security* para responden, ternyata didapatkan hasil yang tidak memiliki pengaruh yang signifikan. Hal ini diperkuat dengan hasil uji hipotesis pengaruh pendidikan dengan pengetahuan dengan nilai *estimate* sebesar 0,103, kemudian nilai dari *critical ratio (C.R)* adalah 0,906, dan probabilitas (p) H0 gagal tolak dengan nilai lebih dari > 0,05. Untuk pengaruh terhadap kesadaran dengan nilai *estimate* sebesar -0,028, kemudian nilai dari *critical ratio (C.R)* adalah -0,560 dan probabilitas (p) H0 gagal tolak dengan nilai lebih dari > 0,05. Kemungkinan hasil yang didapat tidak berpengaruh, yakni pendidikan seseorang tidak secara langsung didapat melalui pendidikan secara formal, namum bisa saja didapat secara non formal. Karena pendidikan formal yang dipelajari di Indonesia sendiri belum sepenuhnya mempelajari secara dalam tentang *cyber security* itu sendiri maka ketika ingin mempelajari hal tersebut bisa melalui pendidikan nonformal atau mengambil pendidikan tinggi yang secara khusus mempelajari hal tersebut, wajar jika pengetahuan dan kesadaran tentang *cyber security* tidak berpengaruh terhadap pendidikan formal itu sendiri.

Selanjutnya, kita lihat hasil analisis pengaruh faktor pendapatan terhadap pengetahuan dan kesadaran *cyber security,* pendapatan dibagi menjadi dua yaitu pendapatan tinggi (di atas Rp5juta perbulan dan pendapatan rendah (di bawah Rp5juta perbulan). Hasil uji hipotesis pendapatan terhadap pengetahuan yaitu nilai *estimate* sebesar -0,128 untuk rendah dan 0,006 untuk tinggi, kemudian nilai dari *critical ratio (C.R)* adalah -1,252 untuk rendah dan 0,027 untuk tinggi, dan masing-masing probabilitas (p) H0 gagal tolak dengan nilai lebih dari > 0,05. Untuk uji hipotesis pendapatan terhadap kesadaran yaitu nilai *estimate* sebesar -0,003 untuk rendah dan -0,167 untuk tinggi, kemudian nilai dari *critical ratio (C.R)* adalah -0,073 untuk rendah dan -1,729 untuk tinggi, dan masing-masing probabilitas (p) H0 gagal tolak dengan nilai lebih dari > 0,05 maka dinyatakan bahwa hasil tidak memiliki pengaruh yang signifikan. Alasan faktor pendapatan tidak berpengaruh terhadap pengetahuan maupun kesadaran karena tidak hanya orang dengan pendapatan tinggi saja yang bisa mendapatkan pengetahuan dan

menyadarinya, bahkan orang dengan pendapatan rendah juga bisa mendapatkan informasi dan langsung menyadari (Ar-Rasily & Dewi, 2016). Selain itu, pendapatan seseorang juga mempengaruhi fasilitas yang menjadi prioritasnya.

Analisis selanjutnya yaitu faktor pekerjaan seseorang terhadap pengetahuan dan kesadaran *cyber security* mereka. Analisis yang dilakukan mendapatkan hasil pekerjaan terhadap pengetahuan yaitu nilai *estimate* sebesar 0,089, kemudian nilai dari *critical ratio (C.R)* adalah 0,875, dan probabilitas (p) H0 gagal tolak dengan nilai lebih dari > 0,05. Kemudian untuk pengaruh pekerjaan terhadap kesadaran yaitu nilai *estimate* sebesar -0,018, kemudian nilai dari *critical ratio (C.R)* adalah -0,413, dan probabilitas (p) H0 gagal tolak dengan nilai lebih dari > 0,05 dengan begitu pekerjaan tidak memiliki pengaruh yang signifikan terhadap pengetahuan dan kesadaran *cyber security* para pelaku *e-commerce*. Hal ini bisa disimpulkan bahwa individu yang bekerja maupun yang tidak bekerja tidak berpengaruh terhadap pengetahuan dan kesadaran *cyber security* karena pekerjaan masing-masing individu tidak hanya berfokus pada satu bidang yang terkait *cyber*, tetapi masih banyak bidang pekerjaan yang tidak terjun langsung terhadap *cyber security* itu sendiri, sehingga hal ini tidak mempengaruhi pengetahuan dan kesadaran mereka terhadap hal tersebut.

Lebih lanjut peneliti melihat faktor domisili dan daerah asal terhadap pengetahuan dan kesadaran *cyber security*. Hasil analisis untuk domisili yaitu nilai *estimate* sebesar -0,094, kemudian nilai *critical ratio (C.R)* adalah -0,678, dan probabilitas (p) H0 gagal tolak dengan nilai lebih dari > 0,05. Sementara hasil untuk daerah asal, yakni nilai *estimate* sebesar -0,154, kemudian nilai *critical ratio (C.R)* adalah 1,518, dan probabilitas (p) H0 gagal tolak dengan nilai lebih dari > 0,05, maka hasil tersebut menyatakan bahwa faktor domisili dan daerah asal tidak memiliki pengaruh yang signifikan. Dalam kesimpulannya, keberagaman tempat tinggal dan daerah asal yang terjadi di Indonesia membuat akses informasi yang didapat juga berbeda-beda sehingga hal ini yang mempengaruhi hal tersebut. Lebih lanjut lagi, daerah asal atau domisili juga mempengaruhi bagaimana seseorang tersebut menyikapi hal terjadi atas fenomena yang terjadi berdasarkan pengetahuan yang didapat dari domisili atau daerah asalnya. Sehingga, hal ini membuat tidak adanya pengaruh daerah asal dan domisili terhadap pengetahuan dan kesadaran *cyber security.*

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis data telah terjawab bahwa tingkat kesadaran pelaku *e-commerce* dipengaruhi oleh pengetahuan *cyber security*, yakni memiliki hubungan positif yang berpengaruh signifikan terhadap kesadaran *cyber security*. Maka ketika ancaman siber datang, individu dengan pengetahuan *cyber security* yang baik akan menyadari dengan ancaman dan akan segera mengamankan diri dari hal yang menggangu dalam menggunakan *e-commerce.*

Selain itu, perbedaan jenis kelamin merupakan salah satu faktor dalam hal pengetahuan *cyber security*. Penelitian ini mendapatkan hasil, bahwa terdapat kesenjangan pengetahuan yang besar antara laki-laki dan perempuan, di mana perempuan memiliki pengetahuan *cyber security* yang lebih rendah daripada laki-laki yang secara tidak langsung berpengaruh pada kesadaran *cyber security*. Sehingga hal ini membuat perempuan lebih rentan menjadi korban *cybercrime*.

5.2 Saran

Hal ke depan yang dapat dikerjakan dari penelitian ini adalah dengan menentukan spesifikasi model yang lebih tepat, sehingga untuk beberapa faktor yang belum terjawab atau tidak signifikan bisa ditemukan jawabannya. Selain itu, penelitian ini bisa dijadikan sebagai bahan kajian untuk edukasi kepada pelaku *e-commerce* terhadap pengetahuan *cyber security*-nya.

DAFTAR PUSTAKA

Amaliya, U. (2009). E-Commerce di Singapura dan Indonesia : Sebuah Perbandingan Kebijakan. *Jurnal Ilmu Sosial dan Ilmu Politik, 1*(e-commerce), 1-21.

Ashaf, A. F. (2009). *Jurnalis Perempuan dan Aktivisme Media: Perspektif Kritis.* Bandung: Unpad Press.

Bishop, M. (2003). What is computer security? *IEEE Security & Privacy, 1*(1), 67-69.

Bollen, K. A. (1989). *Structural Equations with Latent Variables.* New York: Wiley.

Chai, S., Das, S., & Rao, H. R. (2014). Factors Affecting Bloggers' Knowledge Sharing: An Investigation Across Gender. *Journal of Management Information Systems, 28*, 309-342.

Chalmers, D. (1997). *The Conscious Mind: In Search of a Fundamental Theory.* Oxford: Oxford University Press.

Chandio, F. H. (2011). Studying acceptance of online banking information system: A structural equation model. *Brunel University Brunel Business School PhD Theses*.

Das, K., Tamhane, T., Vatterott, B., Wibowo, P., & Wintels, S. (2018). The digital archipelago: How online commerce is driving Indonesia's economic development. *McKinsey & Company*, 1-72.

Direktorat Tindak Pidana Siber Bareskrim Polri. (2019, Desember). *Patroli SIber.* Retrieved from https://patrolisiber.id/statistic

Finch, J., & West, S. G. (1997). The investigation of personality structure: Statistical models. *Journal of Research in Personality*, 439-485.

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the. *Journal of Business Research, 57*, 768-775.

George, D., & Mallery, P. (2003). *SPSS for Windows 2003 Step By Step: A Simple Guide and Reference 11.0 Update.* Boston: Allyn and Bacon.

Ghozali, I., & Fuad. (2008). *Structural Equation Modeling : Teori, Konsep, dan Aplikasi Dengan Lisrel 8.80.* Semarang: UNDIP.

GlobalWebIndex. (2019). *Commerce Flagship Report on the Latest Trends in Online Commerce.*

Hair Jr, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2009). *Multivariate Data Analysis (7th Edition).* Pearson.

Heale, R., & Alison, T. (2015). Validity and reliability in quantitative studies. *Evidence-Based Nursing, 18*(3), 66-67.

Holgado-Tello, P. F., Chacon-Moscoso, S., Barbero-Garcia, I., & Vila-Abad, E. (2010). Polychoric versus Pearson correlations in exploratory. *Quality and Quantity*, 153-166.

Hox, J., & Bechger, T. (1999). An Introduction to Structural Equation Modeling. *Family Science Review, 11*, 354-373.

Hu, L.-t., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling*, 1-55.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power Analysis and Determination of Sample Size for. *Psychological Methods, 1*(2), 130-149.

Marsh, H. W., Balla, J. R., & McDonald, R. P. (1988). Goodness-of-fit indexes in confirmatory factor analysis: The effect of sample size. *Psychological Bulletin, 103*(3), 391-410.

Norris, M., & Lecavalier, L. (2009). Evaluating the Use of Exploratory Factor Analysis in Developmental Disability Psychological Research. *Journal of Autism and Developmental Disorders*, 8-20.

Park, C.-H., & Kim, Y.-G. (2006). The Effect of Information Satisfaction and Relational Benefit on Consumers' Online Shopping Site Commitments. *Journal of Electronic Commerce in Organizations*, 70-90.

Prihandini, T. I., & Sunaryo, S. (2011). STRUCTURAL EQUATION MODELLING (SEM) DENGAN MODEL STRUKTURAL REGRESI SPASIAL. *Prosiding Seminar Nasional Statistika Universitas Diponegoro*, 162-170.

Ramadiani. (2010). Structural Equation ModelUntuk Analisis Multivariate Menggunakan LISREL. *Jurnal Informatika Mulawarman*, 14.

Reber, A. S., & Reber, S. E. (2010). *Kamus Psikologi.* Yogyakarta: Pustaka Pelajar.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end. *Computers & Security , 28*, 816-826.

Settersten, J., Richard A., & Angel, J. (2011). *Handbook of Sociology of Aging.* Springer.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness. *Computers & Education, 52*, 92-100.

Soekidjo, N. (2003). *Pengembangan Sumber Daya Manusia.* Jakarta: PT. Rineka Cipta.

Statista. (2020, May). *eCommerce*. (Statista) Retrieved from https://www.statista.com/outlook/243/120/ecommerce/indonesia#market-users

Sugiyono. (2009). *Metode Penelitian Kuantitatif, Kualitatif dan R&D.* Bandung: Alfabeta.

Sugiyono. (2016). *Metode Penelitian Kuantitatif, Kualitatif dan R&D.* Bandung: PT Alfabet.

Supranto, J. (2004). *Analisis Multivariat: Arti dan interpretasi.* Jakarta: PT. Rineka Cipta.

Ullman, J. B., & Bentler, P. M. (2003). Structural Equation Modeling. *Handbook of Psychology*.

Wheaton, B., Muthen, B., Alwin, D. F., & Summers, G. F. (1977). Assesing Reliability and Stability in Panel Models. *Sociological Methodology*, *8*, 84-136.

Widarjono, A. (2010). *Analisis Statistika Multivariat Terapan.* Yogyakarta: Unit Penerbit dan Percetakan STIM YKPN.

Worthington, R. L., & Whittaker, T. A. (2006). Scale development research: A content analysis and recommendations for best practice. *The Counseling Psychologist*, 806-838.

**

LAMPIRAN

Kuisioner Penelitian

Bapak/Ibu/Saudara/i yang saya hormati, perkenalkan saya Galih Rahmadi mahasiswa Program Studi Informatika Universitas Islam Indonesia Yogyakarta.

Saya bermaksud mengadakan penelitian dengan judul Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia. Maka dengan segala kerendahan hati peneliti, memohon kesediaan Bapak/Ibu/Saudara/i untuk sedikit meluangkan waktu sekitar 10 menit dalam mengisi kuesioner ini.

Saya memohon kesediaan Bapak/Ibu/Saudara/i untuk menjawab semua pertanyaan yang ada secara JUJUR dan TERBUKA, mengingat data yang saya perlukan sangat besar sekali artinya. Peneliti menjamin KERAHASIAAN identitas dan setiap jawaban responden, dikarenakan penelitian ini semata-mata bersifat ilmiah dan hanya dipergunakan untuk keperluan penyusunan skripsi.

Atas segala bantuan dan partisipasi yang Bapak/Ibu/Saudara/i berikan, saya ucapkan terima kasih. Semoga segala kebaikan mendapatkan balasan yang lebih baik dari Tuhan Yang maha Esa dan hasil dari penelitian ini dapat bermanfaat bagi kita semua. Aamiin.

Hormat saya,
Galih Rahmadi

Bagian 1: Pertanyaan Umum

Berisi pertanyaan umum mengenai demografi dan data diri Anda. Mohon isi dengan penuh keterbukaan dan kejujuran, segala rahasia akan dijamin oleh peneliti.

1. Inisial:
2. Umur:
3. Jenis Kelamin:
    - Laki-laki
    - Perempuan
4. Pendidikan terakhir:
    - SD
    - SMP
    - SMA

**

- Sarjana (S1)
- Magister (S2)
- Doktor (S3)

5. Pendapatan Bulanan:
    - Kurang dari Rp. 1.000.000
    - Rp. 1.000.000 - 2.999.999
    - Rp. 3.000.000 - 4.999.999
    - Rp. 5.000.000 - 9.999.999
    - Rp. 10.000.000 - 19.999.999
    - Rp. 20.000.000 atau lebih
6. Pekerjaan
    - Tidak bekerja
    - Negeri
    - Lepas (Freelance)
    - Swasta
7. Domisili
    - Nanggroe Aceh Darussalam
    - Sumatera Utara
    - Sumatera Barat
    - Riau
    - Kepulauan Riau
    - Jambi
    - Bengkulu
    - Sumatera Selatan
    - Kepulauan Bangka Belitung
    - Lampung
    - Banten
    - DKI Jakarta
    - Jawa Barat
    - Jawa Tengah
    - Jawa Timur
    - DI Yogyakarta

**

- Bali
- Nusa Tenggara Barat
- Nusa Tenggara Timur
- Kalimantan Barat
- Kalimantan Selatan
- Kalimantan Tengah
- Kalimantan Timur
- Kalimantan Utara
- Gorontalo
- Sulawesi Barat
- Sulawesi Selatan
- Sulawesi Tenggara
- Sulawesi Tengah
- Sulawesi Utara
- Maluku
- Maluku Utara
- Papua
- Papua Barat

8. Daerah Asal
    - Nanggroe Aceh Darussalam
    - Sumatera Utara
    - Sumatera Barat
    - Riau
    - Kepulauan Riau
    - Jambi
    - Bengkulu
    - Sumatera Selatan
    - Kepulauan Bangka Belitung
    - Lampung
    - Banten
    - DKI Jakarta
    - Jawa Barat

**

- Jawa Tengah
- Jawa Timur
- DI Yogyakarta
- Bali
- Nusa Tenggara Barat
- Nusa Tenggara Timur
- Kalimantan Barat
- Kalimantan Selatan
- Kalimantan Tengah
- Kalimantan Timur
- Kalimantan Utara
- Gorontalo
- Sulawesi Barat
- Sulawesi Selatan
- Sulawesi Tenggara
- Sulawesi Tengah
- Sulawesi Utara
- Maluku
- Maluku Utara
- Papua
- Papua Barat

Bagian 2: Pengetahuan tentang keamanan

1. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu apa itu phising]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
2. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu apa itu cyber crime]
    - Sangat Tidak Setuju
    - Tidak Setuju

**

- Netral
- Setuju
- Sangat Setuju

3. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu apa itu carding]
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
4. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu apa itu social engineering
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
5. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu apa itu Two-Factor Authentication (2FA)]
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
6. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu bagaimana melindungi dari 'phising, 'cyber crime', 'social engineering']
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
7. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu situs e-Commerce yang aman seperti apa (HTTPS, SSL, dll)]
   - Sangat Tidak Setuju

**

- Tidak Setuju
- Netral
- Setuju
- Sangat Setuju

8. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu jika kartu debit dan kredit bisa dicuri]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
9. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu bagaimana password yang kuat]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
10. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu bentuk password yang unik]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
11. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu untuk menyimpan password baik secara fisik maupun digital]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju

**

12. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu kerentanan transaksi pada jaringan publik]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
13. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu untuk tidak menyimpan data transaksi]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
14. Pengetahuan Tentang Keamanan (Cyber Security) [Saya tahu untuk tidak mengakses akun bank pada saat menggunakan jaringan publik]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju

Bagian 3: Kesadaran tentang kemanan

1. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk mengabaikan email yang mengandung phising]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
2. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk melindungi diri dari cyber crime]

**

- Sangat Tidak Setuju
- Tidak Setuju
- Netral
- Setuju
- Sangat Setuju

3. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk mengantisipasi dari kejahatan carding (transaksi pada EDC resmi)]
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
4. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk tidak memberikan informasi pribadi kamu (e-mail, username, password)]
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
5. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar Two-Factor Authentication (2FA) berguna melindungi akun dari pembobolan]
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
6. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk melindungi dari 'phising, 'cyber crime', 'social engineering']
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju

**

- Sangat Setuju

7. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk mengakses situs e-Commerce yang menggunakan HTTPS/SSL]
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
8. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk menjaga kartu debit atau kredit dari pencurian]
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
9. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk menggunakan password yang kuat]
   - Sangat Tidak Setuju
   - Tidak Setuju
   - Netral
   - Setuju
   - Sangat Setuju
10. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk menggunakan password yang unik/berbeda]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
11. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk menyimpan password pada platform yang aman]
    - Sangat Tidak Setuju

**

- Tidak Setuju
- Netral
- Setuju
- Sangat Setuju

12. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk menggunakan e-Commerce saat menggunakan jaringan publik]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
13. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk menyimpan data transaksi e-Commerce]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju
14. Kesadaran Tentang Keamanan (Cyber Security) [Saya sadar untuk mengakses akun bank pada saat menggunakan jaringan publik]
    - Sangat Tidak Setuju
    - Tidak Setuju
    - Netral
    - Setuju
    - Sangat Setuju